Canad. Math. Bull. Vol. **41** (1), 1998 pp. 81–85

# THE CARDINALITY OF THE CENTER OF A PI RING

CHARLES LANSKI

ABSTRACT. The main result shows that if $R$ is a semiprime ring satisfying a polynomial identity, and if $Z(R)$ is the center of $R$, then $\operatorname{card} R \leq 2^{\operatorname{card} Z(R)}$. Examples show that this bound can be achieved, and that the inequality fails to hold for rings which are not semiprime.

The purpose of this note is to compare the cardinality of a ring satisfying a polynomial identity (a PI ring) with the cardinality of its center. Before proceeding, we recall the definition of a central identity, a notion crucial for us, and a basic result about polynomial identities. Let $C$ be a commutative ring with 1, $F\{X\} = C\{x_1, \ldots, x_n\}$ the free algebra over $C$ in noncommuting indeterminates $\{x_i\}$, and set $G = \big\{f(x_1, \ldots, x_n) \in F\{X\} \mid \text{some coefficient of } f \text{ is a unit in } C\big\}$. If $R$ is an algebra over $C$, then $f(x_1, \ldots, x_n) \in G$ is a polynomial identity (PI) for $R$ if for all $r_i \in R$, $f(r_1, \ldots, r_n) = 0$. The standard identity of degree $n$ is $S_n(x_1, \ldots, x_n) = \sum_\sigma (-1)^{sg\sigma} x_{\sigma(1)} \cdots x_{\sigma(n)}$ where $\sigma$ ranges over the symmetric group on $n$ letters. The Amitsur-Levitzki theorem is an important result about $S_n$ and shows that $M_k(C)$ satisfies $S_n$ exactly for $n \geq 2k$ [5; Lemma 2, p. 18 and Theorem, p. 21]. Call $f \in G$ a *central identity* for $R$ if $f(r_1, \ldots, r_n) \in Z(R)$, the center of $R$, for all $r_i \in R$, but $f$ is not a polynomial identity. One can obtain a trivial example of a central identity by adding a polynomial identity to a fixed element from $Z(R)$. A result with major consequences for the theory of PI rings was the proof of the existence of nonconstant central identities for matrix rings $M_n(F)$ by E. Formanek [1]. One among the many important applications of this work was a result of L. Rowen [6] showing that any nonzero ideal in a semiprime PI ring must intersect the center of the ring nontrivially. Thus, for a semiprime PI ring, there is an important and interesting relationship between the ring and its center. In particular, the center cannot be too small. A natural and intriguing question which arises is how small the center can be relative to the size of the ring? When $R$ is a prime PI ring with center $Z(R)$, then $R$ and $Z(R)$ have the same cardinality unless $R$ is finite. This follows from a theorem of E. Formanek [2; Theorem 1, p. 79], which uses Rowen's result and shows that when $R$ is a prime PI ring, the $Z(R)$ module $R$ embeds in a free $Z(R)$ module of finite rank. Another approach is to observe that if $S$ is the central localization of $R$ at $Z(R) - (0)$, then $S$ is a finite dimensional (simple) algebra over the quotient field of $Z(R)$ [5; Theorem 2, p. 57]. For future reference we record this observation as a theorem. Denote the cardinality of $S$ by $|S|$.

Received by the editors June 26, 1996.
AMS subject classification: Primary: 16R20; secondary: 16N60, 16R99, 16U50.
© Canadian Mathematical Society 1998.



https://doi.org/10.4153/CMB-1998-013-2 Published online by Cambridge University Press

THEOREM A. *If $R$ is a prime* PI *ring then either $R$ is finite or $|R| = |Z(R)|$.*

We shall need to refer to the theorem of L. Rowen [6; Theorem 2, p. 221] mentioned above, so we state it for convenience.

THEOREM B. *If $R$ is a semiprime* PI *ring and $I \neq 0$ is an ideal of $R$ then $I \cap Z(R) \neq 0$.*

We begin with some examples, the first of which is easy and shows that when $R$ is not semiprime, no particular relation exists between $|R|$ and $|Z(R)|$, except for $|Z(R)| \leq |R|$.

EXAMPLE 1. Let $1 < \alpha < \beta$ be cardinal numbers with $\beta$ infinite, $F$ a field with $|F| \leq \alpha$, and $X$ a set of commuting indeterminates over $F$ with $|X| = \beta$. Then $R = \begin{bmatrix} F & F[X] \\ 0 & F \end{bmatrix} \subseteq M_2(F[X])$ satisfies the standard identity $S_4$, $Z(R) = F \cdot I_2$, so $|Z(R)| \leq \alpha < \beta = |R|$.

If the ring $R$ in Example 1 satisfies a central identity, then by linearization it satisfies one which is additive in each variable. Substituting elements from $\{Fe_{11}, F[X]e_{12}, Fe_{22}\}$ into this central identity shows that it must be a PI for $R$. Thus, $R$ satisfies no central identity. We present another less obvious, but still easy example which satisfies a nonconstant central identity.

EXAMPLE 2. Again let $2 < \alpha < \beta$ be cardinal numbers with $\beta$ infinite, $F$ a field with char $F \neq 2$, $|F| \leq \alpha$, and $V = \{v_i \mid i \in W\}$, $Y = \{y_i \mid i \in W\}$, and $\{z\}$ disjoint sets of noncommuting indeterminates over $F$ with $|W| = \beta$. Let $H$ be the ideal of the free algebra $F\big\{V \cup Y \cup \{z\}\big\}$ generated by $v_iy_i - z$ and $y_iv_i + z$, for all $i \in W$, and all other products of two elements from $V \cup Y \cup \{z\}$ except for $\{v_iy_i \text{ and } y_iv_i \mid i \in W\}$. If $R$ is the quotient $F\big\{V \cup Y \cup \{z\}\big\}/H$, then by identifying indeterminates with their images, consider $R = F + Fz + \sum_W Fv_i + \sum_W Fy_i$. Note that, $Fz + \sum_W Fv_i + \sum_W Fy_i$ is an ideal of $R$ whose cube is zero because all its products are zero except that $v_iy_i = z$ and $y_iv_i = -z$, for all $i \in W$. Now $|R| = \beta$, $Z(R) = F + Fz$ is finite or $|Z(R)| \leq \alpha$ when $\alpha$ is infinite, $uv - vu \in Z(R)$ for all $u, v \in R$, and $v_iy_i - y_iv_i = 2z \neq 0$. Therefore, $R$ satisfies the central identity $[x_1, x_2] = x_1x_2 - x_2x_1$, and the PI$\big[[x_1, x_2], x_3\big]$.

In view of these examples and Theorem A, only semiprime PI rings which are not prime are left for consideration. Here the situation is not as clear as for prime rings since $|Z(R)| < |R|$ can hold when $Z(R)$ is infinite, as our next example shows.

EXAMPLE 3. Let $\beta$ be an infinite cardinal, $C$ a commutative semiprime ring with $|C| = \beta$, $I$ a set with $|I| = \beta$, and $k > 1$ an integer. Set $H = \prod_I M_k(C) = M_k(C)^I$, the complete direct product of $\beta$ copies of $M_k(C)$. Fix a nonzero subring $S \subset M_k(C)$ so that $S \cap Z\big(M_k(C)\big) = (0)$ and let $R = \{h: I \longrightarrow M_k(C) \mid h(i) \in S$ for all but finitely many $i \in I\}$ with pointwise addition and multiplication; that is, $R$ consists of all elements in $\prod_I M_k(C)$ having finitely many coordinates arbitrary in $M_k(C)$ and all other coordinates in $S$. To see that $R$ is a semiprime ring let $h \in R$ with $h(i) \neq 0$ and observe that $(hRh)(i) = h(i)M_k(C)h(i) \neq 0$, since $C$ a semiprime ring forces $M_k(C)$ to be semiprime. Using $S \cap Z\big(M_k(C)\big) = (0)$, it is easy to see that $Z(R) \cong \oplus_I C$, and so $|Z(R)| = \beta$. Finally, $|R| \leq |M_k(C)^I| = \beta^\beta = 2^\beta$, and in fact $|R| = 2^\beta$, because $2^\beta \leq |S^I| \leq \beta^\beta = 2^\beta$ and there is an

https://doi.org/10.4153/CMB-1998-013-2 Published online by Cambridge University Press

obvious inclusion of $S^I$ into $R = M_k(C)^I$. Note that although $|Z(R)| = \beta$ and ideals of $R$ intersect $Z(R)$, $R$ has $2^\beta$ different ideals defined by the subsets $A$ of $I$ as $T(A) = \{r \in R \mid r(i) = 0 \text{ for all } i \in A\}$. For a specific example one could let $C = F$, a field, or $C = F_p[X]$, and let $S = Ce_{11}$, or $S = Ce_{12}$. The same construction for $C$ finite and $I$ countable yields $R$ uncountable with $Z(R)$ countable.

Our first result for finite centers is presumably well known, but we could not locate it specifically in the literature. Its proof is easy and it will be convenient to have the result, so we present it.

THEOREM 1. *If $R$ is a semiprime* PI *ring with finite center, then $R$ is finite.*

PROOF. Since $R$ is a semiprime ring, $Z(R)$ is a finite commutative ring with no nonzero nilpotent elements, so $Z(R)$ is a direct sum of finite fields. Let $Z(R) = Z = Ze_1 \oplus \cdots \oplus Ze_k = Ze$, where $e = 1_z$ and $\{e_i\}$ are minimal orthogonal idempotents in $Z$ whose sum is $e$. Therefore, $R = Re \oplus R(1-e)$, where $R(1-e) = \{r - re \mid r \in R\}$, and $Z(R) \cap R(1-e) = 0$. But $R(1-e)$ is an ideal of $R$ and $Z\big(R(1-e)\big) = Z(R) \cap R(1-e)$, so by Theorem B, $R(1-e) = 0$ forcing $e = 1_R$, and it follows that $R = Re_1 \oplus \cdots \oplus Re_k$. Hence, $Re_i$ is a semiprime PI ring with $Z(Re_i) = Ze_i$, a finite field, so Theorem B forces each $Re_1$ to be simple, and so finite by Theorem A, proving that $R$ is finite.

We come to our main result, which shows that Example 3 illustrates the largest difference which can occur between $|Z(R)|$ and $|R|$, for $R$ a semiprime PI ring. We shall need to know that there is a central identity $g_n(x_1, \ldots, x_k)$ for the matrix ring $M_n(C)$ which has no constant term and is linear in $x_1$ ([1] or [5: p. 45]). The construction of $g_n$ in [1] or [5] shows that for any commutative ring $K$, $g_n$ is not a PI for $M_n(K)$.

THEOREM 2. *If $R$ is a semiprime* PI *ring and $Z(R)$ is infinite, then $|R| \leq 2^{|Z(R)|}$.*

PROOF. There is a natural embedding of $R$ into the direct product of its prime images, each satisfying the same PI as $R$, so a well known result of S. A. Amitsur [5; Lemma 2, p. 55] forces $R$ to satisfy a standard identity $S_{2n}$ for some $n \geq 1$. Let $n$ be minimal so that $R$ satisfies $S_{2n}$. If $R$ satisfies $S_2 = x_1x_2 - x_2x_1$, then $R$ is commutative and $R = Z(R)$, so we may assume that $n > 1$ and proceed by induction on $n$; that is, if $A$ is a semiprime PI ring satisfying $S_{2m}$ for $m < n$, and if $Z(A)$ is infinite, then $|A| \leq 2^{|Z(A)|}$.

Since no nonzero $z \in Z(R)$ is nilpotent, by using Zorn's Lemma one produces an ideal $P_z$ of $R$ maximal with respect to $P_z \cap \{z^i \mid i \geq 1\} = \emptyset$, and it is straightforward to see that $P_z$ is a prime ideal of $R$. It follows from the definition of $P_z$ that $Z(R) \cap (\bigcap_{Z(R)} P_z) = 0$, where $P_0 = R$. But $\bigcap_{Z(R)} P_z$ is an ideal in the semiprime ring $R$, so $Z(\bigcap_{Z(R)} P_z) = 0$ [3; Lemma 1.1.5, p. 6], forcing $\bigcap_{Z(R)} P_z = 0$ by Theorem B, and $R$ embeds naturally in the direct product $\prod_{Z(R)} R/P_z$. Now each $R/P_z$ satisfies $S_{2n}$ and some of these quotients do not satisfy $S_{2(n-1)}$ since $R$ does not. Let $g_n(x_1, \ldots, x_k)$ be a central identity for $M_n(F)$, $F$ a field, where $g_n$ has integer coefficients, one of which is 1, no constant term, is linear in $x_1$, and is not a PI for any $M_n(D)$ where $D$ is a commutative ring ([1] or [5; p. 45]). We argue that $g_n$ is a central identity for $R$. A result of C. Procesi [5; Proposition, p. 43] shows that $g_n$ is a polynomial identity for $M_{n-1}(F)$, so for $M_k(F)$ with $k \leq n-1$, but not

https://doi.org/10.4153/CMB-1998-013-2 Published online by Cambridge University Press

a PI for $M_n(F)$ by choice of $g_n$. If $T$ is any prime ring satisfying a PI $p(x_1,\ldots,x_k)$, then $W = TZ^{-1}$, the localization of $T$ at $Z(T)-(0)$, also satisfies $p(x_1,\ldots,x_k)$ and is a simple algebra, finite dimensional over its center $K$ [5; Theorem 2, p. 57]. Either $W = M_t(K)$ or $W\otimes_K L = M_t(L)$, for $L$ an algebraic closure of $K$, and $W\otimes_K L$ also satisfies $p(x_1,\ldots,x_k)$ [5; Lemma 1, p. 89], so $2t \le \deg p$ by the Amitsur-Levitzki theorem. In our case, if $R/P_z$ satisfies $S_{2(n-1)}$ then it embeds in some $M_{n-1}(F)$ and $g_n$ is an identity for $R/P_z$. If $R/P_z$ does not satisfy $S_{2(n-1)}$ but $g_n$ is an identity for it, then we conclude first that $R/P_z$ does not embed in any $M_k(F)$ for $k < n$ by the Amitsur-Levitzki theorem. Secondly, since $S_{2n}$ and $g_n$ are identities for $R/P_z$, as above, $R/P_z$ embeds in $M_n(F)$, which satisfies the PI $g_n$, contradicting the choice of $g_n$. Therefore, $g_n$ is a central identity or a PI for each $R/P_z$, so a central identity for $R$; it is not a PI for $R$ since it is not a PI for any quotient $R/P_z$ which fails to satisfy $S_{2(n-1)}$.

Choose $z\in Z(R)$ so that $g_n$ is not a PI on $R/P_z$. Writing $r+P_z = \bar r \in R/P_z$, the fact that $g_n$ is a central identity for $R/P_z$ means that there are $\bar r_i \in R/P_z$, so that $g_n(\bar r_i) = \bar c \in Z(R/P_z)-(0)$. For any $\bar y\in Z(R/P_z)$, $\overline{yc} = g_n(\overline{yr_i},\ldots,\bar r_k)$, since $g_n$ is linear in its first variable. But $g_n(\overline{yr}_1,\ldots,\bar r_k) = g_n(yr_1,\ldots,r_k)+P_z$ with $g_n(yr_1,\ldots,r_k)\in Z(R)$, so $\bar c Z(R/P_z) \subseteq \overline{Z(R)}$ and since $Z(R/P_z)$ is a domain, $|Z(R/P_z)| \le |Z(R)|$ results. Applying Theorem A gives $|R/P_z| \le |Z(R)|$. If $I = \{z\in Z(R) \mid g_n \text{ is not a PI of } R/P_z\}$, $J = Z(R) - \big\{I\cup\{0\}\big\}$, $A = \bigcap_I P_z$, and $B = \bigcap_J P_z$, then $A\cap B \subseteq \bigcap_{Z(R)} P_z = 0$, so $R$ embeds in $R/A\oplus R/B$. Now $R/A$ itself embeds in $\prod_I R/P_z$, and as we have just observed, for $z\in I$, $|R/P_z| \le |Z(R)|$. Therefore, $|\prod_I R/P_z| \le |Z(R)|^{|Z(R)|} = 2^{|Z(R)|}$ since $Z(R)$ is infinite. Hence $|R/A| \le 2^{|Z(R)|}$ and the proof is complete when $A=0$.

Assuming that $A\ne 0$, it follows that $A$ embeds in $R/B$ since $A\cap B = 0$, and of course $R/B$ embeds in $\prod_J R/P_z$. For each $z\in J$, $g_n$ is a PI of $R/P_z$, so by our observations above and Procesi's theorem, $R/P_z$ satisfies $S_{2(n-1)}$ which means that $\prod_J R/P_z$ and $R/B$ satisfy $S_{2(n-1)}$. Since $A$ embeds in $R/B$, $A$ is a semiprime ring satisfying $S_{2(n-1)}$. By Theorem 1 and the induction assumption, either $A$ is finite or $|A| \le 2^{|Z(A)|} \le 2^{|Z(R)|}$ since $Z(A)\subseteq Z(R)$ [3; Lemma 1.1.5, p. 6]. Thus $|R| = |R/A|\,|A| \le 2^{|Z(R)|}2^{|Z(R)|} = 2^{|Z(R)|}$ completing the proof of the theorem.

We record a simple consequence of Theorem 2 for algebraic algebras.

THEOREM 3. *Let $R$ be a semiprime ring and algebra over the integral domain $C$. If $R$ is integral over $C$ of bounded degree, then either $R$ is finite or $|R| \le 2^{|Z(R)|}$.*

PROOF. If $R$ is integral over $C$ of bounded degree $n$, then every $r\in R$ satisfies some relation $r^{n+1}+c_nr_n+\cdots+c_1r = 0$. It is well known and straightforward to show that this relation implies that $\{[x^i,y], \mid 1\le i\le n+1\}$ is $C$-dependent for any $x,y\in R$, so that $R$ satisfies the polynomial identity $S_{n+1}([x^{n+1},y],\ldots,[x^2,y],[x,y])$ [4; p. 230]. Applying Theorem 2 finishes the proof.

We note that Example 1 and Example 2 show that if $R$ is not semiprime, then $R$ algebraic of bounded degree over a field does not imply any particular relationship between $|Z(R)|$ and $|R|$. A similar example for semiprime rings is provided by Example 3 when $C=F$, a field, and $S = Fe_{12}$. Our last example shows that the assumption of bounded degree in Theorem 3 is essential, even for prime or simple algebras.

https://doi.org/10.4153/CMB-1998-013-2 Published online by Cambridge University Press

EXAMPLE 4. Let $1 < \alpha < \beta$ be cardinal numbers with $\beta$ infinite, $F$ a field with $|F| \leq \alpha$, and $V_F$ an $F$-vector space with $\dim_F V = \beta$. If $\{v_i \mid i \in I\}$ is an $F$-basis of $V$, for $I$ a well ordered set with $|I| = \beta$, then one can represent the elements of $\mathrm{Hom}_F(V, V)$ as column (or row) finite $\beta \times \beta$ matrices, say $M_\beta(F)$ with matrix units $\{e_{ij} \mid i, j \in I\}$. Set $M_0 = \{A \in M_\beta(F) \mid A$ has only finitely many nonzero entries$\}$, or equivalently, $M_0 = \{T \in \mathrm{Hom}_F(V, V) \mid v_j \in \ker T$ for all but finitely many $j \in I\}$. It is easy to see that $M_0$ is a simple algebraic $F$-algebra with $|M_0| = \beta$, and that $Z(M_0) = 0$. By taking $R = M_0 + F \cdot I_V$, so adding scalar matrices to $M_0$, it follows that $R$ is a prime algebraic algebra over $F$, $|R| = \beta$, and $|Z(R)| = |F| \leq \alpha$.

## REFERENCES


**1.** E. Formanek, *Central polynomials for matrix rings*. J. Algebra **23**(1972), 129–132.

**2.** ———, *Noetherian* PI-*rings*. Comm. Algebra **1**(1974), 79–86.

**3.** I. N. Herstein, *Rings with involution*. Chicago Lectures in Mathematics, University of Chicago Press, Chicago, 1976.

**4.** N. Jacobson, *Structure of rings*. Amer. Math. Soc. Colloq. Publ. **37**, Amer. Math. Soc., Providence, RI, 1964.

**5.** ———, PI-*algebras*. Lecture Notes in Math. **441**, Springer-Verlag, New York, 1975.

**6.** L. Rowen, *Some results on the center of a ring with polynomial identity*. Bull. Amer. Math. Soc. **79**(1973), 219–223.



*Department of Mathematics*
*University of Southern California*
*Los Angeles, CA 90089-1113*
*USA*


https://doi.org/10.4153/CMB-1998-013-2 Published online by Cambridge University Press