Armendariz Rings

By M. B. REGE and Sima CHHAVCHHHARIA

Department of Mathematics, North Eastern Hill University, India

(Communicated by Shokichi IYANAGA. M. J. A., Jan. 13, 1997)

1. Introduction. Let $R$ be a domain (commutative or not) and $R[x]$ its polynomial ring. Let $f(x) = \sum_{i=0}^{m} a_i x^i$, $g(x) = \sum_{j=0}^{n} b_j x^j$ be elements of $R[x]$. (This notation for the coefficients of $f(x)$ and $g(x)$ will be followed in the absence of explicit mention.) It is an elementary exercise to prove that if $f(x) g(x) = 0$, then $a_i b_j = 0$ for every $i$ and $j$. (Of course the converse always holds.)

E. Armendariz ([1], Lemma 1) noted that the above result can be extended to the class of reduced rings, i.e., rings without non-zero nilpotent elements. In order to study additional classes of rings having this property we introduce the following definition.

1.1. Definition. A ring $R$ is said to have the Armendariz property (or is an Armendariz ring) if whenever polynomials $f(x) = \sum_{i=0}^{m} a_i x^i$, $g(x) = \sum_{j=0}^{n} b_j x^j \in R[x]$ satisfy $f(x) g(x) = 0$, we have $a_i b_j = 0$ for every $i$ and $j$.

By a ring we mean an associative ring with unity. However, the assumption of the existence of identity can be omitted in many places. Many remarks are thus valid in the context of non-commutative rings which are Armendariz. However, factor rings need not be so (see 3.3).

We shall also need the following variants of the construction in 1.2.

1.3. Let $R$ be a commutative ring and $h: R \rightarrow R$ a ring homomorphism. Let $M$ be an $R$-module. On modifying the definition in 1.2 to

$$(a, m)(b, n) = (ab, an + bm),$$

we get a (non-commutative) ring structure on $R \oplus M$ which we shall denote by $R(+)M$.

1.4. Let $R$ be a ring and $A$ an ideal of $R$. The factor ring $R = R/A$ has the natural structure of a left $R$, right $R^*$ bimodule. Denote $\tilde{a} = a + A \in \tilde{R}$ for each $a \in R$. We use this structure to define a ring structure on $R \oplus (R/A)$ as follows:

$$(r, \tilde{a})(r', \tilde{a}') = (rr', \tilde{a}r' + ar').$$

We denote this ring by $R(+)R/A$. Its properties are similar to those of $R(+)M$.

2. Rings which have the Armendariz property. It is easy to see that subrings of Armendariz rings are also Armendariz. However, factor rings need not be so (see 3.3). If $(R_i)_{i \in I}$ are Armendariz, so is $\prod R_i$. We begin with examples of familiar non-reduced rings which are Armendariz.

2.1. Proposition. For each integer $n$, $\mathbb{Z}/n\mathbb{Z}$ is an Armendariz ring, which is not reduced whenever $n$ is a natural number which is not square free.

Proof. We first consider the case $n = p^m$, $p$ a prime. Denote by $f(x)$, $g(x)$ the cosets of $f(x)$, $g(x) \pmod{p^m\mathbb{Z}[x]}$, respectively. Assume $f(x) g(x) = 0$, i.e., $p^m \mid f(x) g(x)$. Since $p$ is a prime, it follows that $f(x) = p^f(x)$ and $g(x) = p^g(x)$ for some $f'$ and $g'$ satisfying the conditions that the greatest common divisor of the coefficients of $f'$ (also of $g'$) is not
divisible by $p$. Clearly $r + s \geq m$. It follows that $a_i b_j = 0$ for every $i$ and $j$, showing that $Z/p^n Z$ is Armendariz.

Let $n$ be a natural number. Then $n = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$ where $p_i$'s are primes. By the Chinese remainder theorem, $Z/nZ \cong Z/p_1^n Z \oplus Z/p_2^n Z \oplus \cdots \oplus Z/p_s^n Z$.

Since each $Z/p_i^n Z$ is Armendariz, it follows that $Z/nZ$ is Armendariz.

The following generalisation of 2.1 has a similar proof.

2.2. Theorem. If $R$ is a commutative P.I.D. and $A$ an ideal of $R$, then $R/A$ is Armendariz.

2.3. Theorem. Let $R$ be a domain, $A$ an ideal of $R$. Suppose $R/A$ is Armendariz. Then $R$ is reduced, then so is the ring $R/A$.

Proof. Let $f(x)$, $g(x)$ be elements of $\{R (+) R\}[x]$, where

$$
\begin{align*}
  f(x) &= \sum_{i=0}^{n} (a_i, \bar{u})x^i = (f_0(x), \bar{f}_0(x)) \\
  g(x) &= \sum_{j=0}^{n} (b_j, \bar{v})x^j = (g_0(x), \bar{g}_0(x)).
\end{align*}
$$

If $f(x)g(x) = 0$, we have $(f_0(x), \bar{f}_0(x))(g_0(x), \bar{g}_0(x)) = (0, 0)$. Thus we have the following equations:

$$
\begin{align*}
  f_0(x)g_0(x) &= 0 \quad (I) \\
  f_0(x)\bar{g}_0(x) + f_1(x)g_0(x) &= 0 \quad (II)
\end{align*}
$$

Case 1. $f_0(x) = 0$. Then (II) becomes $f_1(x)g_0(x) = 0$ over $R/A$. Since $R/A$ is Armendariz, it follows that $\bar{u}b_j = 0$ for all $i$ and $j$. Also $f_0(x) = 0$ implies that $a_i = 0$ for all $i$. We conclude that $(a_i, \bar{u}) (b_i, \bar{v}) = (a_ib_j, a_i\bar{v} + u_ib_j) = 0$ for every $i$ and $j$.

Case 2. $g_0(x) = 0$. This case is similar to case 1.

As a special case of the above proposition, we have the following corollary.

2.4. Corollary. $Z (+) Z/nZ$ is Armendariz for each integer $n$.

It follows from 2.3 that if $R$ is a domain then $R$ is reduced. This result can be extended to reduced rings. The following properties of these rings will be used: i) If $a, b$ are elements of a reduced ring then $ab = 0$ if and only if $ba = 0$. ii) Reduced rings are Armendariz. iii) If $R$ is reduced, then so is the ring $R[x]$. We shall also identify $(R (+) R)[x]$ with the ring $R[x]$ in a natural manner.

2.5. Proposition. Let $R$ be a reduced ring. Then the ring $R (+) R$ is Armendariz.

Proof. Let $f(x) = (f_0(x), f_1(x)), g(x) = (g_0(x), g_1(x))$ be elements of $(R (+) R)[x]$ satisfying $f(x)g(x) = 0$.

Write $f(x) = \sum_{i=0}^{n} (a_i, \bar{u})x^i$ and $g(x) = \sum_{j=0}^{n} (b_j, \bar{v})x^j$. With corresponding representations for $f_i(x), g_i(x)$ (for $k = 0, 1$).

Now we have

(A) $f_0(x)g_0(x) = 0$. (B) $f_0(x)g_1(x) + f_1(x)g_0(x) = 0$.

Since $R[x]$ is reduced, (A) implies

(C) $g_0(x)f_0(x) = 0$.

Multiplying equation (B) by $g_0(x)$ on the left and using (C) we get $g_0(x)f_1(x)g_0(x) = 0$. This implies $(f_1(x)g_0(x))^2 = 0$ and so (since $R[x]$ is reduced)

(D) $f_1(x)g_0(x) = 0$.

This implies (on account of (B)) that

(E) $f_0(x)g_1(x) = 0$.

Now (A), (D) and (E) yield (since $R$ is Armendariz)

$a_i b_j = 0$, $a_i v_j = 0$ and $u_i b_j = 0$ for each $i$ and $j$. It follows that

$$(a_i, \bar{u}) (b_j, \bar{v}) = (a_i b_j, a_i v_j + u_i b_j) = 0$$

for each $i$ and $j$.

The following generalisation of 2.5 has a similar proof.

2.6. Proposition. Let $R$ be a reduced ring and $A$ an ideal of $R$ such that $R/A$ is reduced. Then $R (+) R/A$ is Armendariz.

2.7. Remark. Recall that a ring $R$ is strongly regular ([3], §4) if for each element $a$ in $R$, there exists an element $b$ in $R$ such that $a = ab^2$. A ring is strongly regular, if and only if it is (von Neumann) regular and reduced. If $R$ is a strongly regular ring, then for each ideal $A$ of $R$ it is strongly regular and reduced. On applying 2.6 we get the following result: if $R$ is a strongly regular ring, then for each ideal $A$ of $R$, the ring $R (+) R/A$ is Armendariz.

We conclude this section with a few more examples of Armendariz rings.

2.8. Proposition. Let $K$ be a field, $h: K \rightarrow K$ a field monomorphism, and $V$ a $K$-vector space. Then the ring $K (+) V$ is Armendariz.

Proof. The map $h$ induces a natural ring homomorphism $h: K[x] \rightarrow K[x]$. We have the torsion free “polynomial module” $V[x]$ over $K[x]$. We identify $(K (+) V)[x]$ with $K[x]$. 

Armendariz rings to some other classes of rings. We introduce the following definition.

4.1. Definition. A ring \( R \) is a left McCoy ring if whenever \( g(x) \) is a right zero-divisor in \( R[x] \) there exists a non-zero element \( c \) in \( R \) such that \( cg(x) = 0 \). Right McCoy rings are defined dually. A ring is a McCoy ring if it is both left as well as right McCoy.

4.2. Remark. It was proved by McCoy [5] that commutative rings have the above property; for an inductive proof of this result see [7]; see also [2]. If \( T \) is a ring with identity, the matrix ring \( M_n(T) \) is neither left nor right McCoy. (There do not exist nonzero matrices \( C, D \) satisfying \( Cg(x) = 0 \) and \( f(x)D = 0 \) for the polynomials considered in Remark 3.1.)

4.3. Remark. Let \( R \) be an Armendariz ring and assume that \( g(x) \) is a right zero-divisor in \( R[x] \). Then there exists a non-zero polynomial \( f(x) \in R[x] \) such that \( f(x)g(x) = 0 \). Since \( R \) is Armendariz, \( a_i b_i = 0 \) for each \( i \) and \( i \). Since \( f(x) \neq 0, a, b \neq 0 \) for some \( t : \) clearly \( a, g(x) = 0 \). Thus \( R \) is left (similarly right) McCoy. This shows that Armendariz rings are McCoy. The converse is not true: commutative rings are McCoy, as noted in 4.2, but we have examples of commutative non-Armendariz rings.

4.4. Definition ([3], §4). A ring \( R \) is semi-commutative if it satisfies the following condition: whenever elements \( a, b \) in \( R \) satisfy \( ab = 0 \), then \( abc = 0 \) for each element \( c \) of \( R \).

4.5. Remarks and Questions. The class of commutative rings and the class of reduced rings are contained in the class of semi-commutative rings. Both these (smaller) classes are trivially stable under the formation of polynomial rings.

A ring \( R \) is called normal if every idempotent in \( R \) is central: semi-commutative rings are normal ([3], Lemma 5). Against this background consider the following “stability” assertions:

(i) \( R \) normal \( \Rightarrow R[x] \) normal;
(ii) \( R \) semi-commutative \( \Rightarrow R[x] \) semi-commutative; and
(iii) \( R \) Armendariz \( \Rightarrow R[x] \) Armendariz.

We remark that (i) easily follows from an extension of ([1], Corollary 1) to normal rings. (It may be a known result but we have not seen a proof of (i) in the literature.

We do not know whether (ii) and (iii) are true. In view of these questions, the following
proposition may be of some interest.

4.6. Proposition. If $R$ is a semi-commutative ring which is Armendariz, then $R[x]$ is semi-commutative.

Proof. Let $f(x), g(x)$ be polynomials in $R[x]$ satisfying $f(x)g(x) = 0$. Let $h(x) = \sum_{k=0}^{i} c_k x^k \in R[x]$. Since $R$ is Armenderiz and $f(x)g(x) = 0$, $a_i b_j = 0$ for each $i$ and $j$. Since $R$ is semi-commutative $a_i c_k b_j = 0$ for each $i$, $j$ and $k$. Hence $f(x)h(x)g(x) = 0$. This proves that $R[x]$ is semi-commutative.

4.7. Remark. The concepts introduced and studied in this note have extensions in the context of modules, graded rings and graded modules. Related concepts can also be defined for power series rings. These generalisations will be carried out elsewhere.

Acknowledgement. We thank the referee for a careful reading of the manuscript, which led to improvements in presentation.

References

An Extension of Sturm’s Theorem to Two Dimensions

By Tomokatsu Saito

Department of Mathematics, Sophia University

Communicated by Shokichi Iyanaga, M. I. A. Jan. 13, 1997

1. Introduction and notation. Let \( f(x, y) \in \mathbb{R}[x, y] \) be a square free polynomial with real coefficients, namely \( f(x, y) \) is decomposed into the irreducible factors whose multiplicities are only one. Let \( C \) be the set of points \((x, y)\in \mathbb{R}^2\) such that \( f(x, y) = 0 \). Until now, only the following primitive method has been used to draw the curve \( C \) by computer, within a given rectangle \( R \). We decompose \( R \) into many small rectangles \( D \) and obtain \( C \cap R \) by gathering \( C \cap D \) as found as follows.

Let \( D \) be the set \( \{(x, y) \in \mathbb{R}^2 \mid a \leq x \leq b, c \leq y \leq d\} \), and put \( P_1 = (a, c) \), \( P_2 = (b, c) \), \( P_3 = (b, d) \) and \( P_4 = (a, d) \). For example, if \( f(P_1) f(P_2) < 0 \), then we can find approximately a point \( P_5 \) \( C \cap P_1 P_2 \) and a point \( P_6 \) \( C \cap P_3 P_4 \). Then the line \( P_5 P_6 \) can be considered approximately as \( C \cap D \).

But the above method has next two problems.

1. Even if \( f(P_1) f(P_2) > 0 \), it is possible that \( C \cap P_1 P_2 \neq \emptyset \).
2. Even if \( C \cap (\text{the boundary of } D) = \emptyset \), it is possible that \( C \cap (\text{the interior of } D) \neq \emptyset \).

In this paper, we would like to propose a more reliable method which permit us to liberate from these incertainties.

Let \( \partial D \) be the boundary of \( D \) and \( D' \) be the interior of \( D \). Then \( C \cap D \) is the direct union of \( C \cap \partial D \) and \( C \cap D' \). The search for \( C \cap D \) is made separately in two cases: the first case for \( C \cap \partial D \) and the second case for \( C \cap D' \).

2. First case. This case can be treated as the equation \( f = 0 \) is restricted to a boundary line. Then we can use Sturm’s theorem.

The Sturm sequence associated with the (one-variable) polynomial \( f(x) \) is a sequence of polynomials with \( f_0(x), f_1(x), \ldots, f_n(x) \) defined by the following equations:

\[
\begin{align*}
f_0(x) &= f(x), \quad f_1(x) = f'(x), \\
f_i(x) &= -\text{remainder} \left(f_{i-2}(x), f_{i-1}(x)\right)
\end{align*}
\]

where remainder means the remainder from the division of the former by the latter.

Let \( (a_1, \ldots, a_n) \) be a sequence of real numbers and \( (a'_1, \ldots, a'_n) \) be the subsequence of all non-zero numbers. Then \( \text{var}(a_1, \ldots, a_n) \), the number of sign variations, is the number of \( i \), \( 1 \leq i \leq n \), such that \( a_ia_{i+1} < 0 \).

Theorem (Sturm). Let \( f(x) \) be a square free polynomial. When \( \gcd(f(x), f'(x)) = f_1(x) \), the number of real roots of \( f(x) \) in the interval \( a < x \leq b \) is

\[
\text{var}(f_0(a), f_1(a), \ldots, f_n(a)) - \text{var}(f_0(b), f_1(b), \ldots, f_n(b)).
\]

Let \( D \) be the set \( \{(x, y) \in \mathbb{R}^2 \mid a \leq x \leq b, c \leq y \leq d\} \). Using Sturm’s theorem we can determine whether \( f(x, c) = 0 \) has a root in the interval \([a, b]\) of not. Thus we can determine whether \( C \cap \partial D \neq \emptyset \) or not, and if \( C \cap \partial D \neq \emptyset \), find this set approximately in considering from divisions of \( \partial D \).

3. Second case. When \( C \cap \partial D = \emptyset \) then we can find \( C \cap D' \) in the following manner.

If \( C \cap D' \neq \emptyset \), then there is a point \((x_0, y_0)\) such that \((x_0, y_0) \in C \cap D'\), but if \((x, y) \in C \cap D'\), then \( y \leq y_0 \). Such a point \((x_0, y_0)\) will be called a maximal point (of \( C \cap D' \) with respect to \( y \)). We write \( f_c(x, y) = \frac{\partial}{\partial x} f(x, y) \) and show

\[
f_c(x_0, y_0) = 0 \quad \text{for a maximal point } (x_0, y_0).
\]

If \( f_c(x_0, y_0) \neq 0 \) then using implicit function theorem, there exists a function \( g(y) \) near \( y_0 \) such that \( f(g(y), y) = 0 \) and \((x_0, y_0)\) cannot be a maximal point. Therefore we have \( f_c(x_0, y_0) = 0 \).

As \( f(x, y) \) is square free, we have \( \gcd(f(x, y), f_c(x, y)) = 1 \) in \( \mathbb{R}(y)[x] \). Using Euclidean algorithm we can find \( g(x, y), h(x, y) \in \mathbb{R}[x, y], \)

\[
F(y) \in \mathbb{R}[y]
\]

such that

\[
(3) \quad \text{f(x, y)}g(x, y) + f_c(x, y)h(x, y) = F(y)
\]

If \( f(x, y) = 0, f_c(x, y) = 0 \), then \( F(y) \) must be zero. Using Sturm’s theorem, we can count correctly the number of roots \( F(y) = 0 \) in the interval \([c, d]\) and we can calculate approximately all roots in this interval. Therefore we can calculate