AN ALTERNATIVE APPROACH TO THE STRUCTURE THEORY OF PI-RINGS

MATEJ BRESAR

Abstract. We expose a rather simple and direct approach to the structure theory of prime PI-rings ("Posner’s theorem"), based on fundamental properties of the extended centroid of a prime ring.

1. Introduction

The theory of rings with polynomial identities originated in Kaplansky’s 1948 paper [6], in which he showed that a primitive PI-algebra is finite-dimensional over its center. In 1960 Posner [9] extended this theorem to the prime ring context; he proved that a prime PI-ring has a two-sided classical ring of quotients which is a finite-dimensional central simple algebra. After the discovery of central polynomials on matrix algebras in the early 1970’s, Posner’s theorem was further improved by noticing (by different authors, cf. [11]) that this ring of quotients is actually the algebra of central quotients.

A standard proof of this sharpened version of Posner’s theorem, which can be found in several graduate algebra textbooks (e.g., in [1, 8, 12]), is a beautiful illustration of the power and applicability of the classical structure theory of rings. Its main ingredients are the Jacobson density theorem, the theorem by Nakayama and Azumaya on maximal subfields of division algebras, Amitsur’s theorem on the Jacobson radical of the polynomial ring, the nonexistence of nonzero nil ideals in semiprime PI-rings, and the existence of central polynomials on matrices. The first two theorems are needed for the proof of Kaplansky’s theorem, which is an intermediate step in this standard proof of Posner’s theorem.

The purpose of this paper is to give a more streamlined proof, which in each of its steps avoids representing elements in our rings as matrices or linear operators. All aforementioned ingredients are replaced by a single theorem (Theorem 2.1) describing one of the basic properties of the extended centroid of a prime ring. This theorem is essentially due to Martindale [7], and is one of the cornerstones in the theory of generalized polynomial identities [2] as well as in the theory of functional identities [4]. Our proof is in fact more typical for these two theories than for the PI theory. We have to point out, however, that the idea to use such an approach is not entirely new. Already in [7] Martindale noticed that Posner’s theorem can be derived from his result on generalized polynomial identities in prime rings (see also [2]). But the proof of the latter is not so easy. Focusing only on polynomial identities, but hiddenly regarding them as generalized polynomial and functional identities, we will be able to get a rather simple and straightforward proof.

Section 2 surveys the prerequisites needed for our proof. In Section 3 we study identities in central simple algebras, and in particular prove Kaplansky’s theorem for them. This weak version of Kaplansky’s theorem is our intermediate step which, as we show in Section 4, quickly yields the final result.


Supported by the Slovenian Research Agency (program No. P1-0288).
2. Preliminaries

The purpose of this section is to make this paper accessible to non-specialists. It is divided into two parts. In the first one we review the properties of the extended centroid and related notions, and in the second one we give an elementary introduction to polynomial identities.

2.1. The extended centroid. Let $R$ be a prime ring, i.e., a ring in which the product of two nonzero ideals is always nonzero. Then one can construct the symmetric Martindale ring of quotients $Q = Q_s(R)$ of $R$, which is, up to isomorphism, characterized by the following four properties:

(a) $R$ is a subring of $Q$;
(b) for every $q \in Q$ there exists a nonzero ideal $I$ of $R$ such that $qI \cup IQ \subseteq R$;
(c) if $I$ is a nonzero ideal of $R$ and $0 \neq q \in Q$, then $qI \neq 0$ and $IQ \neq 0$;
(d) if $I$ is a nonzero ideal of $R$, $f : I \to R$ is a right $R$-module homomorphism, and $g : I \to R$ is a left $R$-module homomorphism such that $xf(y) = g(x)y$ for all $x, y \in I$, then there exists $q \in Q$ such that $f(y) = qy$ and $g(x) = xq$ for all $x, y \in I$.

The center $C$ of $Q$ is called the extended centroid of $R$. It is a field containing the center $Z$ of $R$. We remark that $Z$ has no zero divisors, and therefore, provided it is nonzero, one can form its field of fractions. This is a subfield of $C$; examples where it is a proper subfield can be easily constructed. We may consider $Q$ as an algebra over $C$. A subalgebra of special importance is the so-called central closure of $R$, which we denote by $RC$. It consists of elements of the form $\sum \lambda_i r_i$, where $\lambda_i \in C$ and $r_i \in R$. Both $Q$ and $RC$ are prime rings. The extended centroid of $RC$ is just $C$. The same is true for every nonzero ideal of $RC$ (as well as of $R$). If $C \subseteq RC$, then $C$ is the center of $RC$.

The main property of $C$ that we need is given in the following theorem. Its original version was proved by Martindale in [7]. The version that we state is, as one can see from [4, Theorem A.4], a special case of [4, Theorem A.7].

**Theorem 2.1.** Let $R$ be a prime ring with extended centroid $C$, and let $I$ be a nonzero ideal of $R$. Assume that $a_1, b_1, c_j, d_j \in Q_s(R)$ satisfy $\sum_{i=1}^n a_i x b_i = \sum_{j=1}^n c_j x d_j$ for all $x \in I$. If $a_1, \ldots, a_n$ are linearly independent over $C$, then each $b_i$ is a linear combination of $d_1, \ldots, d_m$.

Proving Theorem 2.1 as well as all other facts about $C$ and $Q$ mentioned above, is neither difficult nor lengthy; it is also entirely self-contained, and can be easily incorporated into a course on noncommutative rings. See [2, Chapter 2] for a detailed, and [4, Appendix A] for a more informal survey on this subject.

If $R$ is a simple ring with 1, then it follows easily from (a)-(c) that $R = Q$ and hence $C$ is the center of $R$. We may regard every such ring as a central simple algebra (recall that an algebra over a field is said to be central if its center consists of scalar multiples of 1). Our central simple algebras may be infinite-dimensional.

2.2. Polynomial identities. Let $C$ be a field, and let $C(X_1, X_2, \ldots)$ be the free algebra over $C$ generated by the indeterminates $X_i$, $i = 1, 2, \ldots$. One can view elements in $C(X_1, X_2, \ldots)$ as polynomials in noncommuting indeterminates $X_i$. The degree of such a polynomial is defined in a self-explanatory manner. Let $A$ be an algebra over $C$ and let $f = f(X_1, \ldots, X_n) \in C(X_1, X_2, \ldots)$. We say that $f$ is an identity of $A$ if $f(a_1, \ldots, a_n) = 0$ for all $a_i \in A$. If $f \neq 0$, then $f$ is called a polynomial identity of $A$. We say that $f$ is a PI-algebra if there exists a polynomial identity of $A$.

An element in $C(X_1, X_2, \ldots)$ of the form

$$\sum_{\pi \in S_m} \alpha_\pi X_{\pi(1)} \cdots X_{\pi(m)}, \quad \alpha_\pi \in C,$$

is called a monomial. Monomials form a basis for $C(X_1, X_2, \ldots)$, and the above theorem can be restated as follows:

**Corollary 2.2.** Let $C$ be a field, and let $A$ be a PI-algebra over $C$. Then $A$ has a polynomial identity.

This is the classical polynomial identity theorem of Amitsur and Levitzki.
Theorem 2.1 considers two elements in $M$. Since we will be interested only in prime rings, we give just the definition adjusted to our special setting. Tindale’s theorem on prime GPI-rings [7, Theorem 2]. However, we consider only results: Kaplansky’s theorem on primitive PI-algebras [6, Theorem 1] and Martindale’s theorem on prime GPI-rings [7, Theorem 2].

Accordingly, if we are interested only in the structural properties of a PI-algebra, we may confine ourselves to the study of multilinear polynomials. A commutative algebra satisfies the polynomial identity $St_{2} = [X_{1}, X_{2}]$. Next, every finite-dimensional algebra is a PI-algebra. Namely, if $\dim_{C} A = m$ then $A$ satisfies $St_{m+1}$. Another important class of PI-algebras is provided by the Amitsur-Levitzki theorem: If $R$ is any (possibly infinite-dimensional) commutative algebra, then $St_{2n}$ is a polynomial identity of the matrix algebra $A = M_{n}(R)$.

Now let $R$ be “merely” a ring. One can then consider identities of $R$ as elements in $\mathbb{Z}(X_{1}, X_{2}, \ldots)$. However, some care is needed in defining when $R$ is a PI-ring. Some trivial polynomials, such as $p_{X}$ if $R$ has characteristic $p$, must be excluded. Since we will be interested only in prime rings, we give just the definition adjusted to this context: a prime ring $R$ is said to be a PI-ring if a nonzero polynomial in $C(X_{1}, X_{2}, \ldots)$, where $C$ is the extended centroid of $R$, is an identity of $R$. An illustrative example is $R = M_{n}(\mathbb{Z})$. It satisfies $St_{2n}$, so is a prime PI-ring. Its extended centroid is isomorphic to $\mathbb{Q}$, and its central closure is isomorphic to $M_{n}(\mathbb{Q})$.

Everything said so far about polynomial identities is the most standard material that can be found in numerous textbooks.

3. Central simple PI-algebras

The goal of this section is to prove a proposition that combines two well-known results: Kaplansky’s theorem on primitive PI-algebras [6, Theorem 1] and Martindale’s theorem on prime GPI-rings [7, Theorem 2]. However, we consider only simple algebras in our proposition. The novelty is a simple proof, adjusted to this special setting.

Let $A$ be an algebra. For $a, b \in A$ we define $L_{a}, R_{b} : A \to A$ by $L_{a}(x) = ax$, $R_{b}(x) = xb$. Obviously, $L_{a}R_{b} = R_{b}L_{a}$. The set $M(A)$ of all operators of the form $\sum L_{a_{i}}R_{b_{i}}, a_{i}, b_{i} \in A$, forms a subalgebra of the algebra $\text{End}_{C}(A)$ of all linear operators on $A$. We call $M(A)$ the multiplication algebra of $A$. We remark that Theorem [2,1] considers two elements in $M(Q_{s}(R_{C}))$.

Proposition 3.1. Let $A$ be a central simple algebra over a field $C$. The following conditions are equivalent:

(i) $A$ is a PI-algebra;
(ii) $M(A)$ contains a nonzero finite rank operator;
(iii) $\dim_{C} A < \infty$;
(iv) $M(A) = \text{End}_{C}(A)$.

Proof. (i)$\Rightarrow$(ii). Let $f = f(X_{1}, \ldots, X_{n})$ be a multilinear polynomial identity of $A$. Pick $1 \leq i < j \leq n$, and write $f = f_{i} + f_{j}$ where $f_{i}$ is the sum of all monomials of $f$ of the form $mX_{i}m'X_{j}m''$, and $f_{j}$ is the sum of all monomials of $f$ of the form $nX_{i}n'X_{j}n''$ (here, of course, $m, m', \ldots$ are monomials in the other variables). Suppose that both $f_{i}$ and $f_{j}$ are identities of $A$. Since $f \neq 0$, we have $f_{i} \neq 0$ or $f_{j} \neq 0$. Without loss of generality we may assume that $f_{i} \neq 0$. Now we may replace the role of $f$ by $f_{i}$, and hence assume that $X_{i}$ appears before $X_{j}$ in all monomials of $f$. Since $X_{1}X_{2}\ldots X_{n}$ is not an identity of $A$, there exists a pair $1 \leq i < j \leq n$ such that $f_{i}$ and $f_{j}$ are not identities of $A$. We may assume that $i = 1$ and $j = 2$. 

where $S_{m}$ is the symmetric group of degree $m$, is called a multilinear polynomial. Especially important examples are the so-called standard polynomials in which $\alpha_{n}$ is defined as the sign of the permutation $\pi$. The standard polynomial of degree $m$ will be denoted by $St_{m}$. The simplest example of a polynomial that is not multilinear is $X_{1}^{2}$. However, if this polynomial is an identity of $A$, then so is the multilinear polynomial $X_{1}X_{2} + X_{2}X_{1} = (X_{1} + X_{2})^{2} - X_{1}^{2} - X_{2}^{2}$. Somewhat more tedious, but based on the same simple idea, is to prove that if $A$ satisfies a polynomial identity of degree $n$, then it also satisfies a multilinear polynomial identity of degree $\leq n$. Hence, we may confine ourselves to the study of multilinear polynomials.

Everything said so far about polynomial identities is the most standard material that can be found in numerous textbooks.
Fix $u_i \in A$ such that $f_1(u_1, \ldots, u_n) \neq 0$. The identity $f_1(x, y, u_1, \ldots, u_n) = -f_2(x, y, u_3, \ldots, u_n)$ for all $x, y \in A$ can be rewritten as a (functional) identity

$$
(1) \quad \sum_{i=1}^r a_i x T_i(y) = \sum_{j=1}^s S_j(y) x d_j \quad \text{for some } T_i, S_j \in M(A), a_i, d_j \in A.
$$

Since both sides of (1) are nonzero if we take $x = u_1$ and $y = u_2$, some of the $a_i$'s are nonzero. Without loss of generality we may assume that $\{a_1, \ldots, a_r\}$, $t \leq r$, is a maximal linearly independent subset of $\{a_1, \ldots, a_r\}$. Expressing the $a_i$'s with $i > t$ through the $a_i$'s with $i \leq t$ we see that (1) can be rewritten as

$$
(2) \quad \sum_{i=1}^t a_i x W_i(y) = \sum_{j=1}^s S_j(y) x d_j \quad \text{for some } W_i, S_j \in M(A), a_i, d_j \in A.
$$

Of course, some of the $W_i$'s are nonzero; we may assume that $W_1$ is one of them. Now, for any fixed $y \in A$ we infer from (2) and Theorem 2.1 that $W_1(y)$ lies in the linear span of $d_1, \ldots, d_s$. Thus, (ii) holds.

(ii)⇒(iii). Let $W = \sum_{i=1}^n L_i R_i$ be a nonzero finite rank operator in $M(A)$. Picking a maximal linearly independent subset of $\{a_1, \ldots, a_n\}$ and expressing the other $a_i$'s as linear combinations of elements from this set, we see that there is no loss of generality in assuming the linear independence of $\{a_1, \ldots, a_n\}$. We may also assume that $b_1 \neq 0$. The proof is by induction on $n$.

Let $n = 1$. Since $A$ is simple, there exist $u_j, v_j, w_k, z_k \in A$ such that $\sum_j u_j a_1 v_j = \sum_j w_k a_1 z_k = 1$. Consequently, $\sum_{j,k} L_{ij} R_{jk} W L_{ij} R_{jk}$ is the identity operator, and is of finite rank. But this means that $\dim_C A < \infty$.

Now let $n > 1$. We will just repeat the appropriate argument from [7]. If each $b_i$, $i \geq 2$, is a scalar multiple of $b_1$, then we are back to the $n = 1$ case. We may therefore assume that $b_2$ and $b_1$ are linearly independent. By Theorem 2.1 there exists $c \in A$ such that $b_1 c b_2 \neq b_2 c b_1$. Define $W' \in M(A)$ by $W' = W b_2 c - R_{cb} W$. Obviously, $W'$ has finite rank, and note that $W' = \sum_{i=1}^n L_i R_i$, where $c_1 = b_1 c b_1 - b_2 c b_1$. Since $a_2, \ldots, a_n$ are linearly independent and $c_2 \neq 0$, Theorem 2.1 shows that $W' \neq 0$. By induction the proof is complete.

(iii)⇒(iv). Let $\{a_1, \ldots, a_n\}$ be a basis of $A$. Suppose $\lambda_{ij} \in C$ are such that $\sum_{i,j} \lambda_{ij} L_i R_{ij} = 0$. Rewriting this as $\sum_{i=1}^n L_i (\sum_{j=1}^n \lambda_{ij} R_{ij}) = 0$ we see by using Theorem 2.1 that $\sum_{j=1}^n \lambda_{ij} R_{ij} = 0$, which in turn yields $\lambda_{ij} = 0$ for all $i, j$. Therefore $\dim_C M(A) = n^2 = \dim_C \text{End}_C(A)$, and so $M(A) = \text{End}_C(A)$.

Since (iii)⇒(i) and (iv)⇒(ii) are trivial, this completes the proof. □

Remark 3.2. The first step in the standard proof of Kaplansky’s theorem is the reduction to the case where the algebra in question is a division algebra. This can be done quite easily by applying the Jacobson density theorem. Proposition 5.1 of course covers division algebras, so we now have a new proof of Kaplansky’s theorem that does not use the theorem on maximal subfields of division algebras.

Remark 3.3. The proof of (i)⇒(ii) is also applicable to generalized polynomial identities. Explaining this in detail would make this paper, which is intended for a wider audience, too technical. Therefore we will just give a few comments that should be sufficient for specialists. Let $f$ be a multilinear generalized polynomial identity of degree $n \geq 2$ of a prime ring $R$ (in the sense of [2]). Fixing all variables except two, we arrive at (1). The only problem is to show that we can choose the two non-fixed variables in such a way that both sides of (1) are not identically zero. We argue as in the first paragraph of the (i)⇒(ii) proof, and in that way we arrive at a generalized polynomial identity $\sum_i a_0 x_1 a_{11} x_2 a_{22} \ldots x_{n-1} a_{nn}$ (instead of $X_1 X_2 \ldots X_n$). But using Theorem 2.1 this identity can be easily handled. Therefore we may assume (1) with both sides nonzero. Repeating the above argument leads us
to the situation where [2] Lemmas 6.1.2 and 6.1.4] can be used to prove Martindale’s
characterization of prime GPI-rings [2 Theorem 6.1.6].

It seems that the proof that we outlined is somewhat simpler than the one given
in [2 pp. 216-217].

4. Prime PI-rings

We are now in a position to prove the ultimate version of Posner’s theorem.

**Theorem 4.1.** If $R$ is a prime PI-ring with extended centroid $C$, then:

(a) its central closure $R_C$ is a finite-dimensional central simple algebra over $C$;
(b) every nonzero ideal of $R$ intersects the center $Z$ of $R$ nontrivially;
(c) $C$ is the field of fractions of $Z$;
(d) every element in $R_C$ is of the form $z^{-1}r$ with $0 \neq z \in Z$, $r \in R$.

**Proof.** (a) Let $U$ be a nonzero ideal of $R_C$. Since $R_C$ is a prime PI-ring (namely, it
clearly satisfies the same multilinear identities as $R$), so is $U$. Let $f = f(X_1, \ldots, X_n)$
be a multilinear polynomial identity of $U$ of minimal degree $n$. Write

$$f = gX_n + \sum_i g_iX_nh_i$$

where each $h_i$ is a monomial of degree $\geq 1$ and with leading coefficient 1, and $g$
and $g_i$ are multilinear polynomials. Without loss of generality we may assume that
$g \neq 0$. As the degree of $g$ is $n-1$, $g$ is not an identity of $U$. Pick $u_1, \ldots, u_{n-1} \in U$ so
that $u = g(u_1, \ldots , u_{n-1}) \neq 0$. We have $uXf = uz = \sum v_iwx_i$ for some
$v_i \in RC + C$, $w_i \in U$ and all $x \in U$. Theorem 2.1 implies that 1 lies in the $C$-linear span of the
$w_i$’s. This in particular shows that 1 lies in $R_C$, hence $C \subseteq R_C$, and so $1 \in \sum CW_i \subseteq U$.
Thus $R_C$ is a simple algebra over its center $C$. Proposition 5.1 tells us that it is
finite-dimensional.

(b) Let $\varphi$ be a nonzero $C$-linear functional on $R_C$. In view of (iv) in Proposition
5.1 there exists $T \in M(R_C)$ such that $T(x) = \varphi(x)1$ for all $x \in A$. Let $p_i, q_i \in R_C$
be such that $T = \sum_{i=1}^n L_{p_i}R_{q_i}$, $q_i \neq 0$, and $p_1, \ldots, p_n$ are linearly independent
(the latter can indeed be required, since otherwise we can pick a maximally linearly
independent subset of the $p_i$’s and then rewrite $T$ in an appropriate way). Let $J_i$
and $K_i$ be nonzero ideals of $R$ such that $p_iJ_i \subseteq R$ and $K_iq_i \subseteq R$. Now pick any
nonzero ideal $I$ of $R$. Then, since $R$ is prime, $I' = (J_i\cap \ldots \cap J_n)I(K_i\cap \ldots \cap K_n)$ is
again a nonzero ideal of $R$, and note that $T(I') \subseteq I \cap C$. Theorem 2.1 shows that
$T(I') \neq 0$, and so $I \cap C \neq 0$. Since $I \subseteq R$ we actually have $I \cap C = I \cap Z$.

(c) Let $\lambda \in C$. Take a nonzero ideal $I$ of $R$ such that $\lambda I \subseteq R$. Picking $0 \neq z \in$I \cap Z, we thus have $\lambda z \in R \cap C = Z$. Therefore $\lambda = z^{-1}z'$ with $z, z' \in Z$.

(d) Use a common denominator. \hfill \Box

**Remark 4.2.** A well known result by Rowen [11] says that (b) holds even for
semiprime PI-rings. The standard proof is based on central polynomials. Using
this tool - more precisely, we need the existence of a multilinear central polynomial
with integer coefficients on a finite-dimensional central simple algebra - one can
also derive this more general result by using our approach. Basically one just has
to follow Rowen’s argument, which, however, can be simplified by omitting the reduction
to the semiprimitive case. Namely, in view of (a) we may deal with subdirect
products of prime rings instead of primitive ones.

Let us point out that we have also used some sort of “central polynomials” in the
proof of (b). However, instead of usual polynomials we have dealt with a generalized
polynomial $\sum_{i=1}^n p_iQq_i$. As we saw, proving that such a “polynomial” can have only
central values is fairly easy. This cannot be said for the proof of the existence of
the usual central polynomials.
Remark 4.3. The fact that in our proof we have avoided using the existence of central polynomials on matrix algebras \cite{5,10}, makes it possible for us to obtain a new proof of that. Indeed, one just has to use (b) to conclude that the algebra of generic $n \times n$ matrices (which is easily seen to be a prime PI-ring \cite{12} Corollary 23.52) has a nonzero center; cf. \cite{3} p.324).

Acknowledgement. The author would like to thank Amiram Braun and Louis Rowen for drawing his attention to \cite{3}, and to Igor Klep and Špela Špenko for useful remarks.

References


Faculty of Mathematics and Physics, University of Ljubljana, and Faculty of Natural Sciences and Mathematics, University of Maribor, Slovenia

E-mail address: matej.bresar@fmf.uni-lj.si