A CLASSIFICATION OF POLYNOMIAL FUNCTIONS SATISFYING THE JACOBI IDENTITY OVER INTEGRAL DOMAINS

JEAN-LUC MARICHAL AND PIERRE MATHONET

Abstract. The Jacobi identity is one of the properties that are used to define the concept of Lie algebra and in this context is closely related to associativity. In this paper we provide a complete description of all bivariate polynomials that satisfy the Jacobi identity over infinite integral domains. Although this description depends on the characteristic of the domain, it turns out that all these polynomials are of degree at most one in each indeterminate.

1. Introduction

Let $\mathcal{R}$ be an infinite integral domain with identity. In this paper we are interested in a classification of all bivariate polynomials P over $\mathcal{R}$ satisfying Jacobi's identity

$$P(P(x,y),z) + P(P(y,z),x) + P(P(z,x),y) = 0. \tag{1}$$

To give a simple example, consider the set $\mathcal{R} = \mathbb{Z}_3[x]$ of univariate polynomials whose coefficients are in $\mathbb{Z}_3$. One can easily verify that the bivariate polynomial P over $\mathbb{Z}_3[x]$ defined by

$$P(A,B) = (1-x^2)AB + (x+1)(1-x^2)(A+B) + x(x+1)(1-x-x^2)$$

satisfies Jacobi's identity (1).

As it is well known, the Jacobi identity is one of the defining properties of Lie algebras. Recall that a *Lie algebra* (see, e.g., [4–6]) is a vector space $\mathfrak{g}$ together with a binary map $[\cdot,\cdot]\colon \mathfrak{g}\times\mathfrak{g}\to\mathfrak{g}$, called *Lie bracket*, such that

1. $[\cdot,\cdot]$ is bilinear,
2. $[x,y] = -[y,x]$ for all $x,y\in\mathfrak{g}$.
3. $[[x,y],z] + [[y,z],x] + [[z,x],y] = 0$ for all $x,y,z\in\mathfrak{g}$.

The second condition is usually called skew-symmetry while the third one is known as the Jacobi identity. By using a prefix notation for the Lie bracket, the Jacobi identity simply becomes the functional equation given in (1).

The classical associativity property is closely connected to Lie algebras in the following way (see, e.g., [6, p. 6]). The Lie bracket defined by $[x,y] = xy - yx$ on any associative algebra satisfies the three properties above, including Jacobi's identity. This is one of the reasons why "the Jacobi identity can be viewed as a substitute for associativity" [5, p. 54].

We now state our main result, which provides a complete description of the possible polynomial solutions over $\mathcal{R}$ of Jacobi's identity (1). Although the form

Date: March 10, 2017.
2010 *Mathematics Subject Classification.* Primary 39B72; Secondary 13B25, 17B99.
Key words and phrases. Jacobi's identity, polynomial, integral domain.

of these polynomials depends on the characteristic of $\mathcal{R}$, they are all of degree at most one in each indeterminate.

Main Theorem. *Consider a bivariate polynomial $P \in \mathcal{R}[x,y]$.*

- *If $\mathrm{char}(\mathcal{R}) \neq 3$, then P satisfies Jacobi's identity iff there exist $B, C \in \mathcal{R}$ satisfying $B^2 + BC + C = 0$ such that*
$$P(x,y) = Bx + Cy,$$
- *If $\mathrm{char}(\mathcal{R}) = 3$, then P satisfies Jacobi's identity iff one of the following conditions holds:*
  - *there exist $A, B, D \in \mathcal{R}$ satisfying $AD = B^2 - B$ such that*
  $$P(x,y) = Axy + B(x+y) + D,$$
  - *there exist $B, C, D \in \mathcal{R}$ satisfying $B^2 + BC + C = 0$ such that*
  $$P(x,y) = Bx + Cy + D.$$

The reader interested in possible generalizations of the Main Theorem might want to consider extensions of functional equation (1) to n-indeterminate polynomials, by analogy with n-ary generalizations of Lie algebras, where Jacobi's identity involves an n-linear bracket. In this direction we remark that a complete classification of n-ary associative polynomials over $\mathcal{R}$ can be found in [10] and that, in the special case when $\mathcal{R}$ is the complex plane $\mathbb{C}$, this classification was recently generalized to n-ary associative formal power series in [3].

Remark. In the literature on Lie algebras the Jacobi identity is sometimes given in one of the following alternative forms (which are equivalent to the one above under bilinearity and skew-symmetry):

$$[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0, \tag{2}$$

$$[x,[y,z]] = [[x,y],z] + [y,[x,z]], \tag{3}$$

$$[[x,y],z] = [x,[y,z]] + [[x,z],y]. \tag{4}$$

It is however easy to see that P satisfies the functional equation corresponding to (2) iff the polynomial P' defined by $P'(x,y) = P(y,x)$ satisfies (1). As far as equations (3) and (4) are concerned, one can show that the corresponding functional equations have no nonzero solution. The proof of this latter observation is given in Appendix B.

Note. The problem addressed in this paper was suggested by Jörg Tomaschek [11], who in turn was asked this question by Wolfgang Prager (University of Graz, Austria) while the latter was studying local analytic solutions of the Bokov functional equation that appears in theoretical physics (see [1, 12]).

2. Technicalities and proof of the Main Theorem

We use the following notation throughout this paper. For any integer $m \geq 1$ and any prime $p \geq 2$, we denote by $s_m(p)$ the set of positive integers expressible as sums of m powers of p, that is, integers n whose base p expansions $n = \sum_{i=0}^{k} n_i p^i$ (with $0 \leq n_i < p$ for $i = 0, \ldots, k$) satisfy $\sum_{i=0}^{k} n_i = m$. We also use the Kronecker delta symbol: $\delta_{i,j} = 1$, if $i = j$, and $\delta_{i,j} = 0$, if $i \neq j$. For any bivariate polynomial $P = P(x,y)$, we let $\deg(P)$ denote the degree of P, that is, the highest degree of the homogeneous terms of P in both variables. We also let $\deg_1(P)$ (resp. $\deg_2(P)$)

denote the degree of P in its first (resp. second) variable. For any nonnegative integer $k \leq \deg(P)$, unless otherwise stated we let P_k denote the homogeneous component of degree k of P, that is, the polynomial obtained from P by considering the terms of degree k only. For any monomial M of P, we let $[M]P(x,y)$ denote the coefficient of M in $P(x,y)$ (we let $[M]P(x,y) = 0$ if M is not a monomial of P), and similarly for polynomials in more than two indeterminates. Finally, we define the following trivariate polynomial

$$J_P(x,y,z) \;=\; P(P(x,y),z) + P(P(y,z),x) + P(P(z,x),y).$$

Recall that the definition of $\mathcal{R}$ enables us to identify the ring $\mathcal{R}[x_1,\ldots,x_n]$ of polynomials in n indeterminates over $\mathcal{R}$ with the ring of polynomial functions from $\mathcal{R}^n$ to $\mathcal{R}$. Recall also that if $\mathrm{char}(\mathcal{R}) = p > 0$, then p must be prime. In this case we have $(x+y)^p = x^p + y^p$ for any $x, y \in \mathcal{R}$ and this identity (often referred to as the freshman's dream) immediately extends to any sum of more than two terms.

In this paper we will often make use of the following theorem, established in 1878 by E. Lucas [7–9]. For a more recent reference, see [2].

Theorem 1 (Lucas' theorem)**.** *For any integers $n, m \geq 0$ and any prime $p \geq 2$, the following congruence relation holds:*

$$\binom{n}{m} \;\equiv\; \prod_{i=0}^{k} \binom{n_i}{m_i} \pmod{p},$$

where $n = \sum_{i=0}^{k} n_i p^i$ and $m = \sum_{i=0}^{k} m_i p^i$ are the base p expansions of n and m, respectively. This uses the convention that $\binom{a}{b} = 0$ for any integers a, b such that $0 \leq a < b$.

Corollary 2. *For any integer $n > 1$ and any prime p, the following two conditions are equivalent.*

(i) $n \in s_1(p)$.
(ii) *p divides $\binom{n}{m}$ for any integer m such that $0 < m < n$.*

Moreover, if $\mathrm{char}(\mathcal{R})$ is a prime p, then any of these conditions holds iff $(x+y)^n = x^n + y^n$ for any $x, y \in \mathcal{R}$.

Proof. (i) ⇒ (ii). This implication immediately follows from Lucas' theorem.

(ii) ⇒ (i). We prove this implication by contradiction. Suppose $n \notin s_1(p)$. Let $n = \sum_{i=0}^{k} n_i p^i$ be the base p expansion of n, let $j \in \{0,\ldots,k\}$ such that $n_j \neq 0$, and let $m = n - p^j$. Then we have $0 < m < n$ and by Lucas' theorem we also have $\binom{n}{m} \equiv n_j \pmod{p}$. This means that p does not divide $\binom{n}{m}$, which is a contradiction. The second part of the corollary is straightforward. □

Corollary 3. *Let $n > 1$ be an integer and let p be a prime.*

(a) *If $n = n_1 + n_2 \in s_2(p)$ for some $n_1, n_2 \in s_1(p)$ (with n_1, n_2 distinct if $p = 2$), then*
   - *p divides $\binom{n}{m}$ for any integer $m \in \{1,\ldots,n-1\} \smallsetminus \{n_1, n_2\}$.*
   - $\binom{n}{n_1} \equiv \binom{n}{n_2} \equiv (1 + \delta_{n_1,n_2}) \pmod{p}$.

(b) *If p divides $\binom{n}{m}\binom{m}{\ell}$ for any integers ℓ, m such that $0 < \ell < m < n$, then $n \in s_1(p) \cup s_2(p)$.*

Proof. Assertion (a) is a straightforward consequence of Lucas' theorem. To show that assertion (b) holds, we first proceed as in the proof of the implication (ii) ⇒ (i)

of Corollary 2. Suppose $n \notin s_1(p) \cup s_2(p)$. Let $n = \sum_{i=0}^{k} n_i p^i$ be the base p expansion of n, let $j \in \{0, \ldots, k\}$ such that $n_j \neq 0$, and let $m = n - p^j$. Then we have $0 < m < n$ and $\binom{n}{m} \not\equiv 0 \pmod{p}$. Since $n \notin s_2(p)$ we must have $m \notin s_1(p)$ and we conclude the proof by applying Corollary 2. □

We now prove the Main Theorem. Let $P\colon \mathcal{R}^2 \to \mathcal{R}$ be a polynomial function satisfying Jacobi's identity (1), that is, such that $J_P = 0$.

Suppose first that $\deg_2(P) = 0$, that is, $P(x, y) = P(x)$. Using Jacobi's identity, we obtain that $P(P(x))$ is a constant, and hence P is a constant C satisfying $3C = 0$. Therefore, C can be any constant if $\mathrm{char}(\mathcal{R}) = 3$, and $C = 0$, otherwise. Thus, we shall henceforth assume that $\deg_2(P) \geq 1$.

Proposition 4. *If $P\colon \mathcal{R}^2 \to \mathcal{R}$ is a polynomial function satisfying $J_P = 0$ and $\deg_2(P) \geq 1$, then $\deg_1(P) \leq 1$.*

We prove Proposition 4 by contradiction. Thus we suppose that $\deg_1(P) = d \geq 2$.

Claim 1. We have $\deg_2(P) = \deg(P) = d$. Moreover, the polynomial function P is of the form

$$P(x, y) = \sum_{k=0}^{d} \sum_{j=0}^{k} c_{k,j}\, x^j y^{k-j} \tag{5}$$

with $c_{d,d}\, c_{d,0} \neq 0$, $c_{d,d}^d + c_{d,0}^d = 0$, and

$$P_d(x, y)^d = c_{d,d}^d (x^{d^2} - y^{d^2}). \tag{6}$$

Proof of Claim 1. In this proof we use the notation $[x^k]_x J_P(x, y, z)$ to denote the coefficient of x^k in the expansion of J_P in powers of x.

Set $d_2 = \deg_2(P) \geq 1$. Then there exist polynomial functions $R_j\colon \mathcal{R} \to \mathcal{R}$ ($j = 0, \ldots, d$) and $S_k\colon \mathcal{R} \to \mathcal{R}$ ($k = 0, \ldots, d_2$), with $R_d \neq 0$ and $S_{d_2} \neq 0$, such that

$$P(x, y) = \sum_{j=0}^{d} x^j R_j(y) = \sum_{k=0}^{d_2} y^k S_k(x).$$

We then have

$$J_P(x, y, z) = \sum_{j=0}^{d} \Big(\sum_{k=0}^{d} x^k R_k(y) \Big)^j R_j(z) + \sum_{k=0}^{d_2} x^k S_k(P(y, z)) + \sum_{j=0}^{d} \Big(\sum_{k=0}^{d_2} x^k S_k(z) \Big)^j R_j(y).$$

Now, if $d > d_2$, then

$$[x^{d^2}]_x J_P(x, y, z) = R_d(y)^d\, R_d(z)$$

from which we derive $R_d = 0$, a contradiction. Similarly, if $d < d_2$, then

$$[x^{d\, d_2}]_x J_P(x, y, z) = S_{d_2}(z)^d\, R_d(y)$$

and hence we obtain $R_d = 0$ or $S_{d_2} = 0$, again a contradiction. Thus we have proved that $d = d_2$. It then follows that

$$[x^{d^2}]_x J_P(x, y, z) = R_d(y) \big(R_d(y)^{d-1} R_d(z) + S_d(z)^d \big)$$

and hence

$$R_d(y)^{d-1} R_d(z) + S_d(z)^d = 0. \tag{7}$$

Since $d \geq 2$, from identity (7) it follows that both R_d and S_d are nonzero constant polynomial functions. Thus the polynomial function P is of the form

$$P(x,y) \;=\; \sum_{j=0}^{d}\sum_{k=0}^{d} p_{j,k}\, x^j y^k,$$

with $p_{d,0}\, p_{0,d} \neq 0$ and $p_{d,k} = p_{j,d} = 0$ for $j,k = 1,\ldots,d$. Identity (7) also implies $p_{d,0}^d + p_{0,d}^d = 0$.

Now, let $r = \deg(P) \geq d$ and let M be an arbitrary monomial of J_P of degree rd in (x,y) and degree 0 in z (e.g., $M = x^i y^{rd-i}$ for some $i \in \{0,\ldots,rd\}$). We then have

$$[M]\, P(P(x,y),z) \;=\; [M] \sum_{j=0}^{d} p_{j,0}\, P(x,y)^j \;=\; [M]\, p_{d,0}\, P_r(x,y)^d$$

and

$$\begin{aligned}[M]\, P(P(y,z),x) \;&=\; [M] \sum_{j=0}^{d}\sum_{k=0}^{d} p_{j,k}\, P(y,0)^j x^k \\ &=\; [M]\Big(p_{d,0} P(y,0)^d + p_{0,d}\, x^d + \sum_{j=0}^{d-1}\sum_{k=0}^{d-1} p_{j,k}\, P(y,0)^j x^k\Big) \;=\; [M]\, \delta_{r,d}\, p_{d,0}^{d+1}\, y^{d^2}\end{aligned}$$

Indeed, for $j,k = 0,\ldots,d-1$, $P(y,0)^j x^k$ is of degree $jd+k \leq (d-1)d+(d-1) < d^2 \leq rd$.

We show similarly that

$$[M]\, P(P(z,x),y) \;=\; [M] \sum_{j=0}^{d}\sum_{k=0}^{d} p_{j,k}\, P(0,x)^j y^k \;=\; [M]\, \delta_{r,d}\, p_{d,0}\, p_{0,d}^d\, x^{d^2}.$$

Let us now show by contradiction that $\deg(P) = d$. Suppose that $r > d$. By combining the latter three identities with $J_P = 0$ we immediately obtain $0 = [M]\, J_P(x,y,z) = [M]\, p_{d,0}\, P_r(x,y)^d$, a contradiction. We then have $\deg(P) = d$. Using the same three identities for $r = d$, we obtain

$$P_d(x,y)^d + p_{d,0}^d\, y^{d^2} + p_{0,d}^d\, x^{d^2} = 0.$$

Finally, since $\deg(P) = d$, the polynomial function P must be of the form (5), with $c_{d,d} = p_{d,0}$ and $c_{d,0} = p_{0,d}$. Therefore the identities $c_{d,d}\, c_{d,0} \neq 0$, $c_{d,d}^d + c_{d,0}^d = 0$, and (6) hold. □

We now show that $\mathrm{char}(\mathcal{R})$ must be a prime number. This shows that a contradiction is already reached if $\mathrm{char}(\mathcal{R}) = 0$, which then proves Proposition 4 in this case.

Claim 2. The characteristic of $\mathcal{R}$ is a prime p and we have $d \in s_1(p)$. Moreover, we have $P_d(x,y) = c_{d,d}(x^d - y^d)$ and $(x+y)^d = x^d + y^d$ for any $x, y \in \mathcal{R}$.

Proof of Claim 2. By Claim 1 we have $\deg(P) = d$ and $[y^d]P(x,y) = c_{d,0} \neq 0$. Then we have

$$P_d(x,y) \;=\; c_{d,d}\, x^d + \sum_{j=0}^{r} c_{d,j}\, x^j y^{d-j} \tag{8}$$

for some integer $0 \leq r \leq d-1$, with $c_{d,r} \neq 0$. Equation (6) then becomes

$$c_{d,d}^d\, y^{d^2} + \sum_{k=0}^{d-1} \binom{d}{k} (c_{d,d}\, x^d)^k \Big(\sum_{j=0}^{r} c_{d,j}\, x^j y^{d-j}\Big)^{d-k} \;=\; 0. \tag{9}$$

Clearly, the literal part of the monomial of highest degree in x in the left-hand side of (9) is $x^{d(d-1)+r}y^{d-r}$. Indeed, it corresponds to the values $k = d-1$ and $j = r$ in the sums and therefore has the coefficient $d\,c_{d,d}^{d-1}c_{d,r}$. Since $c_{d,d}\,c_{d,r} \neq 0$, we must have $d1 = 0$ (here the symbol 1 denotes the identity of $\mathcal{R}$). If follows that the characteristic of $\mathcal{R}$ should be a prime $p \geq 2$ that divides d.

We now show by contradiction that $d \in s_1(p)$. Suppose that $d \notin s_1(p)$. Then by Corollary 2 we can let m be the greatest $k \in \{1,\dots,d-1\}$ such that $\binom{d}{k} \not\equiv 0 \pmod p$. Equation (9) then reduces to

$$c_{d,d}^{d}\,y^{d^2} + \sum_{k=0}^{m}\binom{d}{k}(c_{d,d}\,x^d)^k\Big(\sum_{j=0}^{r}c_{d,j}\,x^j y^{d-j}\Big)^{d-k} \;=\; 0. \tag{10}$$

The literal part of the monomial of highest degree in x in the left-hand side of (10) is $x^{md+r(d-m)}\,y^{(d-r)(d-m)}$. It corresponds to the values $k = m$ and $j = r$ and therefore has the coefficient $\binom{d}{m}c_{d,d}^{m}\,c_{d,r}^{d-m} \neq 0$, which leads to a contradiction. Therefore $d \in s_1(p)$ and hence by Corollary 2 we have $(x+y)^d = x^d + y^d$ for any $x, y \in \mathcal{R}$.

Now, by Claim 1 we have $(c_{d,d} + c_{d,0})^d = c_{d,d}^d + c_{d,0}^d = 0$ and hence $c_{d,d} + c_{d,0} = 0$. By Corollary 2 the identity (9) then reduces to

$$c_{d,d}^{d}\,y^{d^2} + \sum_{j=0}^{r}c_{d,j}^{d}\,x^{dj}y^{d(d-j)} \;=\; 0\,,$$

which implies $r = 0$. Using (8) we finally obtain $P_d(x,y) = c_{d,d}(x^d - y^d)$. □

Remark. From now on we will often make an implicit use of Fermat's little theorem: if $m \in s_1(p)$ then $a^m \equiv a \pmod p$ for every integer a.

We will now show (through Claims 3–6) that for every integer k such that $1 < k \leq d$ the polynomial function P_k is of one of the following three forms.

- **Type 0**: $P_k = 0$.
- **Type 1**: $P_k \neq 0$, $k \in s_1(p)$, and
$$P_k(x,y) \;=\; c_{k,k}(x^k - y^k).$$
- **Type 2**: $P_k \neq 0$, $k = k_1 + k_2 \in s_2(p)$, with $k_1 \geq k_2$ and $k_1, k_2 \in s_1(p)$, and
$$P_k(x,y) \;=\; c_{k,k}\,x^k + \frac{c_{k,k_1}}{1+\delta_{k_1,k_2}}\,(x^{k_1}y^{k_2} + x^{k_2}y^{k_1}) + c_{k,0}\,y^k.$$
Note: This latter form simply means that $c_{k,j} = 0$ whenever $j \notin \{k, k_1, k_2, 0\}$ and that $c_{k,k_1} = c_{k,k_2}$.

For every real $r \geq 0$ and every $m \in \{0,1,2\}$ we let

$$\mathcal{S}_{m,r} \;=\; \{k \text{ integer} \mid r < k \leq d \text{ and } P_k \text{ is of type } m\}.$$

It is clear that the sets $\mathcal{S}_{0,r}$, $\mathcal{S}_{1,r}$, $\mathcal{S}_{2,r}$ are pairwise disjoint. Moreover, if $r \leq r' \leq d$, then we have $\mathcal{S}_{m,r} \supseteq \mathcal{S}_{m,r'} \supseteq \mathcal{S}_{m,d} = \varnothing$.

By Claim 2 we have $d = \sup \mathcal{S}_{1,1}$. Regarding $\mathcal{S}_{2,1}$ we have two cases to consider.

- If $\mathcal{S}_{2,1} = \varnothing$, then we set $r_0 = 1$.
- If $\mathcal{S}_{2,1} \neq \varnothing$, then we set $q = q_1 + q_2 = \sup \mathcal{S}_{2,1}$, with $q_1 \geq q_2$ and $q_1, q_2 \in s_1(p)$. We also set $r_0 = q_1 + \frac{q_2 q}{d}$. We then have $1 \leq q_1 < r_0 < q < d$. Note that r_0 is an integer iff d divides $q_2 q = q_2^2(1 + q_1/q_2)$. But p does not divide $(1 + q_1/q_2)$ since $q_1/q_2 \in s_1(p)$. Hence r_0 is an integer iff d divides q_2^2, or equivalently, iff $d \leq q_2^2$. In this case we also have $d \leq q_1 q_2$ and hence d divides $q_1 q_2$.

Note that if $\mathcal{S}_{2,r} \neq \varnothing$ for some $r \geq 1$, then clearly $\mathcal{S}_{2,1} \neq \varnothing$ and $r < q$.

Remark. In all the equations that we will now consider, some expressions are associated with polynomial functions P_k for which $k \in \mathcal{S}_{2,1}$ (e.g., expressions involving q, q_1, and q_2). The proofs corresponding to those equations show that these expressions are to be ignored when $\mathcal{S}_{2,1} = \varnothing$.

For every real $r \geq 1$ we set

$$\alpha_r \;=\; \sum_{\substack{k\in\mathcal{S}_{1,r}\setminus\{d\}\\ \ell\in\mathcal{S}_{1,r},\, k\ell=rd}} c_{k,k}\, c_{\ell,\ell}^{k}\,,$$

$$\beta_r \;=\; \sum_{k\in\mathcal{S}_{2,r}} \sum_{\substack{a,b\in\mathcal{S}_{1,r}\\ a,b>q,\, ak_1+bk_2=rd}} c_{k,k}\, c_{a,a}^{k_1}\, c_{b,b}^{k_2}\,, \qquad \gamma_r \;=\; c_{r,r}\, c_{d,d}^{r} + \beta_r.$$

If r is an integer, then we easily see that $\alpha_r = 0$ if $r \notin s_1(p)$, and $\beta_r = 0$ if $r \notin s_1(p) \cup s_2(p)$. If $r = r_0$ is not an integer, then $rd = q_1 d + q_1 q_2 + q_2^2 \in s_3(p)$ and hence $\alpha_r = \beta_r = 0$. Since $c_{r,r}$ is to be ignored in this case, we also have $\gamma_r = 0$.

The proofs of the following two claims (Claims 3 and 4) are rather technical. For this reason we relegate them to Appendix A.

Claim 3. Let $r \in \{\lceil r_0\rceil, \ldots, d-1\}$ be such that $\{r+1, \ldots, d\} \subseteq \bigcup_{m=0}^{2} \mathcal{S}_{m,r}$. If i, u are integers such that $1 \leq i < u < r$, then

$$(-1)^{u-i}\binom{u}{i} c_{r,u} c_{d,d}^{u} + \delta_{r,r_0}\delta_{u,\frac{qq_2}{d}}\, \chi_{\{\frac{q_1q_2}{d},\frac{q_2^2}{d}\}}(i)\, c_{q,q_1}^{q_2+1} \;=\; 0. \tag{11}$$

Here, $\chi_{\{j,k\}}(i) = \max\{\delta_{i,j}, \delta_{i,k}\}$.

Claim 4. Let $r \in \{\lceil r_0\rceil, \ldots, d-1\} \cup \{r_0\}$ be such that $\{\lfloor r\rfloor + 1, \ldots, d\} \subseteq \bigcup_{m=0}^{2} \mathcal{S}_{m,r}$. Then the following two conditions hold.

- If either r, u are integers such that $1 \leq u < r$, or $r = r_0$ is not an integer and $u = \frac{q_2 q}{d}$, then

$$\begin{aligned} &c_{d,d}\, c_{r,u}^{d} + (-1)^{r-u}\binom{r}{u}\gamma_r \\ &\qquad + \delta_{r,r_0}(1+\delta_{q_1,q_2}) c_{q,q}\, [x^{du} y^{d(r-u)}](P_d(x,y)^{q_1} P_q(x,y)^{q_2}) \;=\; 0, \end{aligned} \tag{12}$$

  where the first two summands are to be ignored when $r = r_0$ is not an integer.
- If r is an integer, then

$$\begin{aligned} &c_{d,d}(c_{r,r}^{d} + c_{r,0}^{d}) + (1+(-1)^r)\gamma_r \\ &\qquad + \delta_{r,r_0}(1+\delta_{q_1,q_2}) c_{q,q_1} c_{d,d}^{q_1}(c_{q,q} - c_{q,0})^{q_2} - \delta_{r,1} c_{d,d} \;=\; 0. \end{aligned} \tag{13}$$

Claim 5. We have $\{\lfloor r_0\rfloor + 1, \ldots, d\} \subseteq \bigcup_{m=0}^{2} \mathcal{S}_{m,1}$.

Proof of Claim 5. We prove by decreasing induction that any integer $k \in \{\lfloor r_0\rfloor + 1, \ldots, d\}$ is in $\bigcup_{m=0}^{2} \mathcal{S}_{m,1}$. This is true for $k = d$ since $d \in \mathcal{S}_{1,1}$. Suppose that the result holds for $k = r+1, \ldots, d$ for some integer r such that $r_0 < r < d$ and let us show that it holds for $k = r$. There are three mutually exclusive cases to consider.

- If $r \notin s_1(p) \cup s_2(p)$, then $\beta_r = 0$ and by Corollary 3(b) there exists integers i_0, u_0 satisfying $1 \leq i_0 < u_0 < r$ such that $\binom{r}{u_0}\binom{u_0}{i_0} \not\equiv 0 \pmod{p}$. Using (11) with $i = i_0$ and $u = u_0$ we immediately obtain $c_{r,u_0} = 0$. Then, using (12) with $u = u_0$ we obtain $\gamma_r = 0$, which implies $c_{r,r} = 0$ (since $\beta_r = 0$). Using

again (12) we obtain that $c_{r,u} = 0$ for every integer u such that $1 \le u < r$. Finally, by (13) we obtain $c_{r,0} = 0$ and hence $P_r = 0$, that is, $r \in \mathcal{S}_{0,1}$.

- If $r \in s_1(p)$, then by Corollary 2 we have $\binom{r}{u} \equiv 0 \pmod p$ for every integer u such that $1 \le u < r$. Using (12) we then obtain $c_{r,u} = 0$ for every integer u such that $1 \le u < r$. In (13) we have $(-1)^r \equiv -1 \pmod p$ and hence $0 = c_{r,r}^d + c_{r,0}^d = (c_{r,r} + c_{r,0})^d$. Therefore P_r is of type 0 or 1, that is, $r \in \mathcal{S}_{0,1} \cup \mathcal{S}_{1,1}$.
- If $r = r_1 + r_2 \in s_2(p)$, with $r_1 \ge r_2$ and $r_1, r_2 \in s_1(p)$, then by Corollary 3(a) we have $\binom{r}{u} \equiv 0 \pmod p$ for every integer $u \in \{1, \dots, r-1\} \setminus \{r_1, r_2\}$. Using (12) we obtain $c_{r,u} = 0$ for every integer $u \in \{1, \dots, r-1\} \setminus \{r_1, r_2\}$. Now, if $r_1 \ne r_2$, then using (12) for $u = r_1$ and then for $u = r_2$, we obtain $c_{r,r_1} = c_{r,r_2}$. Therefore, P_r is of type 0 or 2, that is, $r \in \mathcal{S}_{0,1} \cup \mathcal{S}_{2,1}$.

This completes the proof of the claim. □

We now show that $\{2, \dots, d\} \subseteq \mathcal{S}_{0,1} \cup \mathcal{S}_{1,1}$ (i.e., P_k is of type 0 or 1 for $k = 2, \dots, d$).

Claim 6. We have $r_0 = 1$ (i.e., $\mathcal{S}_{2,1} = \varnothing$).

Proof of Claim 6. We proceed by contradiction. Suppose that $r_0 > 1$, that is, $\mathcal{S}_{2,1} \ne \varnothing$ and $r_0 = q_1 + \frac{q_2 q}{d}$. Using (12) with $r = r_0$ and $u = u_0 = \frac{q_2 q}{d}$, we obtain

$$c_{d,d}\, c_{r_0,u_0}^d + (-1)^{q_1} \binom{r_0}{u_0} \gamma_{r_0} - (1 + \delta_{q_1,q_2})\, c_{d,d}^{q_1}\, c_{q,q}^{q_2+1} = 0. \tag{14}$$

Setting $r = q$ and $u = q_1$ in (12) and (13), we obtain

$$c_{d,d}\, c_{q,q_1}^d = (1 + \delta_{q_1,q_2})\, c_{q,q}\, c_{d,d}^q \tag{15}$$

and

$$c_{d,d}(c_{q,q}^d + c_{q,0}^d) + 2c_{q,q}\, c_{d,d}^q = 0. \tag{16}$$

Indeed, $\delta_{q,r_0} = 0$ and since $\mathcal{S}_{2,q} = \varnothing$ we have $\beta_q = 0$ and hence $\gamma_q = c_{q,q} c_{d,d}^q$. Moreover, by Corollary 3(a) we have $\binom{q}{q_1} \equiv (1 + \delta_{q_1,q_2}) \pmod p$.

Now we have two cases to consider.

- If r_0 is not an integer, then the first two summands of (14) are to be ignored and hence we immediately derive $c_{q,q} = 0$. Then from (15) and (16) we derive $c_{q,0} = c_{q,q_1} = 0$, that is, $P_q = 0$ (i.e., $q \in \mathcal{S}_{0,1}$), a contradiction.
- If r_0 is an integer (in which case d divides both $q_1 q_2$ and q_2^2), then using (11) with $r = r_0$, $u = u_0 = \frac{q_2 q}{d}$, and $i = \frac{q_1 q_2}{d}$ (we note that $\binom{u_0}{i} \equiv (1 + \delta_{q_1,q_2}) \pmod p$ by Corollary 3(a)) and then raising both sides of the resulting equation to the power d we obtain

$$c_{q,q_1}^{d(q_2+1)} = (1 + \delta_{q_1,q_2})\, c_{r_0,u_0}^d\, c_{d,d}^{du_0}. \tag{17}$$

Raising both sides of (15) to the power $(q_2 + 1)$ and then combining the resulting equation with (17) we obtain

$$c_{r_0,u_0}^d = (1 + \delta_{q_1,q_2})\, c_{d,d}^{q_1-1}\, c_{q,q}^{q_2+1}.$$

Substituting for c_{r_0,u_0}^d into (14) and observing by Lucas' theorem that $\binom{r_0}{u_0} \equiv 1 \pmod p$ we obtain $\gamma_{r_0} = 0$.

Now, using (11) with $r = r_0$, $u = u_0 = q_1 + \frac{q_1 q_2}{d}$, and $i = q_1$, we obtain $\binom{u_0}{q_1} c_{r_0,u_0} c_{d,d}^{u_0} = 0$, and therefore $c_{r_0,u_0} = 0$ (since $\binom{u_0}{q_1} \equiv 1 \pmod p$ by

Corollary 3(a)). Using (12) with the same $r = r_0$ and $u = u_0$, we then obtain

$$c_{q,q}\,[x^{q_1 d+q_1 q_2} y^{q_2^2}](P_d(x,y)^{q_1} P_q(x,y)^{q_2}) \;=\; 0,$$

that is, $c_{q,q}\, c_{q,q_1}^{q_2} c_{d,d}^{q_1} = 0$. Combining this latter equation with (15) and (16) we obtain $c_{q,q} = c_{q,0} = c_{q,q_1} = 0$, that is, $P_q = 0$, a contradiction.

This completes the proof of the claim. □

Proof of Proposition 4. On the one hand, using (13) with $r = r_0 = 1$ and the fact that $\mathcal{S}_{2,1} = \varnothing$ (i.e., q does not exist), we obtain

$$0 \;=\; c_{d,d}(c_{1,1}^d + c_{1,0}^d - 1^d) \;=\; c_{d,d}(c_{1,1} + c_{1,0} - 1)^d,$$

that is,

$$c_{1,1} + c_{1,0} \;=\; 1. \tag{18}$$

On the other hand, by Claims 5 and 6 for any $M \in \{x, y, z\}$ we have

$$\begin{aligned}
[M]P(P(x,y),z) \;&=\; [M]\Big(\sum_{k\in\mathcal{S}_{1,1}} P_k(P(x,y),z) + P_1(P(x,y),z) + P_0\Big) \\
&=\; [M]\Big(\sum_{k\in\mathcal{S}_{1,1}} c_{k,k}(P(x,y)^k - z^k) + c_{1,1}P(x,y) + c_{1,0}z + c_{0,0}\Big).
\end{aligned}$$

Clearly, the sum over $k \in \mathcal{S}_{1,1}$ above cannot contain monomials of degree 1. Therefore we have

$$[M]P(P(x,y),z) \;=\; [M](c_{1,1}P_1(x,y) + c_{1,0}z) \;=\; [M](c_{1,1}(c_{1,1}x + c_{1,0}y) + c_{1,0}z).$$

Since the identity $[x]J_P(x,y,z) = 0$ can be written as $\sum_{M\in\{x,y,z\}}[M]P(P(x,y),z) = 0$, we have

$$c_{1,1}(c_{1,1} + c_{1,0}) + c_{1,0} \;=\; 0. \tag{19}$$

Since the system (18)–(19) is inconsistent we immediately reach a contradiction. □

Proof of the Main Theorem. By Proposition 4, there exist two polynomial functions $R\colon\mathcal{R}\to\mathcal{R}$ and $S\colon\mathcal{R}\to\mathcal{R}$ such that

$$P(x,y) \;=\; x\,R(y) + S(y).$$

We then have

$$\begin{aligned}
J_P(x,y,z) \;=\;& x\,R(y)R(z) + S(y)R(z) + S(z) \\
&+ y\,R(z)R(x) + S(z)R(x) + S(x) \\
&+ z\,R(x)R(y) + S(x)R(y) + S(y).
\end{aligned}$$

Suppose that $\deg(R) = r > 1$ and set $A = [y^r]R(y)$. We can then readily see that

$$[x\,y^r z^r]J_P(x,y,z) \;=\; A^2.$$

We then have $A = 0$, a contradiction. Therefore $R(y) = A_1 y + A_0$ for some $A_1, A_0 \in \mathcal{R}$. Now, suppose that $\deg(S) = s > 1$ and set $B = [y^s]S(y)$. It is then easy to see that

$$[y^s]J_P(x,y,z) \;=\; (A_0 + 1)B \quad\text{and}\quad [y^s z]J_P(x,y,z) \;=\; A_1 B.$$

However, one can readily see that P cannot satisfy Jacobi's identity if $A_1 = 0$ and $A_0 = -1$. Thus we must have $B = 0$, again a contradiction.

Finally, the polynomial P must be of the form

$$P(x,y) \;=\; Axy + Bx + Cy + D$$

for some $A, B, C, D \in \mathcal{R}$ and we can immediately verify that this polynomial satisfies Jacobi's identity iff

$$3A^2 \;=\; 3D(B+1) \;=\; A(2B+C) \;=\; B^2 + BC + C + AD \;=\; 0.$$

The statement of the Main Theorem then follows straightforwardly. □

Appendix A. Proofs of Claims 3 and 4

Before providing the proofs of Claims 3 and 4, we first show that for any $r \geq r_0$ and any $k = k_1 + k_2 \in \mathcal{S}_{2,r}$, with $k_1 \geq k_2$ and $k_1, k_2 \in s_1(p)$, the following conditions hold.

(a) $k_1 = q_1$ and $k_2 \leq q_2$.
(b) $d(r-k_1) \geq qk_2$. The equality holds iff $r = r_0$ and $k = q$.
(c) $d(r-k_2) \geq qk_1$. The equality holds iff $r = r_0$, $k = q$, and $q_1 = q_2$.
(d) $ak_1 + bk_2 \leq rd$ for all $a \leq d$ and $b \leq q$. The equality holds iff $a = d$, $b = q$, $k_2 = q_2$, and $r = r_0$.
(e) $ak_1 + bk_2 \leq rd$ for all $a \leq q$ and $b \leq d$. The equality holds iff $a = q$, $b = d$, $k_2 = q_2$, $q_1 = q_2$, and $r = r_0$.

Proof. if $\mathcal{S}_{2,1} = \varnothing$, then $\mathcal{S}_{2,r} = \varnothing$ for every $r \geq r_0 = 1$ and then there is nothing to prove. We therefore assume that $\mathcal{S}_{2,1} \neq \varnothing$. We then have $r_0 = q_1 + q_2 q/d$ and $q_1 < r_0 \leq r < k \leq q$.

(a) We have $k_1 = q_1$. Indeed, if we had $k_1 > q_1$, then we would have $k > k_1 \geq pq_1 \geq 2q_1 \geq q_1 + q_2 = q$, a contradiction. If we had $k_1 < q_1$, then we would have $q_1 \geq pk_1 \geq 2k_1 \geq k_1 + k_2 = k$, a contradiction. Finally, $k \leq q$ implies $k_2 \leq q_2$.
(b) We have $d(r-k_1) - qk_2 \geq d(r_0 - q_1) - qq_2 = 0$.
(c) We have $d(r-k_2) - qk_1 \geq d(r_0 - q_2) - qq_1 = (q_1 - q_2)(d-q) \geq 0$.
(d) We have $ak_1 + bk_2 \leq dq_1 + qq_2 = r_0 d \leq rd$.
(e) We have $ak_1 + bk_2 \leq qq_1 + dq_2 \leq dq_1 + qq_2 = r_0 d \leq rd$, where the second inequality is equivalent to $(q_1 - q_2)(d-q) \geq 0$. □

Proof of Claim 3. We consider the identity $[M]J_P(x,y,z) = 0$ for $M = x^{di} y^{d(u-i)} z^{r-u}$. Since $di \geq d$ and $d(u-i) \geq d$, we have $[M]P(P(y,z),x) = 0$ and $[M]P(P(z,x),y) = 0$. Also, we have

$$\begin{aligned}[M]P(P(x,y),z) \;=\; & [M]\sum_{k\in\mathcal{S}_{1,r}} P_k(P(x,y),z) + [M]\sum_{k\in\mathcal{S}_{2,r}} P_k(P(x,y),z) \\ & + [M]P_r(P(x,y),z) + [M]\sum_{k<r} P_k(P(x,y),z).\end{aligned}$$

Let us compute the latter four summands separately.

- We clearly have

$$[M]\sum_{k\in\mathcal{S}_{1,r}} P_k(P(x,y),z) \;=\; [M]\sum_{k\in\mathcal{S}_{1,r}} c_{k,k}(P(x,y)^k - z^k) \;=\; 0.$$

- Assuming that $\mathcal{S}_{2,r} \neq \varnothing$ and setting $M' = x^{di}y^{d(u-i)}$, we obtain

$$\begin{aligned}
&[M]\sum_{k\in\mathcal{S}_{2,r}} P_k(P(x,y),z)\\
&= [M]\sum_{k\in\mathcal{S}_{2,r}} \frac{c_{k,k_1}}{1+\delta_{k_1,k_2}}\big(P_{du/k_1}(x,y)^{k_1}z^{k_2} + P_{du/k_2}(x,y)^{k_2}z^{k_1}\big)\\
&= [M']\sum_{k\in\mathcal{S}_{2,r}} \frac{c_{k,k_1}}{1+\delta_{k_1,k_2}}\big(P_{du/k_1}(x,y)^{k_1}\delta_{k_2,r-u} + P_{du/k_2}(x,y)^{k_2}\delta_{k_1,r-u}\big)\\
&= [M']\sum_{k\in\mathcal{S}_{2,r}} \frac{c_{k,k_1}}{1+\delta_{k_1,k_2}}\big(P_{d(r-k_2)/k_1}(x,y)^{k_1}\delta_{k_2,r-u} + P_{d(r-k_1)/k_2}(x,y)^{k_2}\delta_{k_1,r-u}\big).
\end{aligned}$$

If $d(r-k_2)/k_1 > q$, then $P_{d(r-k_2)/k_1}$ is of type 0 or 1, so it does not contain any product terms and hence M' cannot appear in $P_{d(r-k_2)/k_1}(x,y)^{k_1}$. We arrive at the same conclusion for $P_{d(r-k_1)/k_2}$. Using conditions (b) and (c) above, we then obtain

$$\begin{aligned}
&[M]\sum_{k\in\mathcal{S}_{2,r}} P_k(P(x,y),z)\\
&= [M']\frac{\delta_{r,r_0}\,c_{q,q_1}}{1+\delta_{q_1,q_2}}\big(\delta_{q_1,q_2}\,P_q(x,y)^{q_1}\delta_{q_2,r_0-u} + P_q(x,y)^{q_2}\delta_{q_1,r_0-u}\big)\\
&= [M']\,\delta_{r,r_0}\delta_{u,\frac{qq_2}{d}}\,c_{q,q_1}P_q(x,y)^{q_2}\\
&= [M']\,\delta_{r,r_0}\delta_{u,\frac{qq_2}{d}}\,\frac{c_{q,q_1}^{q_2+1}}{1+\delta_{q_1,q_2}}\big(x^{q_1q_2}y^{q_2^2} + x^{q_2^2}y^{q_1q_2}\big)\\
&= \delta_{r,r_0}\delta_{u,\frac{qq_2}{d}}\,\chi_{\{\frac{q_1q_2}{d},\frac{q_2^2}{d}\}}(i)\,c_{q,q_1}^{q_2+1}.
\end{aligned}$$

- Since M is of degree du in (x,y), we have

$$\begin{aligned}
[M]P_r(P(x,y),z) &= [M]\sum_{j=0}^{r} c_{r,j}\,P(x,y)^j z^{r-j} = [M]\,c_{r,u}\,P(x,y)^u z^{r-u}\\
&= [M]\,c_{r,u}\,c_{d,d}^u(x^d-y^d)^u z^{r-u} = (-1)^{u-i}\binom{u}{i}c_{r,u}c_{d,d}^u.
\end{aligned}$$

- Let us now compute $[M]\sum_{k<r}P_k(P(x,y),z)$. If $k < r-u$, the degree in z of $P_k(P(x,y),z)$ cannot reach $r-u$. If $r-u \le k < r$, we have

$$[M]P_k(P(x,y),z) = [M]\,c_{k,k-(r-u)}P(x,y)^{k-(r-u)}z^{r-u}.$$

This expression is 0 since the degree in (x,y) of $P(x,y)^{k-(r-u)}$ does not exceed $d(k-(r-u)) < du$.

This completes the proof of the claim. □

Proof of Claim 4. We first consider the identity $[M]J_P(x,y,z) = 0$ for the monomials $M = x^{du}y^{d(r-u)}$ with $0 \le u \le r$. These monomials are of degree rd in (x,y) and 0 in z. Thus we have

$$\begin{aligned}
[M]P(P(x,y),z) &= [M]\sum_{k\in\mathcal{S}_{1,r}} c_{k,k}P(x,y)^k + [M]\sum_{k\in\mathcal{S}_{2,r}} c_{k,k}P(x,y)^k\\
&\quad + [M]\,c_{r,r}P(x,y)^r + [M]\sum_{k<r} c_{k,k}P(x,y)^k.
\end{aligned}$$

Let us compute the latter four summands separately.

- We show that $[M]\sum_{k\in\mathcal{S}_{1,r}} c_{k,k}P(x,y)^k = [M](c_{d,d}P_r(x,y)^d + \alpha_r(x-y)^{rd})$. Since $k \in \mathcal{S}_{1,r}$ implies $k \in s_1(p)$, we have

$$[M]\sum_{k\in\mathcal{S}_{1,r}} c_{k,k}P(x,y)^k \;=\; [M]\sum_{k\in\mathcal{S}_{1,r}} c_{k,k}P_{\frac{rd}{k}}(x,y)^k.$$

  We then observe that if $d > k \in \mathcal{S}_{1,r}$ (hence $d \geq pk$) and $P_\ell \neq 0$, with $\ell = \frac{rd}{k}$, then necessarily $\ell \in \mathcal{S}_{1,r}$. Indeed, since $\ell > r$ we must have $\ell \in \mathcal{S}_{1,r} \cup \mathcal{S}_{2,r}$ by the hypotheses of the claim. If $r_0 = 1$, then $\mathcal{S}_{2,r} = \varnothing$ and hence $\ell \in \mathcal{S}_{1,r}$. If $r_0 > 1$, then we have $\ell = \frac{rd}{k} \geq pr \geq 2r_0 > 2q_1 \geq q$, and hence $\ell \in \mathcal{S}_{1,r}$ by definition of q.

  Therefore, we have

$$\begin{aligned}[M]\sum_{k\in\mathcal{S}_{1,r}\setminus\{d\}} c_{k,k}P(x,y)^k &= [M]\sum_{k\in\mathcal{S}_{1,r}\setminus\{d\}} c_{k,k}\sum_{\ell\in\mathcal{S}_{1,r},\,k\ell=rd} c^k_{\ell,\ell}(x-y)^{rd}\\ &= [M]\,\alpha_r(x-y)^{rd},\end{aligned}$$

  which immediately gives the stated identity.
- Assuming that $\mathcal{S}_{2,r} \neq \varnothing$, let us show that

$$[M]\sum_{k\in\mathcal{S}_{2,r}} c_{k,k}P(x,y)^k \;=\; [M]\big(\beta_r(x-y)^{rd}+\delta_{r,r_0}(1+\delta_{q_1,q_2})c_{q,q}(P_d(x,y)^{q_1}P_q(x,y)^{q_2})\big).$$

  Indeed, the left-hand side of this identity can be rewritten as

$$[M]\sum_{k\in\mathcal{S}_{2,r}}\sum_{a,b=0}^{d} c_{k,k}P_a(x,y)^{k_1}P_b(x,y)^{k_2}.$$

  Since $P_a(x,y)^{k_1}P_b(x,y)^{k_2}$ is a homogeneous polynomial function of degree $ak_1 + bk_2$, we can use conditions (d) and (e) above to analyze all the summands corresponding to $a \leq q$ or $b \leq q$. If $a > q$ and $b > q$ (hence $a > r$ and $b > r$ since $q > r$ when $\mathcal{S}_{2,r} \neq \varnothing$), then necessarily $a, b \in \mathcal{S}_{0,r} \cup \mathcal{S}_{1,r}$ and we obtain the stated identity.
- We have $[M]\,c_{r,r}P(x,y)^r = [M]\,c_{r,r}P_d(x,y)^r = [M]\,c_{r,r}c^r_{d,d}(x-y)^{rd}$.
- We have $[M]\sum_{k<r} c_{k,k}P(x,y)^k = 0$ since the degree of $P(x,y)^k$ is bounded by $kd < rd$.

Summing up, we obtain

$$\begin{aligned}[M]P(P(x,y),z) &= [M]\big(c_{d,d}P_r(x,y)^d + (\alpha_r+\gamma_r)(x-y)^{rd}\\ &\quad + \delta_{r,r_0}(1+\delta_{q_1,q_2})c_{q,q}(P_d(x,y)^{q_1}P_q(x,y)^{q_2})\big).\end{aligned} \tag{20}$$

If r, u are integers such that $1 \leq u < r$, then $M = x^{du}y^{d(r-u)}$ is a polynomial multiple of x^dy^d. Since no monomial in $P(P(y,z),x)$ and $P(P(z,x),y)$ is a polynomial multiple of x^dy^d we must have $[M]J_P(x,y,z) = [M]P(P(x,y),0)$. We then observe that if $\alpha_r \neq 0$, then $r \in s_1(p)$ and in this case we have $[M](x-y)^{rd} = 0$ and hence α_r can be ignored in (20). We then immediately obtain (12).

If $r = r_0$ is not an integer and $u = \frac{q_2q}{d}$, then $M = x^{q_2q}y^{q_1d}$ and $r < q$. We then have

$$[M]P(P(y,z),x) \;=\; [M]\sum_{k\leq q} P_k(P(y,z),x) + [M]\sum_{k>q} P_k(P(y,z),x),$$

where the first summand is clearly zero. The second summand is also zero since $k > q > r$ implies $k \in \mathcal{S}_{0,r} \cup \mathcal{S}_{1,r}$. We show similarly that $[M]P(P(z,x),y) = 0$.

Moreover, the summands involving P_r and $(\alpha_r + \gamma_r)$ are to be ignored in (20). We therefore obtain (12), in which the first two summands are to be ignored.

Let us now prove (13). We consider the monomial $M = x^{rd}$ and hence we have

$$[M]J_P(x,y,z) \;=\; [M]P(P(x,0),0) + [M]P(P(0,x),0) + [M]P(P(0,0),x).$$

The first summand is exactly the right-hand side of (20) when $u = r$, that is

$$c_{d,d}\, c_{r,r}^{d} + (\alpha_r + \gamma_r) + \delta_{r,r_0}(1 + \delta_{q_1,q_2})\, c_{q,q}\, c_{d,d}^{q_1}\, c_{q,q}^{q_2}.$$

Similarly, the second summand is the right-hand side of (20) when $u = 0$, that is

$$c_{d,d}\, c_{r,0}^{d} + (\alpha_r + \gamma_r)(-1)^r - \delta_{r,r_0}(1 + \delta_{q_1,q_2})\, c_{q,q}\, c_{d,d}^{q_1}\, c_{q,0}^{q_2}.$$

The third summand is simply equal to $\delta_{r,1}c_{d,0} = -\delta_{r,1}c_{d,d}$ since $d \in \mathcal{S}_{1,r}$. We then conclude the proof by observing that $(1 + (-1)^r)\,\alpha_r = 0$ since if $\alpha_r \neq 0$ then $r \in s_1(p)$. □

Appendix B. Case of equations (3) and (4)

The functional equations corresponding to (3) and (4) are respectively given by

$$P(P(x,y),z) + P(y,P(x,z)) - P(x,P(y,z)) \;=\; 0, \tag{21}$$

$$P(x,P(y,z)) + P(P(x,z),y) - P(P(x,y),z) \;=\; 0. \tag{22}$$

It is then easy to see that P satisfies (22) iff the polynomial P' defined by $P'(x,y) = P(y,x)$ satisfies (21).

Now, let $P{:}\mathcal{R}^2 \to \mathcal{R}$ be a polynomial function satisfying (21) and let us show that necessarily $P = 0$.

Suppose that $\deg_2(P) \geq 1$ and let us prove by contradiction that $\deg_1(P) \leq 1$. Suppose that $\deg_1(P) = d \geq 2$. By using the notation of the proof of Claim 1, we see that (21) can be rewritten as

$$\sum_{j=0}^{d}\Big(\sum_{k=0}^{d} x^k R_k(y)\Big)^j R_j(z) + \sum_{k=0}^{d_2}\Big(\sum_{j=0}^{d} x^j R_j(z)\Big)^k S_k(y) - \sum_{j=0}^{d} x^j R_j(P(y,z)) \;=\; 0.$$

If $d > d_2$ (resp. $d < d_2$), then by equating the coefficients of x^{d^2} (resp. x^{dd_2}) in the expansion in powers of x of each side of the latter equation, we obtain a contradiction. Therefore, we have $d = d_2$. By equating the coefficients of x^{d^2} we then obtain

$$R_d(y)^d + R_d(z)^{d-1} S_d(y) \;=\; 0,$$

which shows that both R_d and S_d are nonzero constant polynomial functions.

Now, by identifying x and y in (21), we obtain

$$P(P(x,x),z) \;=\; 0, \tag{23}$$

or equivalently,

$$\sum_{k=0}^{d} z^k S_k(P(x,x)) \;=\; 0.$$

By equating the coefficients of z^d in the latter equation we obtain $S_d = 0$, a contradiction. Therefore we have $\deg_1(P) \leq 1$ and hence we have

$$P(x,y) \;=\; x\,R_1(y) + R_0(y).$$

Substituting in (23), we then obtain

$$(x\,R_1(x) + R_0(x))\,R_1(z) + R_0(z) \;=\; 0.$$

If $x\,R_1(x) + R_0(x)$ is nonconstant, then $R_1 = 0$ and then also $R_0 = 0$. Otherwise, if $x\,R_1(x) + R_0(x)$ is a constant C, then $R_0(z) = -C\,R_1(z)$ and hence $C = x\,R_1(x) + R_0(x) = x\,R_1(x) - C\,R_1(x)$, from which we derive $R_1 = 0$ and then also $R_0 = 0$. Finally, $P = 0$, which contradicts the assumption that $\deg_2(P) \geq 1$. Hence we have $\deg_2(P) = 0$, in which case we immediately see that $P = 0$.

Acknowledgments

This research is partly supported by the internal research project R-AGR-0500 of the University of Luxembourg. The authors thank Michel Rigo of the University of Liège for pointing out Lucas' theorem. They also thank Jörg Tomaschek of Deloitte Austria for bringing this problem to their attention.

References

[1] O. G. Bokov. A model of Lie fields and multiple-time retarded Greens functions of an electromagnetic field in dielectric media. *Nauchn. Tr. Novosib. Gos. Pedagog. Inst.* 86:3–9, 1973.
[2] N. Fine. Binomial coefficients modulo a prime. *Amer. Math. Monthly* 54:589–592, 1947.
[3] H. Fripertinger. On n-associative formal power series. *Aeq. Math.* 90(2):449–467, 2016.
[4] R. Gilmore. *Lie groups, Lie algebras, and some of their applications*. John Wiley and Sons, New York, 1974.
[5] B. C. Hall. *Lie groups, Lie algebras, and representations. An elementary introduction*. Springer-Verlag, New York, 2003.
[6] N. Jacobson. *Lie algebras*. Courier Dover Publications, 1979.
[7] E. Lucas. Théorie des fonctions numériques simplement périodiques. *Am. J. Math.* 1(2): 184–196, 1878.
[8] E. Lucas. Théorie des fonctions numériques simplement périodiques. *Am. J. Math.* 1(3): 197–240, 1878.
[9] E. Lucas. Théorie des fonctions numériques simplement périodiques. *Am. J. Math.* 1(4): 289–321, 1878.
[10] J.-L. Marichal and P. Mathonet. A description of n-ary semigroups polynomial-derived from integral domains. *Semigroup Forum* 83:241–249, 2011
[11] Jörg Tomaschek. Deloitte Austria. Private communication.
[12] A. V. Yagzhev. A functional equation from theoretical physics. *Funct. Anal. Appl.* 16(1):38–44, 1982.

Mathematics Research Unit, University of Luxembourg, Maison du Nombre, 6, avenue de la Fonte, L-4364 Esch-sur-Alzette, Luxembourg
E-mail address: jean-luc.marichal[at]uni.lu

University of Liège, Department of Mathematics, Allée de la Découverte 12 - B37, B-4000 Liège, Belgium
E-mail address: p.mathonet[at]ulg.ac.be