JOURNAL OF ALGEBRA 7, 100-125 (1967)

Rings Nonembeddable in Fields with Multiplicative Semigroups Embeddable in Groups*

ABRAHAM A. KLEIN

Institute of Mathematics, The Hebrew University, Jerusalem, Israel

Communicated by P. M. Cohn[1]

Received September 12, 1966

1. INTRODUCTION

Necessary and sufficient conditions for a semigroup to be embeddable in a group were given by Mal'cev [*5*]. Similar conditions for a ring to be embeddable in a field are not yet known. Mal'cev [*4*] has constructed (noncommutative) integral domains that cannot be embedded in a (skew) field. His examples are based on the fact that the multiplicative semigroup (of nonzero elements) cannot be embedded in a group and this clearly implies that the rings are not embeddable in fields.

The aim of this paper is to construct integral domains that cannot be embedded in a field, but whose multiplicative semigroups are embeddable in groups, and this solves the problem stated in [*1*], p. 277.

If an integral domain R can be embedded in a field, then necessarily the ring of $n \times n$ matrices R_n satisfies certain properties of matrices over a field. In particular if $C \in R_n$ is a nilpotent matrix, then $C^n = 0$. To obtain our example, we construct an integral domain R with a nilpotent matrix $C \in R_n$ such that $C^n \neq 0$, and then we show the multiplicative semigroup of R can be embedded in a group. This is obtained by embedding R in an integral domain $\mathscr{R}$, whose multiplicative semigroup satisfies Doss' condition [*2*] for a semigroup to be embeddable in a group.

---

* This is a part of the author's Ph.D. thesis prepared at the Hebrew University of Jerusalem under the supervision of Professor S. A. Amitsur.

[1] *Editor's note:* The problem discussed here (first raised by Mal'cev in the 1930's) was solved by three people this summer (1966), all working independently and obtaining different proofs. They are the author, L. A. Bokut', and A. J. Bowtell. Mr. Bowtell's solution (which is comparatively brief) was also submitted to this Journal and appears as the paper immediately following.

2. Summary and Notations

The following is a list of the notations used and an outline of the construction of the integral domain R.

(1) $F = \{0, 1\}$—the field of two elements.

(2) $F[x] = F[x_1, \ldots, x_n]$—the free noncommutative polynomial ring (with 1) generated by a set of indeterminates $\{x_1, \ldots, x_n\}$, $n \geqslant 2$, over F.

(3) $F[[x]]$—the ring of formal power series of $F[x]$, namely, infinite sums of homogeneous polynomials of distinct degrees.

(4) P—the subring of $F[x]$ generated by all monomials $x_i x_j$ and 1; clearly P contains those polynomials all of whose homogeneous components of odd degree are 0.
$\mathscr{P}$—the subring of $F[[x]]$ of those series all of whose homogeneous components of odd degree are 0.

(5) $A = (x_i x_j)$—the matrix in P_n, whose entry in the ith row and jth column is $x_i x_j$.

(6) k—a fixed integer $\geqslant 1$ and z_{ij}—the (i, j) entry of the matrix A^{k+1}; thus, $A^{k+1} = (z_{ij})$.

(7) T—the ideal in P generated by $\{z_{ij} \mid 1 \leqslant i, j \leqslant n\}$ and $R = P/T$.
$\mathscr{T}$—the ideal in $\mathscr{P}$ generated by $\{z_{ij} \mid 1 \leqslant i, j \leqslant n\}$ and $\mathscr{R} = \mathscr{P}/\mathscr{T}$.

The integral domain we construct is obtained by taking a fixed $k \geqslant n$ and proving that R is an integral domain. The matrix $C = (x_i x_j + T) \in R_n$ and $C^{k+1} = (z_{ij} + T) = 0$, hence C is nilpotent. But since the polynomials of T are of degree $\geqslant 2k + 2$ and the entries of A^n are of degree $2n < 2k + 2$, it follows that $C^n \neq 0$. Thus, we have:

Theorem 1. *If $k \geqslant n$, then R is not embeddable in a field.*

After proving that R is an integral domain, we show that for $n \geqslant 3$ (independent of k) the multiplicative semigroup $R^* = R - \{0\}$ is embeddable in a group in the following way:
The injection $F[x] \to F[[x]]$ induces the injections $P \to \mathscr{P}$ and $T \to \mathscr{T}$, and it is proved that $R = P/T$ can be embedded in $\mathscr{R} = \mathscr{P}/\mathscr{T}$. Next it is shown that $\mathscr{R}$ is also an integral domain and hence $\mathscr{R}^* = \mathscr{R} - \{0\}$ is a semigroup which satisfies the cancellation laws. It is then proved that $\mathscr{R}^*$ satisfies the following condition: if two elements of $\mathscr{R}^*$ have a common left-multiple, then one of them is a right-divisor of the other. By a result of Doss [*2*], this condition is sufficient for a semigroup with cancellation laws to be embeddable in a group. Hence $\mathscr{R}^*$ is embeddable in a group and R^* which is embeddable in $\mathscr{R}^*$ is also embeddable in a group.

The most difficult part of this paper is the proof that R is an integral domain. This is carried out by choosing unique representatives in every class of P/T, and giving a method for passing from a polynomial $p \in P$ to the representative of $p + T$ by a finite number of steps. In particular the representative of T is 0. It is then proved that the representative of the residue class of the product of two nonzero representatives is not 0, which means that P/T is an integral domain.

3. The Ideal T and the Representatives of R

In this section we shall define the representatives of $R = P/T$ called henceforth "special polynomials" or just "special".

We begin by calculating the polynomials z_{ij} which generate T. By definition z_{ij} are the entries of the matrix A^{k+1}, where $A = (x_i\, x_j)$. It is readily seen that $A = (x_i)^* (x_j)$ where $(x_j) = (x_1, \ldots, x_n)$ and $(x_i)^*$ is its transpose. Then $A^{k+1} = [(x_i)^* (x_j)]^{k+1} = (x_i)^* [(x_j)(x_i)^*]^k (x_j)$. Let $y = x_1{}^2 + \cdots + x_n{}^2$, then $(x_j)(x_i)^* = x_1{}^2 + \cdots + x_n{}^2 = y$. Hence we have

$$A^{k+1} = (x_i)^* y^k (x_j) = (x_i y^k x_j)$$

and consequently:

$$z_{ij} = x_i y^k x_j = x_i \Big(\sum_{1 \leqslant l_1, \ldots, l_k \leqslant n} x_{l_1}^2 \cdots x_{l_k}^2 \Big) x_j , \qquad 1 \leqslant i, j \leqslant n. \tag{1}$$

In view of the fact that F is the field of two elements, every polynomial $p \in F[x]$ can be written in an unique way as a sum of distinct monomials (the unity 1 is identified with the empty monomial). The set of monomials which appear in this sum will be denoted by $\{p\}$. For $p = 0$ we obtain the empty set.

We recall that P is the subring of $F[x]$ of those polynomials which are sums of monomials of even degree.

Definition. A monomial of P will be called "special" if it is not of the form $m x_i x_n^{2k} x_j m'$, where m, m' are monomials of even degree (belong to P) and $1 \leqslant i, j \leqslant n$. A polynomial $p \in P$ will be called "special" if the set of monomials $\{p\}$ contains only special monomials.

Let S denote the set of all special polynomials and the following are some properties of this set.

Lemma 2. *S is an additive group and if $\{p\} \subseteq \{q\}$, $q \in S$, then $p \in S$.*

Proof. Every sum of special monomials is a special polynomial. Thus a sum (which is also a difference since the characteristic is 2) of two special polynomials is special. Clearly the zero-polynomial is special, hence S is an additive group. If $\{p\} \subseteq \{q\}$, then p is a subsum of q, and since $q \in S$, p is also a sum of special monomials and it is therefore special.

LEMMA 3. (a) *If* $p_1 \in F[x]$ *and* $x_i p_1 \in S$ *for some* i, *then* $x_j p_1 \in S$ *for all* j.

(b) *If*

$$p = \sum_{i=1}^{n} x_i p_i \in S$$

then all $x_i p_i \in S$.

(c) *If*

$$p = \sum_{j=1}^{n} x_1 x_j p_j \in S,$$

then all $p_j \in S$.

Proof. (a) $x_i p_1 \in S$ means that no monomial of $\{x_i p_1\}$ is of the form $m x_{i'} x_n^{2k} x_{j'} m' (m, m' \in P)$. Hence if such a monomial appears in $x_j p_1$ then x_j must be either the first indeterminate in m, or $m = 1$ and $x_j = x_{i'}$, but then clearly $x_i p_1$ will also have such a monomial with x_i replacing x_j in the beginning, a contradiction.

(b) For $i \neq j$ $\{x_i p_i\} \cap \{x_j p_j\} = \phi$, hence $\{x_i p_i\} \subseteq \{p\}$, $1 \leqslant i \leqslant n$. As $p \in S$ we obtain by lemma 2 that $x_i p_i \in S$.

(c) As in (b) we obtain $x_1 x_j p_j \in S$ for $1 \leqslant j \leqslant n$. Hence, if m is a monomial of $\{p_j\}$, its degree is even and from the definition it is clear that m is also special, thus $p_j \in S$.

Now, we proceed to prove some similar properties for the ideal T.

We introduce here the notation $p^{(\alpha)}$ for the homogeneous component of degree α of a polynomial p.

LEMMA 4. *T is a homogeneous ideal.*

PROOF. Let $p \in T$, then p can be written as a finite combination of multiples of the generators z_{ij}:

$$p = \sum_{\mu} p_\mu z_{i_\mu j_\mu} p'_\mu, \qquad \text{where} \qquad p_\mu, p'_\mu \in P. \tag{2}$$

The $z_{i_\mu j_\mu}$ are homogeneous of degree $2k + 2$, hence the homogeneous component of degree α of p is

$$p^{(\alpha)} = \sum_{\mu,\beta,\gamma} p_\mu^{(\beta)} z_{i_\mu j_\mu} p_\mu'^{(\gamma)}, \qquad \text{where} \qquad \beta + \gamma + 2k + 2 = \alpha$$

and β, γ are even; thus $p^{(\alpha)} \in T$.

REMARK. The same proof for $\mathscr{P}$ and $\mathscr{T}$ (defined in 2) yields that $\mathscr{T}$ is a homogeneous ideal in $\mathscr{P}$ and the homogeneous polynomials of $\mathscr{T}$ belong to T.

LEMMA 5. (a) *If $p_1 \in F[x]$ and $x_i p_1 \in T$ for some i, then $x_j p_1 \in T$ for all j.*
(b) *If*

$$p = \sum_{i=1}^{n} x_i p_i \in T,$$

then all $x_i p_i \in T$.

Proof. Let $p \in T$ be written in the form (2) and replace the polynomials p_μ by the sums of their monomials. Thus, p is of the form $p = \Sigma m_\lambda z_{i_\lambda j_\lambda} p'_\lambda$, where the m_λ's are monomials.

(a) Since $x_i p_1 \in T$ we can write $x_i p_1 = \Sigma m_\lambda z_{i_\lambda j_\lambda} p'_\lambda$ and assume that if $m_\lambda \neq 1$ then $m_\lambda = x_i m''_\lambda$, and if $m_\lambda = 1$ then $z_{i_\lambda j_\lambda} = x_{i_\lambda} y^k x_{j_\lambda} = x_i y^k x_{j_\lambda} = z_{i j_\lambda}$. Hence,

$$x_i p_1 = \Sigma' z_{i j_\lambda} p'_\lambda + \Sigma'' x_i m''_\lambda z_{i_\lambda j_\lambda} p'_\lambda,$$

where in Σ' we take all the summands of Σ with $m_\lambda = 1$. Thus,

$$x_j p_1 = \Sigma' z_{j j_\lambda} p'_\lambda + \Sigma'' x_j m''_\lambda z_{i_\lambda j_\lambda} p'_\lambda$$

and hence $x_j p_1 \in T$.

(b) We write

$$p = \Sigma m_\lambda z_{i_\lambda j_\lambda} p'_\lambda = \sum_{i=1}^{n} (\Sigma_{(i)} m_\lambda z_{i_\lambda j_\lambda} p'_\lambda),$$

where in $\Sigma_{(i)}$ we take the summands of Σ with $m_\lambda = 1$ and $i_\lambda = i$, or $m_\lambda = x_i m''_\lambda$. Since $\{\Sigma_{(i)}\} \cap \{\Sigma_{(j)}\} = \emptyset$ and $\{x_i p_i\} \cap \{x_j p_j\} = \emptyset$ we obtain $x_i p_i = \Sigma_{(i)} m_\lambda z_{i_\lambda j_\lambda} p'_\lambda \in T$ for all i.

Our next aim is to prove that each residue class of P/T has one and only one special polynomial.

4. EXISTENCE

Let $m \in P$ be a monomial and denote by $\tau(m)$ the number of possible ways of writing m in the form $m_1(x_i x_n^{2k} x_j)\, m_2$ with m_1, m_2 monomials of even degrees $\geqslant 0$. If m is special, then $\tau(m) = 0$. For $m = x_{i_1} \cdots x_{i_{2\alpha}}$ with $2\alpha \geqslant 2k + 2$, we have

$$\tau(m) = \tau(x_{i_1} \cdots x_{i_{2k+2}}) + \tau(x_{i_3} \cdots x_{i_{2k+4}}) + \cdots + \tau(x_{i_{2\alpha-2k-1}} \cdots x_{i_{2\alpha}}) \tag{3}$$

and each term of this sum is either 0 or 1.

Denote by m' a monomial which is obtained from m by replacing some of the x's by x_n, then clearly $\tau(m') \geqslant \tau(m)$. In particular, if we replace all the x's by x_n we get $\tau(x_n^{2\alpha}) \geqslant \tau(m)$. Hence the maximum of $\tau(m)$ for all monomials of degree 2α is $\tau(x_n^{2\alpha}) = r$ ($r = 0$ if $\alpha \leqslant k$ and $r = \alpha - k$ if $\alpha > k$).

Let $p \in P$ be homogeneous of degree $2\alpha > 2k$. Denote by λ_ν the number of monomials $m \in \{p\}$ with $\tau(m) = \nu$, $1 \leqslant \nu \leqslant r$. We introduce the notion of the *height* of p as the non-negative integral vector: $\sigma = (\lambda_r, \lambda_{r-1}, \ldots, \lambda_1)$. Clearly, p is special if and only if its height is $(0, 0, \ldots, 0)$.

For a fixed α consider the lexicographic ordering of integral vectors; namely, let $\sigma' = (\lambda'_r, \lambda'_{r-1}, \ldots, \lambda'_1)$; then $\sigma' < \sigma$ if there is a ν such that $\lambda'_\nu < \lambda_\nu$. But $\lambda'_\mu = \lambda_\mu$ for $\mu > \nu$. The set of heights for a given α is a well-ordered set under lexicographic ordering (e.g., [*3*], Section 39).

LEMMA 6. *If m, m' are monomials of P, $1 \leqslant l_1, \ldots, l_k \leqslant n$, and at least one of the l's is $\neq n$ then:*

$$\tau(mx_ix_{l_1}^2 \cdots x_{l_k}^2 x_j m') < \tau(mx_ix_n^{2k}x_jm').$$

Proof. By replacing some x's in a monomial m by x_n, its τ does not decrease. Hence each summand in the representation (3) of $\tau(mx_ix_{l_1}^2 \cdots x_{l_k}^2 x_j m')$ is $\leqslant$ than the corresponding summand of $\tau(mx_ix_n^{2k}x_jm')$ where the inequality is strict for at least one summand, since $(l_1, \ldots, l_k) \neq (n, \ldots, n)$ and so $\tau(x_ix_{l_1}^2 \cdots x_{l_k}^2 x_j) = 0$, $\tau(x_ix_n^{2k}x_j) = 1$. Thus, we obtain

$$\tau(mx_ix_{l_1}^2 \cdots x_{l_k}^2 x_j m') < \tau(mx_ix_n^{2k}x_jm').$$

LEMMA 7. *If $p \in P$ is homogeneous and $mx_ix_n^{2k}x_jm'$ ($m, m' \in P$) is one of its monomials, then the height of $p' = p + mz_{ij}m'$ is lower than the height of p.*

Proof. Let $\sigma = (\lambda_r, \ldots, \lambda_1)$ be the height of p and let $\tau(mx_ix_n^{2k}x_jm') = \nu$. Since $mx_ix_n^{2k}x_jm' \in \{p\}$, by definition of σ we have $\lambda_\nu \geqslant 1$. We assert that the height of p' is $\sigma' = (\lambda_r, \ldots, \lambda_{\nu+1}, \lambda_\nu - 1, \lambda'_{\nu-1}, \ldots, \lambda'_1)$, which is by definition lower that σ. Indeed, by (1) we have

$$mz_{ij}m' = m\Big(\sum_{1 \leqslant l_1, \ldots, l_k \leqslant n} x_ix_{l_1}^2 \cdots x_{l_k}^2 x_j\Big)m'.$$

Thus, $p' = p + mz_{ij}m'$ does not contain $mx_ix_n^{2k}x_jm'$ as this monomial appears in p and in $mz_{ij}m'$ and we deal with a ring of characteristic 2. Hence, if a monomial of p' does not belong to p, it is of the form $mx_ix_{l_1}^2 \cdots x_{l_k}^2x_jm'$ where $(l_1, \ldots, l_k) \neq (n, n, \ldots, n)$, and by the previous lemma we have

$$\tau(mx_ix_{l_1}^2 \cdots x_{l_k}^2x_jm') < \tau(mx_ix_n^{2k}x_jm') = \nu.$$

It follows therefore that, if the height of p' is $\sigma' = (\lambda_r', \ldots, \lambda_{\nu+1}', \lambda_\nu', \lambda_{\nu-1}', \ldots, \lambda_1')$, then $\lambda_r' = \lambda_r, \ldots, \lambda_{\nu+1}' = \lambda_{\nu+1}$ and $\lambda_\nu' = \lambda_\nu - 1$, which proves our assertion.

LEMMA 8. *Let p be homogeneous of degree $2\alpha > 2k$ and define $q_0 = p$; if q_μ contains a nonspecial monomial $m_\mu x_{i_\mu}x_n^{2k}x_{j_\mu}m_\mu'$, set $q_{\mu+1} = q_\mu + m_\mu z_{i_\mu j_\mu}m_\mu'$ for $\mu = 0, 1, \ldots$. Then the chain $q_0, q_1, \ldots$ is finite and its last element is special.*

Proof. Let σ_μ be the height of q_μ. By the previous lemma we have: $\sigma_0 > \sigma_1 > \cdots$ and by the well-ordering of the set of heights (of homogeneous polynomials of degree 2α), this chain must terminate at σ_l, say. Hence q_l does not contain a monomial of the form $mx_ix_n^{2k}x_jm'(m, m' \in P)$ and it is therefore special.

COROLLARY. *If $p \in P$ is homogeneous, then $p = p_0 + p_1$ with $p_0 \in S$, $p_1 \in T$ and $\deg p_0 = \deg p$ if $p \notin T$, $\deg p_1 = \deg p$ if $p \notin S$.*

Indeed, if $\deg p \leqslant 2k$, then p is special and we take $p_0 = p$ and $p_1 = 0$. If $\deg p > 2k$, then in the previous lemma we have obtained

$$q_l = p + \sum_{\mu=0}^{l-1} m_\mu z_{i_\mu j_\mu} m_\mu'.$$

Hence we take $p_0 = q_l$ which is special and $p_1 = \sum_{\mu=0}^{l-1} m_\mu z_{i_\mu j_\mu} m_\mu'$ which belongs to T. If $p \notin T$ then $p_0 \neq 0$ and $\deg p_0 = \deg p$. Similarly, if $p \notin S$ then $p_1 \neq 0$ and $\deg p_1 = \deg p$.

Since every $p \in P$ can be expressed as a sum of its homogeneous components and S, T are additive groups, it follows immediately that

THEOREM 9. *Every residue class of P/T contains a special polynomial.*

Using the above corollary we prove here one additional lemma which will be used in the next section.

LEMMA 10. *If $r \in T$, then r can be written as a sum of the form $\Sigma mz_{ij}m'$, where $m, m' \in P$ are monomials and all first terms m are special.*

Proof. We shall prove that $r = \Sigma pz_{ij}p'$ where $p \in S$, $p' \in P$ and our result will follow by replacing p and p' by the sum of their monomials.

Since $r \in T$ we can write $r = \Sigma p z_{ij} p'$, where $p, p' \in P$ and clearly we may assume that they are homogeneous. If all the polynomials p in this sum are special the result is proved. Assume that this is not the case and look at the polynomials $p \notin S$ of maximal degree ν, say. Write $p = p_0 + p_1$ with $p_0 \in S$, $p_1 \in T$ and if $p_1 \neq 0$ then $\deg p_1 = \deg p = \nu$. Note that since $p_1 = \Sigma p_{1\mu} z_{i_\mu j_\mu} p'_{1\mu}$ and all summands are of the same degree, then $\deg p_{1\mu} < \deg p_1$. Now, we write

$$r = \Sigma p z_{ij} p' = \Sigma' p z_{ij} p' + \Sigma'' p z_{ij} p',$$

where in Σ' we take all summands of Σ with $p \notin S$ and $\deg p = \nu$, and for those p we have: $p = p_0 + \Sigma p_{1\mu} z_{i_\mu j_\mu} p'_{1\mu}$. Hence,

$$r = \Sigma' p_0 z_{ij} p' + \Sigma' \Sigma p_{1\mu} z_{i_\mu j_\mu} (p'_{1\mu} z_{ij} p') + \Sigma'' p z_{ij} p'.$$

This can be written in the form $\Sigma q z_{ij} q'$ with q equal to p_0, $p_{1\mu}$ or p which appears in Σ''. Now $p_0 \in S$, $\deg p_{1\mu} < \deg p = \nu$, and for those $p \notin S$ which appear in Σ'', $\deg p < \nu$ (by the maximality of ν). Hence we have $r = \Sigma q z_{ij} q'$ with $q, q' \in P$ and the degree of a $q \notin S$ is $< \nu$. Repeating the above process several times, the maximal degree ν lowers in each step and the final representation of r is the required for obtaining our lemma.

5. Uniqueness

In this section we prove the following theorem.

THEOREM 11. *Every residue class of P/T contains only one special polynomial.*

Proof. The theorem will follow if we prove that $S \cap T = \{0\}$. Indeed let p_1 and p_2 be any two special polynomials of the same residue class. Then $p_1 - p_2 \in T$ and since S is an additive group we have $p_1 - p_2 \in S$. Thus, if $S \cap T = \{0\}$ it follows $p_1 - p_2 = 0$ and hence $p_1 = p_2$.

Assume that $S \cap T \neq \{0\}$. Let $q \neq 0$ be a non-zero element of (c1) *minimal degree* in $S \cap T$, such that it has a representation $q = \Sigma m z_{ij} m'$ as in Lemma 10 (m, $m' \in P$ are monomials and $m \in S$) with a (c2) *minimal number of summands d*, say. Among the representations of q with d summands we choose one with (c3) $\Sigma \deg m$ *maximal*, and let us write it in the form

$$= \sum_{=1}^{d} m_\lambda z_{i_\lambda j_\lambda} m'_\lambda . \tag{4}$$

We shall obtain a contradiction by proving in six steps (A)-(F) that (4) cannot exist.

For convenience we set

$$q_\lambda = m_\lambda z_{i_\lambda j_\lambda} m'_\lambda, \qquad \lambda = 1,..., d \tag{5}$$

and so (4) has the form: $q = \sum_{\lambda=1}^{d} q_\lambda$. Note that $q_\lambda \neq q_{\lambda'}$ for $\lambda \neq \lambda'$ since the characteristic is 2.

(A) *There exists x_i such that $q_\lambda = x_i q'_\lambda$ for all q_λ of (4) and without loss of generality we may assume $x_i = x_1$.*

Proof. We write, as in the proof of Lemma 5 (b),

$$q = \sum_{\lambda=1}^{d} q_\lambda = \sum_{j=1}^{n} \Sigma_{(j)} q_\lambda ,$$

where in $\Sigma_{(j)}$ we take the summands q_λ of the form $x_j q'_\lambda$. Thus $q = \sum_{j=1}^{n} x_j \Sigma_{(j)} q'_\lambda$, and by Lemma 3(b) we have $q_{(j)} = \Sigma_{(j)} q_\lambda = x_j \Sigma_{(j)} q'_\lambda \in S$ and, as all $q_\lambda \in T$ by (5), we have $q_{(j)} \in S \cap T$. By the minimality of d, $q_{(j)} \neq 0$ only for one j.

If $q = q_{(i)}$ and $i \neq 1$, let $q' = x_1 \sum_{\lambda=1}^{d} q'_\lambda$. Clearly q' satisfies all conditions (c1)-(c3) with the same d [by Lemma 3(a)].

We assume henceforth: $q_\lambda = x_1 q'_\lambda$ for $\lambda = 1,..., d$.

(B) *There exists a m_λ in (4) equals to 1 and so $q_\lambda = z_{1 j_\lambda} m'_\lambda$.*

Proof. Assume the assertion (B) is not true. Then $\deg m_\lambda > 0$ for $1 \leqslant \lambda \leqslant d$ and since $\deg m_\lambda$ is even we have: $m_\lambda = x_1 x_j m''_\lambda$. Thus, $q = \sum_{j=1}^{n} \Sigma_{(j)} q_\lambda$, where $\Sigma_{(j)} q_\lambda$ is the sum of the q_λ's with $m_\lambda = x_1 x_j m''_\lambda$. By Lemma 3(c) we have $\Sigma_{(j)} q_\lambda \in S$ and since all $q_\lambda \in T$, $\Sigma_{(j)} q_\lambda \in S \cap T$ for $1 \leqslant j \leqslant n$. By the minimality of d we must have $q = \Sigma_{(j)} q_\lambda$ for some j and therefore $q = x_1 x_j \sum_{\lambda=1}^{d} m''_\lambda z_{i_\lambda j_\lambda} m'_\lambda$. But $q' = \Sigma m''_\lambda z_{i_\lambda j_\lambda} m'_\lambda \in T$ and it is clear that $0 \neq q' \in S$, hence we have $0 \neq q' \in S \cap T$. But $\deg q' < \deg q$ and this contradicts the minimality of the degree of q which proves that some $m_\lambda = 1$.

The second part of (B) follows immediately. Indeed, some $q_\lambda = z_{i_\lambda j_\lambda} m'_\lambda$ and $i_\lambda = 1$ since $q_\lambda = x_1 q'_\lambda$ by assumption.

(C) *The sum (4) does not contain n summands q_{λ_l}, $1 \leqslant l \leqslant n$, such that $q_{\lambda_l} = m_0 z_{il}(x_l x_j m'_0)$ where m_0, m'_0, i, j are the same for all q_{λ_l} and such that $\deg m_0 \leqslant 2k - 2(m_{\lambda_l} = m_0$, $i_{\lambda_l} = i$, $j_{\lambda_l} = l$, $m_{\lambda_l} = x_l x_j m'_0)$.*

Proof. If this is not the case we shall construct a representation of q with the same number of summands and for which $\Sigma \deg m > \sum_{\lambda=1}^{d} \deg m_\lambda$ which will contradict the assumption of maximality of $\sum_{\lambda=1}^{d} \deg m_\lambda$.

Thus, let $q_{\lambda_l} = m_0 z_{il}(x_l x_j m_0')$, $1 \leqslant l \leqslant n$, and $\deg m_0 \leqslant 2k - 2$ We recall that the matrix $A = (x_i x_j)$ and $A^{k+1} = (z_{ij})$. Since $A^{k+1}A = A^{k+2} = AA^{k+1}$ we obtain for the (i, j)-entry of A^{k+2}

$$\sum_{l=1}^{n} z_{il} x_l x_j = \sum_{l=1}^{n} x_i x_l z_{lj}$$

Using this equation we obtain

$$\sum_{l=1}^{n} q_{\lambda_l} = \sum_{l=1}^{n} m_0 z_{il} x_l x_j m_0' = m_0 \left(\sum_{l=1}^{n} z_{il} x_l x_j\right) m_0'$$

$$= m_0 \left(\sum_{l=1}^{n} x_i x_l z_{lj}\right) m_0' = \sum_{l=1}^{n} (m_0 x_i x_l)\, z_{lj} m_0' .$$

Since $\deg m_0 \leqslant 2k - 2$ we have $\deg (m_0 x_i x_l) \leqslant 2k$ and hence $m_0 x_i x_l$ is special. Replacing the partial sum $\sum_{l=1}^{n} q_{\lambda_l}$ of (4) by the equal sum $\sum_{l=1}^{n} (m_0 x_i x_l)\, z_{lj} m_0'$ we obtain a new representation of the same q (of the form $\Sigma m z_{ij} m'$, m, $m' \in P$ monomials, $m \in S$) with the same number of summands (since d is minimal). For this representation we have:

$$\sum \deg m = \sum_{\lambda \neq \lambda_l} \deg m_\lambda + \sum_{l=1}^{n} \deg m_{\lambda_l} + 2n > \sum_{\lambda=1}^{d} \deg m_\lambda .$$

The next two steps deal with common monomials of two and of three summands of (4).

(D) *Let* q_α, q_β *be summands of (4) such that* $\{q_\alpha\} \cap \{q_\beta\} \neq \emptyset$. *If* $\deg m_\beta = \deg m_\alpha$ *then* $q_\alpha = q_\beta$ *and if* $0 < \deg m_\beta - \deg m_\alpha = 2\nu \leqslant 2k$ *then*

$$\{q_\alpha\} \cap \{q_\beta\} = \{m_\beta x_{i_\beta} y^{k-\nu} x_{j_\alpha} m_\alpha'\}. \tag{6}$$

Proof. By (1) and (5) we have

$$q_\alpha = m_\alpha x_{i_\alpha} y^k x_{j_\alpha} m_\alpha'; \qquad q_\beta = m_\beta x_{i_\beta} y^k x_{j_\beta} m_\beta' . \tag{7}$$

By assumption $\{q_\alpha\} \cap \{q_\beta\} \neq \emptyset$, thus let $m \in \{q_\alpha\} \cap \{q_\beta\}$. Since $m \in \{q_\alpha\}$ we have $m = m_\alpha x_{i_\alpha} x_{s_1}^2 \cdots x_{s_k}^2 x_{j_\alpha} m_\alpha'$ for some $1 \leqslant s_1, \ldots, s_k \leqslant n$, and also $m \in \{q_\beta\}$, hence $m = m_\beta x_{i_\beta} x_{t_k}^2 \cdots x_{t_1}^2 x_{j_\beta} m_\beta'$ for some $1 \leqslant t_1, \ldots, t_k \leqslant n$. (Note that for convenience we have written the indices in the two representations of m in reverse order.) Thus

$$m = m_\alpha x_{i_\alpha} x_{s_1}^2 \cdots x_{s_k}^2 x_{j_\alpha} m_\alpha' = m_\beta x_{i_\beta} x_{t_k}^2 \cdots x_{t_1}^2 x_{j_\beta} m_\beta' . \tag{8}$$

If $\deg m_\alpha = \deg m_\beta$, we deduce

$$m_\alpha = m_\beta, \quad x_{i_\alpha} = x_{i_\beta}, \quad x_{s_1}^2 \cdots x_{s_k}^2 = x_{t_k}^2 \cdots x_{t_1}^2, \quad x_{j_\alpha} = x_{j_\beta}, \quad m'_\alpha = m'_\beta .$$

Hence by (7) $q_\alpha = q_\beta$ and the first assertion of (D) is proved.

Next, let $\deg m_\beta = \deg m_\alpha + 2\nu$ and $0 < \nu \leqslant k$. In this case it follows from (8) that $m_\beta = m_\alpha x_{i_\alpha} x_{s_1}^2 \cdots x_{s_{\nu-1}}^2 x_{s_\nu}$ and therefore

$$x_{s_\nu} x_{s_{\nu+1}}^2 \cdots x_{s_k}^2 x_{j_\alpha} m'_\alpha = x_{i_\beta} x_{t_k}^2 \cdots x_{t_{\nu+1}}^2 x_{t_\nu}^2 \cdots x_{t_1}^2 x_{j_\beta} m'_\beta;$$

from this we obtain

$$x_{s_\nu} = x_{i_\beta}, \quad x_{s_{\nu+1}}^2 \cdots x_{s_k}^2 = x_{t_k}^2 \cdots x_{t_{\nu+1}}^2, \quad x_{j_\alpha} = x_{t_\nu},$$

$$m'_\alpha = x_{t_\nu} x_{t_{\nu-1}}^2 \cdots x_{t_1}^2 x_{j_\beta} m'_\beta .$$

Thus

$$m_\alpha x_{i_\alpha} x_{s_1}^2 \cdots x_{s_{\nu-1}}^2 x_{i_\beta} = m_\beta; \qquad m'_\alpha = x_{j_\alpha} x_{t_{\nu-1}}^2 \cdots x_{t_1}^2 x_{j_\beta} m'_\beta \tag{9}$$

and for the first representation of m in (8) we get

$$m = m_\beta x_{i_\beta} (x_{s_{\nu+1}}^2 \cdots x_{s_k}^2)\, x_{j_\alpha} m'_\alpha .$$

Since $x_{s_{\nu+1}}^2 \cdots x_{s_k}^2$ is a monomial of $y^{k-\nu}$, we deduce that $m \in \{m_\beta x_{i_\beta} y^{k-\nu} x_{j_\alpha} m'_\alpha\}$. This relation is true for any monomial of $\{q_\alpha\} \cap \{q_\beta\}$, and hence

$$\{q_\alpha\} \cap \{q_\beta\} \subseteq \{m_\beta x_{i_\beta} y^{k-\nu} x_{j_\alpha} m'_\alpha\}.$$

To prove the inclusion in the other direction, let $x_{r_1}^2 \cdots x_{r_{k-\nu}}^2$ be any monomial of $y^{k-\nu}$. Since (9) still holds we have

$$\begin{aligned} m_\beta x_{i_\beta} x_{r_1}^2 \cdots x_{r_{k-\nu}}^2 x_{j_\alpha} m'_\alpha &= (m_\alpha x_{i_\alpha} x_{s_1}^2 \cdots x_{s_{\nu-1}}^2 x_{i_\beta})\, x_{i_\beta} x_{r_1}^2 \cdots x_{r_{k-\nu}}^2 x_{j_\alpha} m'_\alpha \\ &= m_\alpha x_{i_\alpha} (x_{s_1}^2 \cdots x_{s_{\nu-1}}^2 x_{i_\beta}^2 x_{r_1}^2 \cdots x_{r_{k-\nu}}^2)\, x_{j_\alpha} m'_\alpha \end{aligned}$$

and this monomial belongs to $\{q_\alpha\}$ by (7). Similarly, it belongs to $\{q_\beta\}$ since

$$m_\beta x_{i_\beta} x_{r_1}^2 \cdots x_{r_{k-\nu}}^2 x_{j_\alpha} m'_\alpha = m_\beta x_{i_\beta} (x_{r_1}^2 \cdots x_{r_{k-\nu}}^2 x_{j_\alpha}^2 x_{t_{\nu-1}}^2 \cdots x_{t_1}^2)\, x_{j_\beta} m'_\beta .$$

Hence $m_\beta x_{i_\beta} (x_{r_1}^2 \cdots x_{r_{k-\nu}}^2)\, x_{j_\alpha} m'_\alpha \in \{q_\alpha\} \cap \{q_\beta\}$ for all $r_1, \ldots, r_{k-\nu}$ and this completes the proof of (D).

(E) *If* $q_{\lambda_1}, q_{\lambda_2}, q_{\lambda_3}$ *appear in (4),* $\{q_{\lambda_i}\} \cap \{q_{\lambda_j}\} \neq \emptyset$ *for all* i, j *and* $\deg m_{\lambda_1} < \deg m_{\lambda_2} < \deg m_{\lambda_3} \leqslant 2k$, *then*

$$\{q_{\lambda_1}\} \cap \{q_{\lambda_3}\} \subseteq \{q_{\lambda_2}\} \cap \{q_{\lambda_3}\}.$$

Proof. Let $\deg m_{\lambda_2} - \deg m_{\lambda_1} = 2\nu$ and $\deg m_{\lambda_3} - \deg m_{\lambda_2} = 2\mu$. Then $\deg m_{\lambda_3} - \deg m_{\lambda_1} = 2(\mu + \nu) \leqslant \deg m_{\lambda_3} \leqslant 2k$. Since $\{q_{\lambda_1}\} \cap \{q_{\lambda_2}\} \neq \emptyset$, we obtain by (9) with $\alpha = \lambda_1$, $\beta = \lambda_2$,

$$m'_{\lambda_1} = x_{j_{\lambda_1}} x^2_{t_{\nu-1}} \cdots x^2_{t_1} x_{j_{\lambda_2}} m'_{\lambda_2}. \tag{10}$$

From $\{q_{\lambda_2}\} \cap \{q_{\lambda_3}\} \neq \emptyset$ and $\deg m_{\lambda_3} - \deg m_{\lambda_2} = 2\mu$ we obtain, by (6) with $\alpha = \lambda_2$, $\beta = \lambda_3$ and μ replacing ν,

$$\{q_{\lambda_2}\} \cap \{q_{\lambda_3}\} = \{m_{\lambda_3} x_{i_{\lambda_3}} y^{k-\mu} x_{j_{\lambda_2}} m'_{\lambda_2}\}. \tag{11}$$

Since $2(\mu + \nu) \leqslant 2k$ and $\{q_{\lambda_1}\} \cap \{q_{\lambda_3}\} \neq \emptyset$, then by (6) with $\alpha = \lambda_1$, $\beta = \lambda_3$ and $\mu + \nu$ replacing ν,

$$\{q_{\lambda_1}\} \cap \{q_{\lambda_3}\} = \{m_{\lambda_3} x_{i_{\lambda_3}} y^{k-(\mu+\nu)} x_{j_{\lambda_1}} m'_{\lambda_1}\}$$

and by (10) this is equal to $\{m_{\lambda_3} x_{i_{\lambda_3}} y^{k-(\mu+\nu)} x^2_{j_{\lambda_1}} x^2_{t_{\nu-1}} \cdots x^2_{t_1} x_{j_{\lambda_2}} m'_{\lambda_2}\}$. But $x^2_{j_{\lambda_1}} x^2_{t_{\nu-1}} \cdots x^2_{t_1}$ is a monomial of y^ν and therefore

$$\{q_{\lambda_1}\} \cap \{q_{\lambda_3}\} \subseteq \{m_{\lambda_3} x_{i_{\lambda_3}} y^{k-(\mu+\nu)} y^\nu x_{j_{\lambda_2}} m'_{\lambda_2}\} = \{m_{\lambda_3} x_{i_{\lambda_3}} y^{k-\mu} x_{j_{\lambda_2}} m'_{\lambda_2}\}$$
$$= \{q_{\lambda_2}\} \cap \{q_{\lambda_3}\},$$

by (11), which proves (E).

Our final step is.

(F) *The sum (4) does not contain a summand* q_τ *for which*

$$m_\tau x_{i_\tau} = x_1 x_n^{2(k+1-\nu)}, \qquad 0 \leqslant \nu \leqslant k+1.$$

Proof. The result is true for $\nu = 0$ since otherwise we have $m_\tau = x_1 x_n^{2k+1} = x_1(x_n^{2k})\, x_n$ which is not special, but by assumption on the representation (4) all m_λ are special.

Assume the assertion (F) is true for all μ with $0 \leqslant \mu \leqslant \nu < k+1$ and we proceed to prove it for $\nu + 1$. If it is not true for $\nu + 1$, let q_τ be such that $m_\tau x_{i_\tau} = x_1 x_n^{2(k+1-(\nu+1))} = x_1 x_n^{2(k-\nu)}$. Hence,

$$q_\tau = m_\tau x_{i_\tau} y^k x_{j_\tau} m'_\tau = x_1 x_n^{2(k-\nu)} y^k x_{j_\tau} m'_\tau.$$

Since $y^k = y^\nu y^{k-\nu}$ and y^ν contains $x_n^{2\nu}$, the polynomial

$$r = x_1 x_n^{2(k-\nu)} x_n^{2\nu} y^{k-\nu} x_{j_\tau} m'_\tau = x_1 x_n^{2k} y^{k-\nu} x_{j_\tau} m'_\tau \tag{12}$$

contains all monomials of $\{q_\tau\}$ that begin with $x_1 x_n^{2k}$ and these are not special; now q is special, hence every monomial of r must also appear in another summand of (4).

Thus, let $V = \{q_{\lambda_1}, \ldots, q_{\lambda_h}\}$ be a set of summands of (4) such that $q_\tau \notin V$ and $\{r\} \subseteq \{q_{\lambda_1}\} \cup \cdots \cup \{q_{\lambda_h}\}$. For simplicity we assume that $V = \{q_1, \ldots, q_h\}$. We also assume that V is *minimal* in the sense that, by omitting any $\{q_\mu\}$, $\{r\} \not\subseteq \bigcup_{\lambda \neq \mu} \{q_\lambda\}$.

From the minimality of V it follows that

$$\{q_\lambda\} \cap \{r\} \neq \emptyset \qquad \text{for} \qquad 1 \leqslant \lambda \leqslant h; \tag{13}$$

otherwise we omit q_λ from V. Since $\{r\} \subset \{q_\tau\}$ we have

$$\{q_\lambda\} \cap \{q_\tau\} \neq \emptyset \qquad \text{for} \qquad 1 \leqslant \lambda \leqslant h. \tag{14}$$

We prove now two additional properties of V:

(a) $\deg m_\lambda < 2(k - \nu)$ for $1 \leqslant \lambda \leqslant h$;

(b) if $q_\lambda, q_{\lambda'} \in V$ and $\lambda \neq \lambda'$, then $\{q_\lambda\} \cap \{q_{\lambda'}\} = \emptyset$.

Proof of (a). First $\deg m_\lambda \leqslant 2k$, since if $\deg m_\lambda > 2k$ we obtain $\deg m_\lambda \geqslant 2k + 2$ and taking a monomial of (13) we see by (12) that it begins with $x_1 x_n^{2k}$ and therefore m_λ begins with $x_1 x_n^{2k}$, contradicting the fact that it is special. Thus, $\deg m_\lambda \leqslant 2k$ and therefore

$$\deg(m_\lambda x_{i_\lambda}) \leqslant 2k + 1 = \deg(x_1 x_n^{2k})$$

from which it follows, again by (13) and (12), that $x_1 x_n^{2k}$ begins with $m_\lambda x_{i_\lambda}$.

We have also $\deg m_\lambda \neq 2(k - \nu) = \deg m_\tau$, since if equality holds, then from (14) we obtain by (D) that $q_\lambda = q_\tau$, but $q_\lambda \in V$ and $q_\tau \notin V$.

If $2(k - \nu) < \deg m_\lambda (\leqslant 2k)$, then $\deg m_\lambda \geqslant 2(k + 1 - \nu)$ and hence $\deg m_\lambda = 2(k + 1 - \mu)$ for some μ, $1 \leqslant \mu \leqslant \nu$. Since $x_1 x_n^{2k}$ begins with $m_\lambda x_{i_\lambda}$ we obtain $m_\lambda x_{i_\lambda} = x_1 x_n^{2(k+1-\mu)}$ with $1 \leqslant \mu \leqslant \nu$, but this contradicts the induction hypothesis. Hence $\deg m_\lambda \not\geqslant 2(k - \nu)$ and (a) is proved.

Proof of (b). Since $\lambda \neq \lambda'$ we have $q_\lambda \neq q_{\lambda'}$. If we assume that $\{q_\lambda\} \cap \{q_{\lambda'}\} \neq \emptyset$ then $\deg m_\lambda \neq \deg m_{\lambda'}$ since otherwise $q_\lambda = q_{\lambda'}$ by (D). Thus, suppose $\deg m_\lambda < \deg m_{\lambda'}$. By (a) we have $\deg m_{\lambda'} < 2(k - \nu) = \deg m_\tau$. Hence $\deg m_\lambda < \deg m_{\lambda'} < \deg m_\tau = 2(k - \nu) \leqslant 2k$ and $\{q_\lambda\} \cap \{q_{\lambda'}\} \neq \emptyset$. By (14) it follows that $\{q_\lambda\} \cap \{q_\tau\} \neq \emptyset$ and $\{q_{\lambda'}\} \cap \{q_\tau\} \neq \emptyset$. Thus, the conditions of

(E) are valid for $\lambda_1 = \lambda$, $\lambda_2 = \lambda'$, $\lambda_3 = \tau$. Hence $\{q_\lambda\} \cap \{q_\tau\} \subseteq \{q_{\lambda'}\} \cap \{q_\tau\}$ and since $\{r\} \subset \{q_\tau\}$ we obtain $\{q_\lambda\} \cap \{r\} \subseteq \{q_{\lambda'}\} \cap \{r\}$. From this it follows that $\{r\} \subseteq \bigcup_{\mu \neq \lambda} \{q_\mu\}$, which contradicts the minimality of V and (b) is proved.

Having the above properties at our disposal we continue with the proof of (F).

If $q_\lambda \in V$ we have $\{q_\lambda\} \cap \{q_\tau\} \neq \emptyset$, and by (a), $\deg m_\lambda < 2(k - \nu) = \deg m_\tau$. Let $\deg m_\tau - \deg m_\lambda = 2\delta > 0$, then $\deg m_\lambda = \deg m_\tau - 2\delta = 2(k - \nu - \delta) \geqslant 0$. By (D) with $\alpha = \lambda$, $\beta = \tau$, $\nu = \delta$, we obtain $\{q_\lambda\} \cap \{q_\tau\} = \{m_\tau x_{i_\tau} y^{k-\delta} x_{j_\lambda} m_\lambda'\}$, and by (9), $m_\lambda' = x_{j_\lambda} x_{t_{\delta-1}}^2 \cdots x_{t_1}^2 x_{j_\tau} m_\tau'$. But $m_\tau x_{i_\tau} = x_1 x_n^{2(k-\nu)}$; hence

$$\{q_\lambda\} \cap \{q_\tau\} = \{x_1 x_n^{2(k-\nu)} y^{k-\delta} x_{j_\lambda}^2 x_{t_{\delta-1}}^2 \cdots x_{t_1}^2 x_{j_\tau} m_\tau'\}.$$

Since $k - \nu - \delta \geqslant 0$, $y^{k-\delta} = y^\nu y^{k-\delta-\nu}$ and recalling that $\{r\}$ contains all those monomials of $\{q_\tau\}$ that begin with $x_1 x_n^{2k}$, we obtain

$$\{q_\lambda\} \cap \{r\} = \{x_1 x_n^{2k} y^{k-\nu-\delta} x_{j_\lambda}^2 x_{t_{\delta-1}}^2 \cdots x_{t_1}^2 x_{j_\tau} m_\tau'\}. \tag{15}$$

Now, let λ be such that $\deg m_\lambda = \min\{\deg m_\mu \mid 1 \leqslant \mu \leqslant h\}$. In the right-hand side of (15) we replace $x_{j_\lambda}^2$ by x_l^2 for every $l \neq j_\lambda$ and obtain the polynomial

$$r_l = x_1 x_n^{2k} y^{k-\nu-\delta} x_l^2 x_{t_{\delta-1}}^2 \cdots x_{t_1}^2 x_{j_\tau} m_\tau'.$$

We have $\{q_\lambda\} \cap \{r_l\} = \emptyset$. Indeed, all monomials of $\{q_\lambda\}$ end with $m_\lambda' = x_{j_\lambda} x_{t_{\delta-1}}^2 \cdots x_{t_1}^2 x_{j_\tau} m_\tau'$ and all monomials of $\{r_l\}$ end with $x_l x_{t_{\delta-1}}^2 \cdots x_{t_1}^2 x_{j_\tau} m_\tau' \neq m_\lambda'$ since $x_l \neq x_{j_\tau}$.

We have

$$\{r_l\} \subseteq \{x_1 x_n^{2k} y^{k-} x_{j_\tau} m_\tau'\} = \{r\} \subseteq \bigcup_{\mu=1}^{h} \{q_\mu\};$$

hence if $m \in \{r_l\}$, then $m \in \{q_{\mu_l}\}$ for some $q_{\mu_l} \in V$, and $q_{\mu_l} \neq q_\lambda$ since $\{q_\lambda\} \cap \{r_l\} = \emptyset$. By the minimality of $\deg m_\lambda$ we have $\deg m_{\mu_l} \geqslant \deg m_\lambda$ and we assert that $\deg m_{\mu_l} = \deg m_\lambda$. Indeed, if $\deg m_{\mu_l} > \deg m_\lambda$, then since $\deg m_{\mu_l} < \deg m_\tau$ [by (a)] it follows that $\deg m_\tau - \deg m_{\mu_l} = 2\epsilon < 2\delta = \deg m_\tau - \deg m_\lambda$. Then by (15), with q_{μ_l} replacing q_λ and ϵ replacing δ, we have

$$\{q_{\mu_l}\} \cap \{r\} = \{x_1 x_n^{2k} y^{k-\nu-\epsilon} x_{j_{\mu_l}}^2 x_{s_{\epsilon-1}}^2 \cdots x_{s_1}^2 x_{j_\tau} m_\tau'\}. \tag{16}$$

Now, $m \in \{q_{\mu_l}\} \cap \{r_l\} \subseteq \{q_{\mu_l}\} \cap \{r\}$; hence, comparing (16) with $\{r_l\}$ and since $\epsilon < \delta$, we obtain

$$x_{s_1}^2 = x_{t_1}^2, \qquad \cdots, \qquad x_{s_{\epsilon-1}}^2 = x_{t_{\epsilon-1}}^2, \qquad x_{j_{\mu_l}}^2 = x_{t_\epsilon}^2.$$

From this it follows that $\{q_{\mu_l}\} \cap \{r\} \supseteq \{q_\lambda\} \cap \{r\}$, hence $\{r\} \subseteq \bigcup_{\mu \neq \lambda} \{q_\mu\}$, which contradicts the minimality of V. Thus, we have $\deg m_\lambda = \deg m_{\mu_l}$ and hence $x_{j_{\mu_l}} = x_l$ and $m'_{\mu_l} = x_l x_{t_{\delta-1}}^2 \cdots x_{t_1}^2 x_{j_\tau} m'_\tau$. Let us define q_{μ_l} for $l = j_\lambda$ by putting $\mu_{j_\lambda} = \lambda$, so q_{μ_l} has been defined for $l = 1,\dots, n$, and $\deg m_{\mu_l} = \deg m_\lambda = 2(k - \nu - \delta) < \deg m_\tau$. Since $\{q_{\mu_l}\} \cap \{q_\tau\} \neq \emptyset$, m_τ begins with $m_{\mu_l} x_{i_{\mu_l}}$, then $m_{\mu_l} x_{i_\mu} = x_1 x_n^{2(k-\nu-\delta)}$ does not depend on l. We denote m_{μ_l} by m_0 and $x_{i_{\mu_l}}$ by $x_i (x_i = x_1$ if $k - \nu - \delta = 0$ and $x_i = x_n$ if $k - \nu - \delta > 0)$. We also denote $x_{t_{\delta-1}}$ by x_j and $x_{t_{\delta-1}} x_{t_{\delta-2}}^2 \cdots x_{t_1}^2 x_{j_\tau} m'_\tau$ by m'_0 (if $\delta = 1$, then we take $m'_\tau = m'_0$ and $x_{j_\tau} = x_j$) and obtain $m'_{\mu_l} = x_l x_j m'_0$. Thus,

$$q_{\mu_l} = m_{\mu_l} x_{i_{\mu_l}} y^k x_{j_{\mu_l}} m'_{\mu_l} = m_0 x_i y^k x_l (x_l x_j m'_0) = m_0 z_{il} (x_l x_j m'_0) \tag{17}$$

for $l = 1,\dots, n$. But by (C) the sum (4) does not contain n summands of the form (17). Thus, from the assumption that (F) is not valid for $\nu + 1$ but is true for all $0 \leqslant \mu < \nu + 1$, we have obtained a contradiction. Hence (F) is valid for $\nu + 1$, which completes the induction on the validity of (F).

We complete now the proof of Theorem 11.

Choose in (F) $\nu = k + 1$, then it follows that the representation (4) of q does not contain a summand q_τ such that $m_\tau x_{i_\tau} = x_1$ and which is necessarily of the form: $q_\tau = z_{1j_\tau} m'_\tau$. This contradicts (B) which proves that the sum (4) does not exist; hence $S \cap T = \{0\}$ and Theorem 11 follows.

6. R has no Zero-Divisors

We have proved that every residue class of $R = P/T$ contains one and only one representative which is a special polynomial. For $p \in P$, we denote by $S(p)$ the unique special polynomial of $\bar{p} = p + T$. Thus, if q is special, then $\bar{p} = \bar{q}$ if and only if $S(p) = q$.

Definition. If $0 \neq p \in S$ and $p^{(\alpha)}$ is its nonzero homogeneous component of least degree, then α will be called the value of p and we shall write $v(p) = \alpha$. For $p = 0$ we set $v(0) = \infty$. If $\bar{p} \in R$ we define $v(\bar{p}) = v(S(p))$.

Note that $v(\bar{p})$ is well defined since $S(p)$ is the unique special polynomial of $\bar{p}$.

We shall prove that if $\bar{p}, \bar{q} \in R$, then $v(\bar{p}\bar{q}) = v(\bar{p}) + v(\bar{q})$, from which it follows that R has no zero divisors. (In fact, v is a valuation on R.) We first need some lemmas.

LEMMA 12. *If* $p_1, \ldots, p_l, p, q \in P$, *then*

(a) $S\left(\sum_{i=1}^{l} p_i\right) = \sum_{i=1}^{l} S(p_i)$;

(b) $S(pq) = S(pS(q))$;

(c) *for every* $\alpha \geqslant 0$, $S(p^{(\alpha)}) = (S(p))^{(\alpha)}$.

Proof. (a) and (b) are evident; let us prove (c).

Let $p = \Sigma p^{(\alpha)}$, then by (a) we have $S(p) = \Sigma S(p^{(\alpha)})$. By the corollary to Lemma 8 it is seen that, since $p^{(\alpha)}$ is homogeneous, then either $S(p^{(\alpha)}) = 0$ or $S(p^{(\alpha)})$ is homogeneous and $\deg(S(p^{(\alpha)})) = \deg(p^{(\alpha)}) = \alpha$. This implies that $(S(p))^{(\alpha)} = S(p^{(\alpha)})$ by the uniqueness of the decomposition of a polynomial as a sum of homogeneous polynomials.

LEMMA 13. *If* $p = x_1 p'$ *then there exists* $u \in F[x]$ *such that the monomials of* $\{p + x_1 y^k u\}$ *do not begin with* $x_1 x_n^{2k}$.

Proof. Let p_1 be the sum of all monomials of $\{p\}$ which begin with $x_1 x_n^{2k}$; then $p_1 = x_1 x_n^{2k} u$ for some $u \in F[x]$ (which is 0 if $p_1 = 0$). Let p_0 be such that $p = p_0 + p_1$, then the monomials of $\{p_0\}$ do not begin with $x_1 x_n^{2k}$. Thus,

$$p + x_1 y^k u = p_0 + x_1 x_n^{2k} u + x_1 y^k u = p_0 + x_1(x_n^{2k} + y^k)\, u.$$

Since $\{y^k\}$ contains x_n^{2k}, $\{y^k + x_n^{2k}\}$ does not contain x_n^{2k}, and hence the monomials of $\{x_1(x_n^{2k} + y^k)\, u\}$ do not begin with $x_1 x_n^{2k}$, and since the same is true for $\{p_0\}$ the required result follows.

LEMMA 14. *If* $p \in P$ *is homogeneous and the monomials of* $\{p\}$ *do not begin with* x_n^{2k-1} *then the same is true for* $\{S(p)\}$.

Proof. If $S(p) = p$ there is nothing to prove. Assume $S(p) \neq p$, then by Lemma 8 there exists a finite chain $p = q_0, q_1, \ldots, q_l$ such that $S(p) = q_l$ and $q_{\mu+1} = q_\mu + m_\mu z_{i_\mu j_\mu} m'_\mu$, where $m_\mu x_{i_\mu} x_n^{2k} x_{j_\mu} m'_\mu \in \{q_\mu\}$, $\mu = 0, 1, \ldots, l-1$. Since $q_0 = p$ does not contain a monomial which begins with x_n^{2k-1}, we can obtain our result by induction; assume the monomials of $\{q_\mu\}$ do not begin with x_n^{2k-1}. Since $q_{\mu+1} = q_\mu + m_\mu z_{i_\mu j_\mu} m'_\mu$, it is sufficient to prove that $\{m_\mu z_{i_\mu j_\mu} m'_\mu\}$ does not contain a monomial that begins with x_n^{2k-1}. Let

$m_\mu x_{i_\mu} x_{l_1}^2 \cdots x_{l_k}^2 x_{j_\mu} m'_\mu$ be any monomial of $\{m_\mu z_{i_\mu j_\mu} m'_\mu\}$. If it begins with x_n^{2k-1}, then clearly the same is true for $m_\mu x_{i_\mu} x_n^{2k} x_{j_\mu} m'_\mu$; but $m_\mu x_{i_\mu} x_n^{2k} x_{j_\mu} m'_\mu \in \{q_\mu\}$, which contradicts the induction hypothesis.

LEMMA 15. *If* $p = \sum_{j=1}^n x_1 x_j p_j \in T$ *is homogeneous and the monomials of* $\{p\}$ *do not begin with* $x_1 x_n^{2k}$, *then all* $p_j \in T$.

Proof. By Lemma 12(a) we have

$$S(p) = S\left(\sum_{j=1}^n x_1 x_j p_j\right) = \sum_{j=1}^n S(x_1 x_j p_j)$$

and since $p \in T$ we obtain $S(p) = \sum_{j=1}^n S(x_1 x_j p_j) = 0$. We shall show that $S(x_1 x_j p_j) = x_1 x_j S(p_j)$ for $1 \leqslant j \leqslant n$. Hence $\sum_{j=1}^n x_1 x_j S(p_j) = 0$ and since $\{x_1 x_j S(p_j)\} \cap \{x_1 x_{j'} S(p_{j'})\} = \emptyset$ for $j \neq j'$, we have $x_1 x_j S(p_j) = 0$ which implies $S(p_j) = 0$ and therefore $p_j \in T$.

To prove that $S(x_1 x_j p_j) = x_1 x_j S(p_j)$ it suffices to show by Lemma 12(b) that $x_1 x_j S(p_j)$ is special. For $j \neq n$, $x_1 x_j S(p_j) \in S$ since $S(p_j) \in S$. It remains to prove that $x_1 x_n S(p_n)$ is special. By assumption the monomials of $\{p\}$ do not begin with $x_1 x_n^{2k}$ and since $\{x_1 x_n p_n\} \subseteq \{p\}$ the same is true for $\{x_1 x_n p_n\}$. Hence the monomials of $\{p_n\}$ do not begin with x_n^{2k-1} and by the previous lemma it follows that the monomials of $\{S(p_n)\}$ do not begin with x_n^{2k-1} and consequently the monomials of $\{x_1 x_n S(p_n)\}$ do not begin with $x_1 x_n^{2k}$. Furthermore, $S(p_n)$ is special so $x_1 x_n S(p_n)$ is special which proves our assertion and hence our lemma.

The following are common assumptions for Lemmas 16, 17, 18:

α, β, γ, h are integers $\geqslant 0$ and $\alpha \geqslant \beta$.

$p, q, r, s \in S$ are homogeneous and $p = p^{(2\alpha)}$, $r = r^{(2\beta)} \neq 0$,

$$pq = (pq)^{(2\gamma)}, \qquad rs = (rs)^{(2\gamma)}.$$

(Note that if $p = 0$ then the assumption $p = p^{(2\alpha)}$ still holds.)

$v \in F[x]$ is homogeneous such that $x_j y^h v = (x_j y^h v)^{(2\gamma)}$.

LEMMA 16. *If* $\beta > 0$ *and* $pq + rs + x_{j_0} y^h v \in T$ *for some* j_0, *then there exist* $p_0, r_0 \in S$ *with* $p_0 = p_0^{(2\alpha)} = x_1 p'_0$, $r_0 = r_0^{(2\beta)} = x_1 r'_0 \neq 0$ *and* $p_0 = 0$ *if* $p = 0$ *such that:* $p_0 q + r_0 s + x_1 y^h v_0 \in T$, *where either* $v_0 = v$ *or* $v_0 = 0$.

Proof. Since $\alpha \geqslant \beta > 0$ we have $p = \sum_{i=1}^n x_i p_i$, $r = \sum_{i=1}^n x_i r_i$. Hence $pq + rs + x_{j_0} y^h v = \Sigma x_i p_i q + \Sigma x_i r_i s + x_{j_0} y^h v \in T$ and this relation can be written in the form

$$x_{j_0}(p_{j_0} q + r_{j_0} s + y^h v) + \sum_{i \neq j_0} x_i (p_i q + r_i s) \in T$$

By Lemma 5(b) we obtain

$$x_{j_0}(p_{j_0}q + r_{j_0}s + y^h v) \in T \qquad \text{and} \qquad x_i(p_i q + r_i s) \in T \qquad \text{for} \qquad i \neq j_0,$$

and by (a) of the same lemma,

$$x_1(p_{j_0}q + r_{j_0}s + y^h v) \in T \text{ and } x_1(p_i q + r_i s) \in T \text{ for } i \neq j_0.$$

Since $r \neq 0$ we have $r_i \neq 0$ for some i. If $i = j_0$ we take $p_0 = x_1 p_{j_0}$, $r_0 = x_1 r_{j_0}$ and $v_0 = v$. If $i \neq j_0$ we take $p_0 = x_1 p_i$, $r_0 = x_1 r_i$ and $v_0 = 0$. In both cases we also obtain that $p_0 = p_0^{(2\alpha)} = x_1 p_0' \in S$, $0 \neq r_0 = r_0^{(2\beta)} = x_1 r_0' \in S$ by Lemma 3. Clearly, if $p = 0$, then all $p_i = 0$ and $p_0 = 0$.

LEMMA 17. *If $\beta > 0, 0 < h \leqslant k$ and $pq + rs + x_1 y^h v \in T$, with $p = x_1 p_0'$, $r = x_1 r_0'$, then for $j = 1, 2, \ldots, n$ there exist $p_j = p_j^{(2\alpha-2)} \in S$ which is 0 if $p = 0$, $r_j = r_j^{(2\beta-2)} \in S$ which is $\neq 0$ for at least one j, and $w \in F[x]$ with the same property as v such that: $p_j q + r_j s + x_j y^{h-1} w \in T$ for all j.*

Proof. By assumption, $pq + rs + x_1 y^h v$ is of the form $x_1 p'$ $(p' = p_0' r + r_0' s + y^h v)$ and for the u of Lemma 13 we obtain that $x_1 y^k u = (x_1 y^k u)^{(2\gamma)}$ and the monomials of $\{x_1 p' + x_1 y^k u\}$ do not begin with $x_1 x_n^{2k}$. Let $v + y^{k-h} u = w$, then w has the same property as v and we have

$$pq + rs + x_1 y^h w = (pq + rs + x_1 y^h v) + x_1 y^k u \in T.$$

Let $p = \sum_{j=1}^n x_1 x_j p_j$, $r = \sum_{j=1}^n x_1 x_j r_j$; then since $h > 0$,

$$pq + rs + x_1 y^h w = \sum_{j=1}^n x_1 x_j p_j q + \sum_{j=1}^n x_1 x_j r_j s + x_1 \left(\sum_{j=1}^n x_j^2\right) y^{h-1} w$$

$$= \sum_{j=1}^n x_1 x_j (p_j q + r_j s + x_j y^{h-1} w).$$

Now, $pq + rs + x_1 y^h w = x_1 p' + x_1 y^k u$ does not contain monomials which begin with $x_1 x_n^{2k}$, it is homogeneous and belongs to T; hence Lemma 15 implies that

$$p_j q + r_j s + x_j y^{h-1} w \in T \qquad \text{for} \qquad j = 1, 2, \ldots, n.$$

Clearly p_j, r_j satisfy all the requirements of the lemma.

REMARK. If the assumptions in the previous lemma hold for $v = 0$, i.e. $pq + rs \in T$, and if $pq + rs$ does not contain monomials which begin with $x_1 x_n^{2k}$ then the u of Lemma 13 is 0 and hence $w = v + y^{k-h} u = 0$ and $p_j q + r_j s \in T$ for $j = 1, 2, \ldots, n$.

LEMMA 18. *If* $pq + rs \in T$, *then for* $0 \leqslant \nu < \min(\beta, k)$ *there exist* $f_\nu = f_\nu^{(2\alpha-2\nu)} = x_1 f'_\nu \in S$, $g_\nu = g_\nu^{(2\beta-2\nu)} = x_1 g'_\nu \in S$ *with* $f_\nu = 0$ *if* $p = 0$ *and* $g_\nu \neq 0$ *such that*

$$f_\nu q + g_\nu s + x_1 y^{k-\nu} w_\nu \in T, \tag{18}$$

where w_ν *has the same property as* v (*for* $h = k$).

Proof. We prove the lemma by induction on ν. For $\nu = 0$ we obtain the result by Lemma 16 with $v = 0$, if we take $f_0 = p_0$, $g_0 = r_0$, $v_0 = 0$.

If (18) holds for some ν such that $\nu + 1 < \min(\beta, k)$ then since $\alpha - \nu \geqslant \beta - \nu > 0$ and $k - \nu > 0$ we obtain (by Lemma 17 with $p = f_\nu$, $r = g_\nu$, $v = w_\nu$, and $\alpha - \nu$, $\beta - \nu$, $k - \nu$, replacing α, β, h, respectively)

$$p_j q + r_j s + x_j y^{k-\nu-1} w \in T \qquad \text{for} \qquad j = 1,..., n.$$

Let j be such that $r_j \neq 0$ then since $\beta - (\nu + 1) > 0$ we obtain the result by Lemma 16 with p_j, r_j, x_j, w replacing p, q, x_{j_0}, v, if we take $f_{\nu+1} = p_0$, $g_{\nu+1} = r_0$, $w_{\nu+1} = v_0$.

Now we turn to the main result of this section which is

THEOREM 19. *R has no zero-divisors.*

Proof. The theorem will follow if we prove that, for $\bar{p}, \bar{q} \in R$,

$$v(\bar{p}\bar{q}) = v(\bar{p}) + v(\bar{q}). \tag{19}$$

Indeed, let $\bar{p}, \bar{q} \neq 0$ then by definition it follows that $v(\bar{p})$, $v(\bar{q})$ are finite and hence by (19) $v(\bar{p}\bar{q})$ is finite and therefore $\bar{p}\bar{q} \neq 0$.

Let us prove first the following assertion [which implies (19) for p, q homogeneous]:

If r, s *are homogeneous and special,* $r \neq 0$ *and* $rs \in T$ ($S(rs) = 0$) *then* $s \in T$ ($s = 0$).

We shall prove this assertion by induction on $\deg r = 2\beta$ using the above lemmas with $p = 0$.

If $\beta \leqslant k$, then Lemma 18 holds for $0 \leqslant \nu < \beta$. Hence for $\nu = \beta - 1$ we obtain $g_{\beta-1} s + x_1 y^{k-(\beta-1)} w_{\beta-1} \in T$ such that $0 \neq g_{\beta-1} = g_{\beta-1}^{(2)} = x_1 g'_{\beta-1}$. Apply Lemma 17 with $p = 0$, $r = g_{\beta-1}$, $h = k - (\beta + 1) > 0$ and obtain

$$r_j s + x_j y^{k-\beta} w \in T, \qquad \text{for} \qquad j = 1,..., n,$$

and since $\deg g_{\beta-1} = 2$, all the r_j are constants, 0, 1, and at least one of them equals 1. Let j be such that $r_j = 1$, thus $s + x_j y^{k-\beta} w \in T$. If $x_j y^{k-\beta} w \notin T$ then for any $i \neq j$ (there exists $i \neq j$ since $n \geqslant 2$) it follows by Lemma 5(a) that $x_i y^{k-\beta} w \notin T$ and since $r_i s + x_i y^{k-\beta} w \in T$ we must have $r_i = 1$, so $s + x_i y^{k-\beta} w \in T$. Finally we have

$$x_j y^{k-\beta} w + x_i y^{k-\beta} w = (s + x_j y^{k-\beta} w) + (s + x_i y^{k-\beta} w) \in T$$

and by Lemma 5(b) we deduce that also $x_j y^{k-\beta} w \in T$, contrary to our assumption. It remains therefore that $x_j y^{k-\beta} w \in T$ and hence $s \in T$ as required.

Let $\beta > k$ and assume the result is true for $\beta - 1$. We have $rs \in T$ and by Lemma 16 with $p = 0$, $v = 0$ we may assume $r = x_1 r_0'$. Now, $r = r^{(2\beta)}$ is special and $2\beta \geqslant 2k + 2$, so r and hence also rs cannot contain monomials which begin with $x_1 x_n^{2k}$. Then by the remark to Lemma 17 we obtain $r_j s \in T$ for $j = 1,\ldots, n$. Let j be such that $r_j \neq 0$, then since $\deg r_j = 2(\beta - 1)$ we obtain the result $s \in T$ by the induction hypothesis.

We can turn now to the proof of (19).

Let $\bar{p}$, $\bar{q} \neq 0$ and w.l.g. we may assume that p, q are special. Let $v(\bar{p}) = \alpha$ and $v(\bar{q}) = \beta$; hence by definition,

$$p = p^{(\alpha)} + p^{(\alpha+1)} + \cdots; \qquad q = q^{(\beta)} + q^{(\beta+1)} + \cdots$$

and $p^{(\alpha)}$, $q^{(\beta)} \neq 0$. By the above assertion with $r = p^{(\alpha)}$, $s = q^{(\beta)}$, we obtain $S(p^{(\alpha)} q^{(\beta)}) \neq 0$ and since $p^{(\alpha)} q^{(\beta)}$ is homogeneous of degree $\alpha + \beta$, it follows by the corollary to Lemma 8 that $\deg (S(p^{(\alpha)} q^{(\beta)})) = \alpha + \beta$. Now we have

$$pq = p^{(\alpha)} q^{(\beta)} + (p^{(\alpha)} q^{(\beta+1)} + p^{(\alpha+1)} q^{(\beta)}) + \cdots,$$

and hence the nonzero homogeneous component of least degree of $S(pq)$ is $S(p^{(\alpha)} q^{(\beta)})$ which is of degree $\alpha + \beta$. Thus, by definition of v it follows that $v(S(pq)) = \alpha + \beta = v(\bar{p}) + v(\bar{q})$ and we obtain (19) since $v(\bar{p}\bar{q}) = v(\overline{pq}) = v(S(pq))$, and our theorem is proved.

The following lemma will be used in the next section and it is proved here since it is also a result of Lemmas 16-18.

LEMMA 20. *Let $0 \neq p, q, r, s \in S$, homogeneous and $p = p^{(2\alpha)}$, $r = r^{(2\beta)}$, $\alpha \geqslant \beta$, $\deg (pq) = \deg (rs)$. If $n \geqslant 3$ and $pq + rs \in T$, then there exists $t \in S$ such that $tq + s \in T$ and $t = t^{(2\alpha - 2\beta)}$.*

Proof. As in Theorem 19 we first prove the result for $\beta \leqslant k$.

Apply Lemma 18 and Lemma 17 as before and obtain

$$p_j q + r_j s + x_j y^{k-\beta} w \in T, \qquad j = 1, 2,\ldots, n; \tag{20}$$

all r_j are constants 0, 1, and at least one of them equals 1.

Consider two cases: (a) $x_1 y^{k-\beta} w \in T$; (b) $x_1 y^{k-\beta} w \notin T$.

(a) Let j be such that $r_j = 1$, then $p_j q + s + x_j y^{k-\beta} w \in T$. Since $x_1 y^{k-\beta} w \in T$ it follows $x_j y^{k-\beta} w \in T$ by Lemma 5 and hence $p_j q + s \in T$ and the theorem is proved with $t = p_j \in S$.

(b) By Lemma 5 also $x_j y^{k-\beta} w \notin T$ for $j = 1, 2, \ldots, n$ and also every subsum of $\sum_{j=1}^{n} x_j y^{k-\beta} w$ does not belong to T. If $\Sigma' x_j y^{k-\beta} w$ is such a subsum, then from (20) we obtain by summation

$$\Sigma' p_j q + \Sigma' r_j s + \Sigma' x_j y^{k-\beta} w \in T \tag{21}$$

From this it follows that $\alpha \neq \beta$. Indeed if $\alpha = \beta$ then the p_j's are also constants. Since $n \geqslant 3$ the two-dimensional vectors (p_1, r_1), $(p_2, r_2), \ldots$, (p_n, r_n) over the field $\{0, 1\}$ are dependent and therefore there exists a subsum of $\sum_{j=1}^{n} (p_j, r_j)$ which is 0. Denote this subsum by $\Sigma'(p_j, r_j)$, then $\Sigma' p_j = 0$, $\Sigma' r_j = 0$ and from (21) it follows that $\Sigma' x_j y^{k-\beta} w \in T$, which is a contradiction.

Since $\alpha \geqslant \beta$ and $\alpha \neq \beta$, we have $\alpha > \beta$.

Let $r_j = 1$ and let $i \neq j$, then by (20) we have

$$p_j q + s + x_j y^{k-\beta} w \in T; \qquad p_i q + r_i s + x_i y^{k-\beta} w \in T.$$

Since $\alpha > 0$, we can write

$$p_j = x_1 p_1' + \cdots + x_n p_n'; \qquad p_i = x_1 p_1'' + \cdots + x_n p_n''.$$

Now, if $r_i = 0$, from $x_1 p_1'' q + \cdots + x_n p_n'' q + x_i y^{k-\beta} w \in T$ it follows by Lemma 5 that $x_i p_i'' q + x_i y^{k-\beta} w \in T$ and also $x_j p_i'' q + x_j y^{k-\beta} w \in T$; hence

$$(p_j + x_j p_i'')\, q + s = (p_j q + s + x_j y^{k-\beta} w) + (x_j p_i'' q + x_j y^{k-\beta} w) \in T$$

and the result is obtained with $t = p_j + x_j p_i''$.

If $r_i = 1$, then $p_i q + s + x_i y^{k-\beta} w \in T$; hence

$$(p_j + p_i)\, q + x_j y^{k-\beta} w + x_i y^{k-\beta} w \in T$$

and again by Lemma 5 we obtain $x_j(p_j' + p_j'')\, q + x_j y^{k-\beta} w \in T$, from which it follows that $(p_j + x_j p_j' + x_j p_j'')\, q + s \in T$. Thus, the result is obtained with $t = p_j + x_j p_j' + x_j p_j''$.

It is readily verified that in each case $\deg t = \deg p_j$ and by Lemmas 18 and 17 $\deg p_j = 2\alpha - 2\beta$. Hence we have $t = t^{(2\alpha - 2\beta)}$.

This completes the proof of the lemma for $\beta \leqslant k$.

Let $\beta > k$ and assume the result is true for $\beta - 1$. We have $pq + rs \in T$ and by Lemma 16 with $v = 0$ we may assume $p = x_1 p_0'$, $r = x_1 r_0'$. Now, $r = r^{(2\beta)}$ is special and $2\beta \geqslant 2k + 2$, so r and hence also rs cannot contain monomials which begin with $x_1 x_n^{2k}$. Since $p = p^{(2\alpha)}$ is special and $\alpha \geqslant \beta$ the same is true for pq. Then by the remark to Lemma 17 we obtain $p_j q + r_j s \in T$ and let j be such that $r_j \neq 0$. Since $\deg r_j = 2(\beta - 1)$, the result follows by induction.

7. The Embedding of R^* in a Group

Our next aim is to show that for $n \geqslant 3$, R^* is embeddable in a group. The proof of this fact is based on the following result due to Doss [2]:

> A semigroup which satisfies the cancellation laws is embeddable in a group, if for any two elements with a common left-multiple, one of them is a right-divisor of the other.

The semigroup R^* does not satisfy this condition as is readily seen by considering the equation $\overline{(x_1^2x_2^2 + 1)\, x_1^2} = x_1^2(x_2^2x_1^2 + 1)$ ($\overline{x_1^2}$ is not a multipl of $\overline{x_2^2x_1^2 + 1}$ and $\overline{x_2^2x_1^2 + 1}$ is not a multiple of $\overline{x_1^2}$). However we can apply Doss' result to a larger semigroup $\mathscr{R}^* = \mathscr{R} - \{0\}$, where $\mathscr{R}$ is the ring defined in Section 2.

First we shall prove that R is embeddable in $\mathscr{R}$. We recall that the injection $F[x] \to F[[x]]$ induces the injections $P \to \mathscr{P}$ and $T \to \mathscr{T}$. Let ϕ be the composition of the injection $P \to \mathscr{P}$ with the natural homomorphism $\mathscr{P} \to \mathscr{P}/\mathscr{T}$. Thus, $\phi : P \to \mathscr{P}/\mathscr{T} = \mathscr{R}$ and $\ker \phi = P \cap \mathscr{T}$. We assert that $P \cap \mathscr{T} = T$ which implies that $R = P/T$ is embeddable in $\mathscr{R}$. Clearly we have $T \subseteq P \cap \mathscr{T}$ since $T \subseteq P$ and $T \subseteq \mathscr{T}$. On the other hand, by the remark to Lemma 4, $\mathscr{T}$ is homogeneous and its homogeneous polynomials belong to T. Hence, if $p = \Sigma p^{(\alpha)} \in P \cap \mathscr{T}$ then all $p^{(\alpha)} \in T$ and also $p = \Sigma p^{(\alpha)} \in T$. Thus, $P \cap \mathscr{T} \subseteq T$ and our assertion is proved.

To prove that $\mathscr{R}$ is an integral domain ($\mathscr{R}^*$ is a semigroup with cancellation laws) we observe that the valuation defined on R can be extended to $\mathscr{R}$ in the following way:

If $p \in \mathscr{P}$ is such that all its homogeneous components are special, then p will be called special, and if $p \neq 0$ and $p^{(\alpha)}$ is its nonzero homogeneous component of least degree we set: $v(p) = \alpha$.

If $p = \Sigma p^{(\alpha)} \in P$, then let $S(p) = \Sigma S(p^{(\alpha)})$. Clearly $S(p)$ is special and it is the unique special element of $\bar{p} = p + \mathscr{T}$.

Thus, for $\bar{p} \in \mathscr{R}$ we define $v(\bar{p}) = v(S(p))$.

The equation $v(\bar{p}\bar{q}) = v(\bar{p}) + v(\bar{q})$ for $\bar{p}, \bar{q} \in \mathscr{R}$ is proved as in Theorem 19 and this clearly implies that $\mathscr{R}$ is an integral domain.

It remains to prove that $\mathscr{R}^*$ satisfies Doss' condition. First we prove the following consequence of Lemma 20.

Lemma 21. *Let $p, q, r, s \in P$ be homogeneous, $q, r \notin T$ and $v(\bar{p}) = \alpha \geqslant \gamma = v(\bar{r})$. If $\bar{p}\bar{q} = \bar{r}\bar{s}$ and $n \geqslant 3$, then there exists $t = t^{(\alpha-\gamma)} \in P$ such that $\bar{p} = \bar{r}\bar{t}$ and $\bar{t}\bar{q} = \bar{s}$.*

Proof. If $\bar{p}\bar{q} = \bar{r}\bar{s} = 0$, then since R is an integral domain and since $\bar{q} \neq 0$, $\bar{r} \neq 0$, we obtain $\bar{p} = \bar{s} = 0$ and the result follows with $t = 0$.

Let $\bar{p}\bar{q} = \bar{r}\bar{s} \neq 0$, then we have also $p, s \notin T$ and $S(p)$, $S(q)$, $S(r)$, $S(s)$ are nonzero, special, and homogeneous. Since

$$\overline{S(p)\, S(q)} = \overline{S(p)}\, \overline{S(q)} = \bar{p}\bar{q} = \bar{r}\bar{s} = \overline{S(r)}\, \overline{S(s)} = \overline{S(r)\, S(s)}$$

it follows that $S(p)\, S(q) + S(r)\, S(s) \in T$. By lemma 12(c) $S(p) = S(p^{(\alpha)}) = (S(p))^{(\alpha)}$ and $S(r) = (S(r))^{(\gamma)} \neq 0$. Thus, all the conditions of Lemma 20 are satisfied for $S(p)$, $S(q)$, $S(r)$, $S(s)$, α, γ replacing p, q, r, s, 2α, 2β respectively, and therefore there exists $t = t^{(\alpha-\gamma)} \in S$ such that $tS(q) + S(s) \in T$. Hence $\bar{t}\bar{q} = \overline{tS(q)} = \overline{S(s)} = \bar{s}$ and therefore $\bar{p}\bar{q} = \bar{r}\bar{t}\bar{q}$ from which it follows that $\bar{p} = \bar{r}\bar{t}$ since $\bar{q} \neq 0$, and our lemma is proved.

If $p_1, p_2 \in P$ and $\bar{p}_1 = \bar{p}_2$, then for convenience we shall write $p_1 \equiv p_2$ meaning $\equiv \bmod T$.

We extend Lemma 21 to power series.

THEOREM 22. *Let $0 \neq p, q, r, s \in \mathscr{P}$ be special and $\bar{p}\bar{q} = \bar{r}\bar{s}$. If $n \geqslant 3$ and $v(p) \geqslant v(r)$, then there exists $\bar{t} \in \mathscr{R}^*$ such that $\bar{p} = \bar{r}\bar{t}$, $\bar{t}\bar{q} = \bar{s}$.*

Proof. Let α, β, γ, δ be the values of p, q, r, s, respectively, then $p^{(\alpha)}$, $q^{(\beta)}$, $r^{(\gamma)}$, $s^{(\delta)} \neq 0$, and

$$\alpha + \beta = v(\bar{p}) + v(\bar{q}) = v(\bar{p}\bar{q}) = v(\bar{r}\bar{s}) = v(\bar{r}) + v(\bar{s}) = \gamma + \delta.$$

$\bar{p}\bar{q} = \bar{r}\bar{s}$ means $pq \equiv rs (\bmod \mathscr{T})$ and since $\mathscr{T}$ is homogeneous and its homogeneous polynomials belong to T we have

$$(pq)^{(\tau)} \equiv (rs)^{(\tau)} \qquad \text{for each} \qquad \tau \geqslant 0. \tag{22}$$

For $\tau = \alpha + \beta = \gamma + \delta$ we obtain $p^{(\alpha)} q^{(\beta)} \equiv r^{(\gamma)} s^{(\delta)}$ and by the previous lemma there exists a homogeneous polynomial of degree $\epsilon = \alpha - \gamma = \delta - \beta$ such that, if we denote it by $t^{(\epsilon)}$, then

$$p^{(\alpha)} \equiv r^{(\gamma)} t^{(\epsilon)}; \qquad t^{(\epsilon)} q^{(\beta)} \equiv s^{(\delta)}. \tag{23}$$

Assume that for $\mu = 0, 1,..., \nu$, $t^{(\epsilon+\mu)}$ (which is 0 or homogeneous of degree $\epsilon + \mu$) has already been defined such that $t_\nu = t^{(\epsilon)} + \cdots t^{(\epsilon+\nu)}$ satisfies

$$p^{(\alpha+\mu)} \equiv (rt_\nu)^{(\alpha+\mu)}; \qquad (t_\nu q)^{(\delta+\mu)} \equiv s^{(\delta+\mu)} \tag{24}$$

for $\mu = 0, 1,..., \nu$, and note that, for $\mu = 0$, (24) is identical with (23).

We proceed to define $t^{(\epsilon+\nu+1)}$ such that (24) will hold for $t_{\nu+1} = t_\nu + t^{(\epsilon+\nu+1)}$ replacing t_ν and for $\mu = 0, 1,..., \nu + 1$.

If this is proved then $t = t^{(\epsilon)} + t^{(\epsilon+1)} + \cdots$ will satisfy:

$$p^{(\alpha+\mu)} \equiv (rt)^{(\alpha+\mu)}; \qquad (tq)^{(\delta+\mu)} \equiv s^{(\delta+\mu)}$$

for each $\mu \geqslant 0$. This means $p \equiv rt \,(\bmod \mathscr{T})$, $tq \equiv s (\bmod \mathscr{T})$ as required in the theorem. It is also clear that $t \in \mathscr{P}$ and $\bar{t} \in \mathscr{R}^*$.

For $\tau = \alpha + \beta + \nu + 1 = \gamma + \delta + \nu + 1$ we have, by (22),

$$(pq)^{(\alpha+\beta+\nu+1)} \equiv (rs)^{(\gamma+\delta+\nu+1)}. \tag{25}$$

Let us calculate both sides of (25) using (24):

$$\begin{aligned}(pq)^{(\alpha+\beta+\nu+1)} &= p^{(\alpha+\nu+1)}q^{(\beta)} + \sum_{\mu=0}^{\nu} p^{(\alpha+\mu)}q^{(\beta+\nu+1-\mu)} \\ &\equiv p^{(\alpha+\nu+1)}q^{(\beta)} + \sum_{\mu=0}^{\nu} (rt_\nu)^{(\alpha+\mu)}\, q^{(\beta+\nu+1-\mu)} \\ &= p^{(\alpha+\nu+1)}q^{(\beta)} + (rt_\nu)^{(\alpha+\nu+1)}\, q^{(\beta)} + \sum_{\mu=0}^{\nu+1} (rt_\nu)^{(\alpha+\mu)}\, q^{(\beta+\nu+1-\mu)} \\ &= [p^{(\alpha+\nu+1)} + (rt_\nu)^{(\alpha+\nu+1)}]\, q^{(\beta)} + [(rt_\nu)\, q]^{(\alpha+\beta+\nu+1)}.\end{aligned}$$

Similarly we have

$$(rs)^{(\gamma+\delta+\nu+1)} \equiv r^{(\gamma)}[(t_\nu q)^{(\delta+\nu+1)} + s^{(\delta+\nu+1)}] + [r(t_\nu q)]^{(\gamma+\delta+\nu+1)}.$$

But $[(rt_\nu)\, q]^{(\alpha+\beta+\nu+1)} = [r(t_\nu q)]^{(\gamma+\delta+\nu+1)}$, and therefore by (25) we obtain

$$[p^{(\alpha+\nu+1)} + (rt_\nu)^{(\alpha+\nu+1)}]\, q^{(\beta)} \equiv r^{(\gamma)}[(t_\nu q)^{(\delta+\nu+1)} + s^{(\delta+\nu+1)}].$$

Since $q^{(\beta)}$, $r^{(\gamma)} \notin T$ we can use the previous lemma and obtain a polynomial which is 0 or homogeneous of degree $\alpha + \nu + 1 - \gamma = \epsilon + \nu + 1$ such that, if we denote it by $t^{(\epsilon+\nu+1)}$, then

$$p^{(\alpha+\nu+1)} + (rt_\nu)^{(\alpha+\nu+1)} \equiv r^{(\gamma)}t^{(\epsilon+\nu+1)}; \qquad t^{(\epsilon+\nu+1)}q^{(\beta)} \equiv (t_\nu q)^{(\delta+\nu+1)} + s^{(\delta+\nu+1)}.$$

Now, for $t_{\nu+1} = t_\nu + t^{(\epsilon+\nu+1)}$ we obtain

$$p^{(\alpha+\nu+1)} \equiv r^{(\gamma)}t^{(\epsilon+\nu+1)} + (rt_\nu)^{(\alpha+\nu+1)} \equiv (rt_{\nu+1})^{(\alpha+\nu+1)}$$

and similarly,

$$(t_{\nu+1}q)^{(\delta+\nu+1)} \equiv s^{(\delta+\nu+1)},$$

which proves (24) for $t_{\nu+1}$ replacing t_ν and $\mu = \nu + 1$; but for $\mu < \nu + 1$,

$$p^{(\alpha+\mu)} \equiv (rt_\nu)^{(\alpha+\mu)} = (rt_{\nu+1})^{(\alpha+\mu)}$$

and also

$$(t_{\nu+1}q)^{(\delta+\mu)} \equiv s^{(\delta+\mu)}$$

and this completes the induction.

From the previous theorem and Doss' result [*2*] it follows that $\mathscr{R}^*$ is embeddable in a group if $n \geqslant 3$, and since R^* is embeddable in $\mathscr{R}^*$ we have:

THEOREM 23. *If $n \geqslant 3$, then R^* is embeddable in a group.*

In Theorem 1 we have proved that if $k \geqslant n$, then R cannot be embedded in a field. Thus, Theorem 1 together with Theorem 23 give our main result which is:

THEOREM 24. *If $k \geqslant n$ and $n \geqslant 3$, then the ring R cannot be embedded in a field, but the multiplicative semigroup R^* is embeddable in a group.*

Finally we note that if $n = 2$ and $k \geqslant 2$, then R^* cannot be embedded in a group. It suffices to show that R^* does not satisfy the following necessary condition for a semigroup to be embeddable in a group, given by Malcev [*4*]:

If $a, b, c, d, a', b', c', d'$ are elements of a semigroup that can be embedded in a group and if

$$aa' = bb', \qquad ac' = bd', \qquad ca' = db', \qquad \text{then} \qquad cc' = dd'.$$

Let us denote the elements of $A^k \in P_2$ by w_{ij} and let

$$a = \bar{w}_{11}, \qquad b = \bar{w}_{12}, \qquad c = \overline{x_1^2}, \qquad d = \overline{x_1x_2},$$

$$a' = \bar{w}_{11}, \qquad b' = \bar{w}_{21}, \qquad c' = \overline{x_1^2}, \qquad d' = \overline{x_2x_1}.$$

$w_{11}w_{11} + w_{12}w_{21}$ is the (1, 1) entry of A^{2k} and therefore belongs to T (which is generated by the entries of A^{k+1}). Hence,

$$aa' = \overline{w_{11}w_{11}} = \overline{w_{12}w_{21}} = bb'.$$

Since $A \cdot A^k = A^{k+1} = A^k \cdot A$ we obtain

$$x_1^2w_{11} + x_1x_2w_{21} = z_{11} \in T \qquad \text{and} \qquad w_{11}x_1^2 + w_{12}x_2x_1 = z_{11} \in T.$$

Hence,

$$ca' = \overline{x_1^2w_{11}} = \overline{x_1x_2w_{21}} = db'; \qquad ac' = \overline{w_{11}x_1^2} = \overline{w_{12}x_2x_1} = bd'.$$

T does not contain polynomials of degree $< 2k + 2$ and in particular, since $k \geqslant 2$, it does not contain $x_1^4 + x_1x_2^2x_1$ which is of degree $4 < 2k + 2$. Hence $\overline{x_1^4} \neq \overline{x_1x_2^2x_1}$ and therefore $cc' \neq dd'$.

Thus, in R^* we have $aa' = bb'$, $ac' = bd'$, $ca' = db'$, but $cc' \neq dd'$ and therefore R^* cannot be embedded in a group.

ACKNOWLEDGMENT

The author wishes to thank Professor Amitsur for his remarks and help in the preparation of this work.

References

1. Cohn, P. M. "Universal Algebra." Harper & Row, New York, 1965.
2. Doss, R. Sur l'immersion d'un semi-groupe dans un groupe. *Bull. Sci. Math.* **72** (1949), 139-150.
3. Kurosh, A. G. "Lectures on General Algebra." Chelsea, New York, 1963.
4. Mal'cev, A. I. On the immersion of an algebraic ring into a field. *Math. Ann.* **113** (1937), 686-691.
5. Mal'cev, A. I. Über die Einbettung von assoziativen Systemen in Gruppen. *Math. Sb.* **6** (1939), 331-336.