The structures of a class of $Z$-local rings

Tongsuo Wu*
Department of Mathematics
Shanghai Jiaotong University
Shanghai 200030, P. R. China
and
Dancheng Lu†
Department of Mathematics
Suzhou University
Suzhou 215006, P. R. China

Abstract: A local ring $R$ is called $Z$-local if $J(R) = Z(R)$ and $J(R)^2 = 0$. In this paper the structures of a class of $Z$-local rings are determined.

Key Words: $Z$-local ring, structure, polynomial rings

Let $R$ be a commutative local ring which is not necessarily noetherian. Denote by $J(R)$ the Jacobson radical of $R$, $Z(R)$ the zero-divisor elements of $R$. $R$ is called $Z$-local if $J(R) = Z(R)$ and $J(R)^2 = 0$. This concept was introduced in [2] where the authors proved that for any commutative ring $S$ such that 2 is regular in $S$ and that $S$ satisfies DCC on principle ideals, if the zero-divisor graph $\Gamma(S)$ of $S$ is uniquely determined by neighborhoods and $S$ is not a Boolean ring, then $S$ is a $Z$-local ring. The zero-divisor graph of a commutative ring was introduced and studied in [1]. In this paper, we will try to determine the structure of a class of $Z$-local rings.

For any commutative ring extension $A \subseteq B$ and any $\alpha \in B$, recall that $\alpha$ is said to be integral over $A$, if there is a monic polynomial $f(x) \in A[x]$ such that $f(\alpha) = 0$. It is well known that $\alpha$ is integral over $A$ if and only if there is a subring $C$ of $B$ which contains $A$, such that $\alpha \in C$ and $C$ is finitely generated.

*Corresponding author. email: tswu@sjtu.edu.cn
†email: ludancheng@suda.edu.cn
as an $A$-module (Please see, e.g., [3, Theorem 9.1]). For an element $\alpha$ integral over $A$, a minimal polynomial of $\alpha$ over $A$ is a monic polynomial $f(x)$ with the least degree such that $f(\alpha) = 0$. In general, a minimal polynomial over $A$ need not be unique. But if $A$ is a field, then it is unique. If $A = \mathbb{Z}_p$ for some prime number $p$, then the minimal polynomial of $\alpha$ over $\mathbb{Z}_p$ is unique modulo $p$, that is, $p$ divides all the coefficients of $f(x) - g(x)$ for any minimal polynomials $f(x)$ and $g(x)$ of $\alpha$ over $\mathbb{Z}_p$. In this case, we will denote it as

$$f(x) \equiv g(x)(\mod p).$$

These observations will be used in the latter part of the paper.

By [2, Theorem 2.5], the characteristic of a $Z$-local ring has only three possible values, i.e., 0, $p$ or $p^2$. For a $Z$-local ring $R$ with characteristic 0, since any element of a $Z$-local ring is either a unit or a zero-divisor, we have $\mathbb{Q} \subseteq T(R) \cong R$.

**Theorem 1.** For a $Z$-local ring $R$, let $F$ be the prime subfield of the field $K = R/J(R)$. Assume that the characteristic of the ring $R$ is not $p^2$ for any prime number $p$. Assume further that $K = F[\alpha]$ is an algebraic extension over $F$ for some $\alpha \in R$, and let $g(x)$ be the minimal polynomial of $\alpha$ over $F$ with degree $n$. Let $\langle S \rangle = \{s_i \mid i \in I\}$ be the $K$-basis of the $K$-module $J(R)$.

1. There is an $F$-algebra epimorphism from $F[x, Y]/ \langle y_i y_j \mid i, j \in I \rangle$ to $R$, where $Y = \{y_i \mid i \in I\}$ is a set of commutative indeterminants.

2. If $\alpha$ is integral over $F$, then one and only one situation occurs in the following:

   - (i) If $g(\alpha) = 0$, then $R \cong K[Y]/ \langle y_i y_j \mid i, j \in I \rangle$, where $g(x)$ is irreducible over $F$ and $m \geq 1$.

   - (ii) If $g(\alpha) \neq 0$, then assume $g(\alpha) = \sum_{i=1}^{m} v_i(\alpha)s_i$, where $v_i(\alpha) \notin J(R)$. Then

$$R \cong F[x, Y]/ \langle g(x)^2, g(x) - \sum_{i=1}^{m} v_i(x)y_i, g(x)y_t, y_sy_r \mid r, s, t \in I \rangle.$$ 

(Notice that in the second case, $m \geq 2$, $g(x)$ is irreducible over $F$ with degree at least 2, and $v_i(x)$ are nonzero polynomials over $F$ and $\deg(v_i(x)) < n$.)

**Proof.** (1). By assumption, we have $F \subseteq R$. Since

$$(F[\alpha] + J(R))/J(R) = F[\alpha] = R/J(R),$$

we have $R = F[\alpha] + J(R)$. Now consider the $F$-algebra homomorphism

$$\sigma : F[x, Y]/ \langle y_i y_j \mid i, j \in I \rangle \rightarrow R = F[\alpha] + J(R), \quad h(x, y_i) \mapsto h(\alpha, s_i).$$
By assumption $S$ is the set of generators of the $R$-module $J(R)$. Since $J(R)^2 = 0$, $R = F[\alpha] + J(R)$, thus $\sigma$ is a surjective $F$-algebra homomorphism. This proves the first part of the theorem.

(2). Now assume further that $\alpha$ is integral over $F$. Let $g(x) \in F[x]$ be the minimal monic polynomial of $\alpha$ over $F$ and assume $\deg(g(x)) = n$. Let $f(x)$ be the minimal monic polynomial of $h$ over $F$ and assume $d = \deg(f(x)) = n$. Let $g(x)$ be the minimal monic polynomial of $\alpha$ over $F$. Then $g(x)$ is irreducible in $F[x]$ and we have $g(x)|f(x)$. Now assume $f(x) = g(x)^u \cdot l(x)$, where $(l(x), g(x)) = 1$. Since $g(\alpha) \in J(R)$, then $l(\alpha) \in U(R)$. By assumption, we must have $f(x) = g(x)^u$, where $u \leq 2$.

Case 1. If $u = 1$, then in $R$ we have $g(\alpha) = 0$. By assumption, for each nonzero polynomial $r(x)$ of degree less than $n$ ($n = \deg((g(x)))$, we have $r(\alpha) \notin J(R)$, i.e., $r(\alpha)$ is invertible in $R$. Thus $R = F[\alpha] \oplus J(R)$, where $F[\alpha]$ is a field and it is also a subring of $R$. In this case, we obviously have an $F$-algebra isomorphism

$$R \cong K[Y]/ \langle \{y_i y_j | i, j \in I\} \rangle.$$  

Case 2. If $u = 2$, then $g(\alpha) \neq 0$ and $g(\alpha) \in J(R)$. In this case, consider

$$\tau : F[x, Y]/W \to R, h(x, y_i) \mapsto h(\alpha, s_i),$$

where

$$W = \langle g(x)^2, g(x) - \sum_{i=1}^{m} v_i(x) y_i, g(x) y_r, y_s y_t | r, s, t \in I \rangle.$$  

By assumption, $\tau$ is a map and thus a surjective $F$-algebra homomorphism. In order to prove that $\tau$ is injective, for any $h(x, y_i) \in F[x, Y]$, we have

$$h(x, y_i) = g(x)^2 A + \sum_{i,j} y_i y_j B_{ij} + (\sum_{r} [g(x)q_r(x) + f_r(x)] y_r) + [g(x)q_\#(x) + f_\#(x)],$$

where the degrees of $q_d(x)$ and $f_e(x)$ are at most $n - 1$ whenever they are not zero. By assumption, $q_d(\alpha)$ and $f_e(\alpha)$ are units of $R$ when the corresponding polynomials are not zero. Then if $h(\alpha, s_i) = 0$, then we must have

$$0 = (\sum_{r} [f_r(\alpha)] s_r + [g(\alpha)q_\#(\alpha) + f_\#(\alpha)], \quad (*)$$

Now if $f_\#(\alpha) \neq 0$, then $f_\#(\alpha)$ is a unit. But from the previous equality ($*$), we also obtain $f_\#(\alpha) \in J(R)$, a contradiction. Thus by assumption and ($*$), we obtain

$$\sum_{r} f_r(\alpha) \cdot s_r = -q_\#(\alpha) \sum_{i=1}^{m} v_i(\alpha) s_i.$$
Thus for \( r \not\in \{1, 2, \ldots, m\} \); \( f_r(x) \) must be zero or else it is a unit and at the same
time, it is in \( J(R) \). For \( r = 1, 2, \ldots, m \), we have \( f_r(\alpha) = -q_\#(\alpha) \cdot v_r(\alpha) \). Since
\( f(x) = g(x)^2 \), we obtain \( f_r(x) = -q_\#(x) \cdot v_r(x) \). Now coming back to the previous
decomposition of \( h(x, y_i) \), we obtain
\[
\sum_r f_r(x) \cdot y_r + g(x)q_\#(x) = q_\#(x)[g(x) - \sum_{i=1}^m v_i(x)y_i].
\]
This shows that \( \tau \) is injective. This completes the whole proof. \( \square \)

Now let \( R \) be a \( \mathbb{Z} \)-local ring with \( \text{char}(R) = p^2 \) for some prime number \( p \).
Then \( \{i | 0 \leq i \leq p^2 - 1\} = \mathbb{Z}_{p^2} \subseteq R \). Denote by \( F \) the prime subfield \( \mathbb{Z}_p \) of
the field \( K = R/J(R) \) and let \( S \cup \{p\} \) be a set of \( K \)-basis of the \( K \)-space \( J(R) \),
where \( p \not\in S \) and \( S = \{s_i | i \in I\} \). Let \( Y = \{y_i | i \in I\} \) be a set of indeterminants
determined by the index set \( I \). Assume further that \( K = F[\overline{\alpha}] \) is an algebraic
extension over \( F \) for some \( \alpha \in R \), and let \( \overline{g}(x) \) be the minimal polynomial of
\( \alpha \) over \( F \) with degree \( n \), where \( g(x) \in \mathbb{Z}_{p^2}[x] \) is a monic polynomial. We also
observe the following facts which will be used repeatedly:

**For any polynomial** \( u(x) \in \mathbb{Z}_{p^2}[x] \), if \( u(x) \not\equiv 0 \pmod{p} \) and its degree
modulo \( p \) is less than \( n \), then \( u(x) \) is a unit of \( R \).

We are now ready to determine the structure of a class of \( \mathbb{Z} \)-local rings with
characteristic \( p^2 \).

**Theorem 2.** For a \( \mathbb{Z} \)-local ring \( R \) with characteristic \( p^2 \), assume that \( R/J(R) = K = F[\overline{\alpha}] \) is an algebraic extension over \( \mathbb{Z}_p \cong F \subseteq R/J(R) \) for some \( \alpha \in R \).
Assume further that \( \alpha \) is integral over \( \mathbb{Z}_p^2 \). Then either \( R \cong \mathbb{Z}_{p^2}[x, Y]/Q_1 \), where
\( Q_1 = \langle Q \cup \{g(x)\} \rangle \) and \( |Y| \geq 0 \), or \( R \cong \mathbb{Z}_{p^2}[x, Y]/Q_2 \), where
\[
Q_2 = \langle Q \cup \{g(x)^2, pg(x), g(x)y_r, g(x) - \sum_{i=1}^m v_i(x)y_i \in I\} \rangle.
\]

In each case, \( \overline{g}(x) \) is irreducible over \( \mathbb{Z}_p \), and
\[
Q = \{px, y, y_t, py_r | r, s, t \in I \},
\]
where \( m \geq 1 \) is a fixed number, and \( v_i(x) \not\equiv 0 \pmod{p} \). We also notice that in
the second case, \( g(x) \) is some polynomial over \( \mathbb{Z}_{p^2} \) such that \( \deg g(x) > 1 \).

**Proof.** First, it is easy to see that \( R = \mathbb{Z}_{p^2}[\alpha] + J(R) \). Since \( \alpha \) is integral over \( \mathbb{Z}_{p^2} \),
we have a minimal polynomial \( f(x) \in \mathbb{Z}_{p^2}[x] \) which is unique modulo \( p \). By the
choice of \( g(x) \), we have \( f(x) = g(x)^u r(x) \pmod{p} \) for some monic \( r(x) \in \mathbb{Z}_{p^2}[x] \).
satisfying \((g(x), \overline{r}(x)) = 1\) in \(F[x]\). Thus \(r(\alpha)\) is invertible in \(R\) since \(g(\alpha) \in J(R)\).

Without loss of generality, we can assume \(f(x) = g(x)^u r(x) + h(x)\), where \(h(x) \equiv 0 \pmod{p}\). If \(u \geq 3\), then we obtain \(0 = f(\alpha) = g(\alpha)^u r(\alpha) + h(\alpha) = h(\alpha)\).

Thus the monic polynomial \(g(x)^2 r(x)\) annihilates \(\alpha\) and it has a degree less than \(\deg f(x)\), contradicting to the choice of \(f(x)\). Thus we must have \(u \leq 2\).

**Case 1.** If \(u = 2\), we have \(h(\alpha) = 0\) again. In this case, we must have \(r(x) = 1\) since \(g(x)^2\) annihilates \(\alpha\). In this case, we can choose \(f(x) = g(x)^2\).

**Case 2.** If \(u = 1\), we have \(f(x) = g(x) r(x) + h(x)\), where \(h(x) \equiv 0 \pmod{p}\).

In this case, we have \(g(\alpha) = -h(\alpha) \cdot r(\alpha)^{-1} = -h(\alpha) w(\alpha)\) for some \(w(x) \in \mathbb{Z}_p^2[x]\).

Obviously \(g(x) \equiv g(x) + h(x) w(x) \pmod{p}\). Thus in this case we can choose the \(g(x)\) such that \(g(\alpha) = 0\).

**1** Let us first consider the case when \(g(\alpha) = 0\).

In this case, consider

\[
\tau : F[x, Y]/Q_1 \rightarrow R = F[\alpha] + J(R), \overline{h(x, y_i)} \mapsto h(\alpha, s_i).
\]

For each generators \(h(x, y_i)\) of \(Q_1\), we have \(h(\alpha, s_i) = 0\). Thus \(\tau\) is a surjective \(F\)-algebra homomorphism. Now for any \(h(x, y_i) \in F[x, Y]\), we have a decomposition

\[
h(x, y_i) \equiv \sum_r f_r(x) y_r + f_\#(x) \pmod{Q_1}, \quad (**)
\]

where \(f_r(x)\) are some polynomials of \(x\) over \(F\) which has degree less than \(n\) when they are nonzero modulo \(p\), for all \(s \neq \#\). If in \(F[x, Y]/Q_1\), \(\overline{h(x, y_i)} \neq 0\), then either one of the \(f_s(x)\) is not zero modulo \(p\), or \(f_\#(x) \neq 0\). Thus if \(f_\#(x) = 0\), then we have some unit \(f_\#(\alpha)\) and hence \(h(\alpha, s_i) \neq 0\). If \(f_\#(x) \neq 0\), we also conclude that \(h(\alpha, s_i) \neq 0\). In fact, assume in the contrary that \(h(\alpha, s_i) = 0\). If \(\deg(f_\#(x)) > 0\) with coefficients modulo \(p\), then \(f_\#(\alpha) \in J(R) \cap U(R)\), a contradiction. If \(f_\#(x) \neq 0\) and \(\deg(f_\#(x)) = 0\), then we need only consider the case when \(f_\#(\alpha) = pi(\mod px)\) for some \(1 \leq i \leq p - 1\) since \(px \in Q_1\). Then we obtain a contradiction \(i \cdot p + \sum_r f_r(\alpha) s_r = 0\), since \(p \notin S\). These arguments show that \(\tau\) is injective. In conclusion, \(\tau\) is an \(F\)-algebra isomorphism under the assumption of \(g(\alpha) = 0\).

**2** Now assume \(g(\alpha) \neq 0\). Then \(g(\alpha)^2 = 0\) and \(p g(\alpha) = 0\) since \(g(\alpha) \in J(R)\). Since this case corresponds to the case of \(f(x) = g(x)^2\), we can choose an \(g(x)\) such that \(g(\alpha) = \sum_{i=1}^m v_i(\alpha) s_i\), where \(v_i(\alpha) \in U(R)\).

In this case, consider

\[
\tau : F[x, Y]/Q_2 \rightarrow R, \overline{h(x, y_i)} \mapsto h(\alpha, s_i),
\]
By the choice of $Q_2$, it is easy to see that $\tau$ is a map and thus a surjective $F$-algebra homomorphism. In order to prove that $\tau$ is injective, for any $h(x, y_i) \in F[x, Y]$, we have

$$h(x, y_i) \equiv \sum_r f_r(x) y_r + [g(x)q_\#(x) + f_\#(x)](\mod Q_2),$$

where the degrees of $q_\#(x)$ and $f_r(x)$ are at most $n-1$ whenever they are not zero, modulo $p$. By assumption, $q_\#(\alpha)$ and $f_r(\alpha)$ are units of $R$ when the corresponding polynomials are not zero modulo $p$ ($r \neq \#$). If $h(\alpha, s_i) = 0$, then we must have

$$0 = (\sum_r f_r(\alpha)) s_r + [g(\alpha)q_\#(\alpha) + f_\#(\alpha)], \quad (*)$$

(Subcase 1.) If $f_\#(x) = 0$, then by assumption and $(*)$, we obtain

$$\sum_r f_r(\alpha) \cdot s_r = -q_\#(\alpha) \sum_{i=1}^m v_i(\alpha) s_i.$$ 

Thus for $r \notin \{1, 2, \cdots, m\}$, $f_r(x)$ must be zero (modulo $p$), or else $f_i(\alpha)$ is a unit and at the same time, it is in $J(R)$. For $r = 1, 2, \cdots, m$, we have $f_r(\alpha) = -q_\#(\alpha) \cdot v_r(\alpha)$ (mod $J(R)$). Since $f(x) = g(x)^2$, we obtain $f_r(x) = -q_\#(x) \cdot v_r(x)$ modulo $p$. Now coming back to the previous decomposition of $h(x, y_i)$, we obtain

$$\sum_r f_r(x) \cdot y_r + g(x)q_\#(x) = q_\#(x)[g(x) - \sum_{i=1}^m v_i(x) y_i] \equiv 0 \mod Q_2.$$ 

(Subcase 2.) If $f_\#(x) \neq 0$, then $\deg(f_\#(x)) = 0$ (modulo $p$), or else $f_\#(\alpha) \in J(R) \cap U(R)$ by $(*)$, a contradiction. In the following, we assume $f_\#(x) \neq 0$ and $\deg(f_\#(x)) = 0$ (with coefficients modulo $p$). Now consider $(*)$ and assume $f_\#(x) \equiv p i (\mod px)$ for some $1 \leq i \leq p - 1$. We have

$$i \cdot p + \sum_r f_r(\alpha) \cdot s_r \equiv -q_\#(\alpha)g(\alpha).$$

Since $i$ is invertible in $R$, $p$ can be written as an $R$-combination of the $s_i$’s. This is certainly impossible. The above arguments show that $\tau$ is injective. This completes the whole proof. \qed

It is well known that any finite field is a simple algebraic extension over it’s prime subfield $\mathbb{Z}_p$ for some prime number $p$. As an application of Theorem 2, we immediately obtain the following results.

**Theorem 3.** Let $R$ be a finite ring whose characteristic is a prime square $p^2$. Then $R$ is a $Z$-local ring if and only if either,

$$R \cong \mathbb{Z}_{p^2}[x, y_1, \cdots, y_m]/\langle g(x), px, y_s y_t, py_r, 1 \leq r, s, t \leq m \rangle.$$
for some polynomials \( g(x) \in \mathbb{Z}_{p^2}[x] \) such that \( \overline{g}(x) \) is irreducible over \( \mathbb{Z}_p \), or \( R \cong \mathbb{Z}_{p^2}[x, y_1, \ldots, y_m]/M \), for some

\[
M = \langle \{ g(x)^2, pg(x), g(x)y_r, px, y_r, py_r, g(x) - \sum_{i=1}^{m} v_i(x)y_i | 1 \leq r, s, t \leq m \} \rangle
\]

where \( g(x) \) is some polynomial over \( \mathbb{Z}_{p^2} \) such that \( \text{deg} g(x) > 1 \) and that \( \overline{g}(x) \) is irreducible over \( \mathbb{Z}_p \), and at least one of the \( v_i(x) \) is not zero modulo \( p \), while \( \text{deg} v_i(x) \) is less than \( \text{deg} g(x) \).

Finally, we remark that each ring of the four types in Theorem 1 and Theorem 2 is obviously a \( \mathbb{Z} \)-local ring. We also remark that not all finite local rings whose zero-divisor graph is uniquely determined are \( \mathbb{Z} \)-local. For example, each of \( \mathbb{Z}_2[x_1, x_2, \ldots, x_n]/ < x_1^2, x_2^2, \ldots, x_n^2 > \) and \( \mathbb{Z}_4[x_1, x_2, \ldots, x_n]/ < x_1^2, x_2^2, \ldots, x_n^2 > \) is a finite local rings with the property that \( J(S) = Z(S) \) and \( x^2 = 0, \forall x \in Z(S) \). Obviously they are not \( \mathbb{Z} \)-local.

**REFERENCES**

1. Anderson D.F.; Livingston P.S. The zero-divisor graph of a commutative ring. J. of Algebra 1999, 217, 434-447.
2. Lu Dancheng and Wu Tongsuo. The zero-divisor graphs which are uniquely determined by neighborhoods. Preprint 2005.
2. Hideyuki Matsumura. Commutative Ring Theory. Cambridge Studies in Advanced Mathematics, 1986.