Let $R$ be a commutative ring possessing (non-zero) zero-divisors. There is a natural graph associated to the set of zero-divisors of $R$. In this article we present a characterisation of two types of $R$. Those for which the associated zero-divisor graph has diameter different from 3 and those $R$ for which the associated zero-divisor graph has girth other than 3. Thus, in a sense, for a generic non-domain $R$ the associated zero-divisor graph has diameter 3 as well as girth 3.

Let $R$ be a commutative ring with $1 \neq 0$ and let $Z(R)$ denote the set of non-zero zero-divisors of $R$. By the zero-divisor-graph of $R$ we mean the graph with vertices $Z(R)$ such that there is an (undirected) edge between vertices $x, y$ if and only if $x \neq y$ and $xy = 0$ (see [1, 3, 4]). Since there is hardly any possibility of confusion, we allow $Z(R)$ to denote the zero-divisor graph of $R$. Following their introduction in [3], zero-divisor graphs have received a good deal of attention. For a more comprehensive list of references the reader is requested to refer to the bibliographies of [1, 2, 4]. Zero-divisor graphs are highly symmetric and structurally very special; for example, in [4] this author has investigated the structure of cycles, the graph-automorphism-group $\Gamma(R)$ and its explicit relationship with the ring-automorphism-group Aut($R$). A sample consequence of interest is: if $\Gamma(R)$ is solvable, so is Aut($R$). For this reason alone it is of interest to understand the nature of zero-divisor graphs. From the available evidence one is tempted to surmise that generic zero-divisor graphs may be completely classifiable (in some sense).

It has been the experience that whenever one assumes $Z(R)$ to have some special feature, one can narrow down $R$ to a small class of rings. The present article provides an instance of this facet.

We tacitly assume that $R$ has at least 2 non-zero zero-divisors. By declaring the length of each edge to be 1, $Z(R)$ becomes a metric space in which the distance between two vertices is, by definition, the length of a shortest path connecting them. The diameter of a metric space is the supremum (possibly $\infty$) of the distances between pairs of points of the space. With this structure, a zero-divisor graph is known to be a connected graph of diameter at most 3 (for example see [1] or [4, (1.2)]). The girth of a graph is the
length of a shortest cycle (or equivalently the number of vertices of a least sided polygon) contained in the graph. If \( Z(R) \) does not contain a cycle, then its girth is defined to be \( \infty \). Obviously the girth of a graph is at least 3. The girth of \( Z(R) \), for an arbitrary \( R \), is known to be either infinite or 3 or 4 (see [4, (1.4)]).

In (1.2) of this article we present a characterisation of the rings \( R \) for which the associated zero-divisor graph has diameter at most 2. In (2.3) we identify those \( R \) whose associated zero-divisor graph has girth exactly 4. In (2.5) and (2.6) we determine the rings \( R \) for which the associated zero-divisor graph has infinite girth. The graph-theoretic counterpart of this has already been dealt with in [4] where the zero-divisor graphs of infinite girth are completely determined. Except for one class of zero-divisor graphs of diameter 2, the nature of zero-divisor graphs having either small diameter or large girth is readily understood from the corresponding ring-theoretic characterisations.

By the total quotient ring of \( R \) we mean the quotient ring \( Q(R) := T^{-1}R \) where \( T \) stands for the multiplicative subset of non zero-divisors of \( R \). Since the canonical homomorphism from \( R \) to \( Q(R) \) is injective, \( R \) is thought of as a sub-ring of \( Q(R) \). As mentioned above, we shall tacitly assume \( Z(R) \) to have at least two elements.

**Theorem 1.1.** The diameter of \( Z(Q(R)) \) is the same as the diameter of \( Z(R) \). The girth of \( Z(R) \) is the same as the girth of \( Z(Q(R)) \).

**Proof:** Observe that the diameter of \( Z(Q(R)) \) is 1 if and only if the diameter of \( Z(R) \) is also 1. Now suppose that the diameter of \( Z(Q(R)) \) is 2. Then the diameter of \( Z(R) \) is at least 2. Consider any \( a, b \in Z(R) \) with \( a \neq b \) and \( ab \neq 0 \). By our assumption about the diameter of \( Z(Q(R)) \), there is a \( q \in Z(Q(R)) \) such that \( a \neq q \neq b \) and \( aq = 0 = bq \). Let \( q := c/t \) with \( c, t \in R \) such that \( t \) is a non zero-divisor of \( R \). Then \( ac = 0 = bc \). It follows that \( c \) is in \( Z(R) \) and hence the distance between \( a, b \) (when considered as vertices of the zero-divisor graph of \( R \)) is 2. Conversely, assuming that the diameter of \( Z(R) \) is 2 it is easy to see that the diameter of \( Z(Q(R)) \) must also be 2. In general, the diameter of any zero-divisor graph is at most 3. Therefore we have established the first assertion.

Since \( Z(R) \) is a sub-graph of \( Z(Q(R)) \), it is clear that the girth of \( Z(R) \) is greater than or equal to the girth of \( Z(Q(R)) \). Earlier we have noted that the girth of any zero-divisor graph, when finite, is either 3 or 4. Suppose \( Z(Q(R)) \) has girth 3. Then there are distinct elements \( q_1, q_2, q_3 \) of \( Z(Q(R)) \) such that \( q_1 q_2 = q_2 q_3 = q_3 q_1 = 0 \). For \( i = 1, 2, 3 \), let \( g_i := a_i/t \) with \( a_i, t \in R \) and where \( t \) is a non zero-divisor of \( R \). Then \( a_1, a_2, a_3 \) are distinct elements of \( Z(R) \) and since \( a_1 a_2 = a_2 a_3 = a_3 a_1 = 0 \), they form a triangle in the graph \( Z(R) \). Thus \( Z(R) \) also has girth 3.

**Theorem 1.2.** Assume that the diameter of \( Z(R) \) is \( \leq 2 \). Then exactly one of the following holds.

(i) \( Z(R) \cup \{0\} \) is a prime ideal of \( R \),
(ii) $R$ is a sub-ring of a product of two integral domains.
If (ii) holds for (a non-domain) $R$, then the diameter of $Z(R)$ is at most 2. If (i) holds for (a non-domain) $R$ and $R$ is Noetherian, then $Z(R)$ is of diameter at most 2.

**Proof:** Suppose $Q(R)$ has two distinct maximal ideals $M_1$ and $M_2$. Let $x \in M_1$ and $y \in M_2$ be such that $x + y = 1$. Then $x, y$ are in $Z(Q(R))$ and

$$(0 : x) \cap (0 : y) = 0$$

(considered as ideals of $Q(R)$.) Since, by (1.1), the diameter of $Z(Q(R))$ is also 2, we must have $xy = 0$. But $y = 1 - x$ and hence $x$ is an idempotent of $Q(R)$. It follows that $Q(R)$ is isomorphic to a product of two rings. Say $Q(R) = R_1 \times R_2$. Suppose $Z(R_1)$ is non-empty. Let $a$ be an element of $Z(R_1)$. Then $(a, 1), (1, 0)$ are elements of $Z(Q(R))$ such that the distance between them is at least 3. This is impossible due to the assumption that $Z(Q(R))$ has diameter 2. Hence $Z(R_1)$ has to be empty. Symmetrically, $Z(R_2)$ must also be empty. Consequently $R_1, R_2$ are domains (in fact, fields) that is, assertion (ii) holds. It is clear that (i) holds if and only if $Q(R)$ has a unique maximal ideal.

If (ii) holds, then the diameter of $Z(R)$ is easily seen to be either 1 or 2. If (i) holds and $R$ is Noetherian, then $P := Z(R) \cup \{0\}$, being an associated prime of 0, is of the form $(0 : x)$ for some $x \in Z(R)$ and hence the diameter of $Z(R)$ is at most 2. \qed

**Remarks.** 1. The diameter of $Z(R)$ is 0 if and only if $Z(R)$ is a singleton set if and only if $R$ is either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{F}_2[X]/X^2\mathbb{F}_2[X]$ (or example, see [4, (1.1)]).

2. The diameter of $Z(R)$ is 1 (that is, $Z(R)$ is a complete graph) if and only if either $R$ is the product of the field of 2 elements with itself or (i) holds with the added property that $P^2 = 0$ (see [1]).

3. Let $A$ be a quasi-local factorial domain of (Krull) dimension at least 2. Let $m(A)$ denote the maximal ideal of $A$ and let $p(A)$ be a set of primes of $A$ such that for each height-one prime ideal $P$ of $A$ there is a unique $p \in p(A)$ with $P = pA$. Let $A[X]$ be the polynomial ring over $A$ in the set of indeterminates $X := \{X_p \mid p \in p(A)\}$. Then $p(A)$ (and hence $X$) is necessarily infinite. Let $J$ be the ideal of $A[X]$ generated by $\{pX_p \mid p \in p(A)\}$ and $I := J + (XA[X])^2$. Define $R := A[X]/I$ and $M := (m(A) + XA[X])/I$. Then $M$ is a maximal ideal of $R$ whose elements constitute the zero-divisors of $R$. Thus (i) holds for $R$. It is straightforward to verify that $A$ is (naturally) a sub-ring of $R$ and given two distinct members $p, q$ of $p(A)$ and an $r \in R$ with $pr = 0 = qr$ we must have $r = 0$. Consequently, $Z(R)$ has diameter 3.

**Lemma 2.1.** Assume that $Z(R)$ has girth 4. Then $R$ has at most one non-zero nilpotent. Furthermore, if $a$ is the non-zero nilpotent of $R$, then $(0 : a)$ is a maximal ideal having $\mathbb{F}_2$ as its residue field.

**Proof:** Assume $R$ has non-zero nilpotents. Let $a$ be a non-zero nilpotent of $R$ such that $a^2 = 0$. If there are 4 distinct elements in the ring $R/(0 : a)$, then there are
3 distinct elements of $Z(R)$ of the form $xa, ya, za$ (with $x, y, z \in R$) which constitute a 3-cycle in $Z(R)$. Thus, in view of our hypothesis, it follows that $R/(0 : a)$ is a ring of cardinality at most 3. It is straightforward to verify that the zero-divisor graph of a ring of cardinality < 9 has girth 3. Hence $(0 : a)$ has cardinality at least 4. If $aR \neq \{0, a\}$, then for any $b \in aR \setminus \{0, a\}$ and any $x \in (0 : a) \setminus \{0, a, b\}$ the elements $a, x, b$ of $Z(R)$ form a 3-cycle, contrary to our hypothesis. Therefore $aR = \{0, a\}$. It now follows that $(0 : a)$ is a maximal ideal having the field of 2 elements as its residue field. If there is some non-zero $x \in (0 : a)$ for which $(0 : x) \cap (0 : a)$ is not a subset of $\{0, a, x\}$, then for any $y \in (0 : x) \cap (0 : a) \setminus \{0, a, x\}$, elements $a, y, x$ form a 3-cycle. Hence $(0 : x) \cap (0 : a)$ is a subset of $\{0, a, x\}$ for all non-zero $x$ in $(0 : a)$.

Let $y$ be a nilpotent of $R$ such that $y^{n+1} = 0$ but $y^n \neq 0$ for a positive integer $n$. Clearly $n \leq 3$, otherwise, $y^n, y^{n-1}, y^{n-2}$ would be distinct elements of $Z(R)$ forming a 3-cycle. In other words $y^4 = 0$ for every nilpotent $y$ of $R$. Suppose there is a nilpotent $y$ in $R$ with $y^3 \neq 0$. If $(0 : y^2) \neq \{0, y^2, y^3\}$, then for any $z \in (0 : y^2) \setminus \{0, y^2, y^3\}$ elements $y^2, z, y^3$ constitute a 3-cycle. On the other hand, if $(0 : y^2) = \{0, y^2, y^3\}$, then since $R/(0 : y^2)$ has cardinality 2 by the above argument, $R$ would be a ring of cardinality at most 6 and hence $Z(R)$ can not possibly have girth 4. Summarising, we must have $y^3 = 0$ for every nilpotent $y$ of $R$. Next suppose there is nilpotent $y$ of $R$ with $y^2 \neq 0$. If $(0 : y) \neq \{0, y^2\}$, then $y, x, y^2$ forms a 3-cycle of $Z(R)$ for any $x \in (0 : y) \setminus \{0, y^2\}$. So $(0 : y) = \{0, y^2\}$. Let $x$ be in $(0 : y^2)$ but not in $(0 : y)$. Then $xy$ is a non-zero element of $(0 : y)$ and hence $xy = y^2$. Now $x - y$ being in $(0 : y)$ it is either 0 or $y^2$. Thus $(0 : y^2)$ is contained in the set $\{0, y, y^2, y + y^2\}$. Since $R$ must have cardinality at least 9 (for $Z(R)$ to have girth 4) and $R/(0 : y^2)$ has cardinality 2, this is impossible. Therefore, we conclude that $y^2 = 0$ for each nilpotent $y$ of $R$.

Let $N(R)$ denote the nil-radical of $R$. Let $a, b$ be non-zero members of $N(R)$. If $ab \neq 0$, then elements $a, a + ab, ab$ form a triangle in $Z(R)$. This being impossible, $N(R)^3 = 0$. If $N(R) \neq aR$, then for any $c \in N(R) \setminus aR$ elements $a, a + c, b$ form a triangle of $Z(R)$. Hence we must have $N(R) = aR$. But we have already shown that $aR = \{0, a\}$. This establishes our assertion.

**Remark.** Observe that if $R := D \times Z/4Z$ where $D$ is an integral domain different from $\mathbb{F}_2$, then $R$ has a non-zero nilpotent and $Z(R)$ does have girth 4.

**Lemma 2.2.** Assume that the nil-radical of $R$ is zero. Then $Z(R)$ is complete bi-partite if and only if $R$ is a sub-ring of a product of 2 integral domains.

**Proof:** The ‘if’ part is straightforward. Suppose $Z(R)$ is complete bi-partite. Then $Z(R)$ has a partition $\{Z_1, Z_2\}$ where $Z_1 = (0 : x) \setminus \{0\}$ for all $x \in Z_2$ and $Z_2 = (0 : x) \setminus \{0\}$ for all $x \in Z_1$. Let $P_1 := Z_1 \cup \{0\}$. Pick $y$ in $Z_2$. Now $P_1 = (0 : y)$. Assume $a, b \in R$ with $ab \in P_1$. Then $aby = 0$. If $by = 0$, then $b$ is in $P_1$. Assume $by \neq 0$. Now $by$ is in $Z(R)$ and $(0 : y) \subseteq (0 : by)$. If $by$ is in $Z_1$, then $0 = (0 : by) \cap (0 : y)$ which is absurd since $(0 : by) \cap (0 : y) = (0 : y)$. This forces $by$ to be in $Z_2$. But then $(0 : by) = (0 : y)$
and \( a \in (0 : by) = (0 : y) = P_1 \). In other words, \( P_1 \) is a prime ideal of \( R \). Likewise \( P_2 := Z_2 \cup \{0\} \) is also a prime ideal of \( R \). Since \( Z_1 \cap Z_2 \) is empty, \( P_1 \cap P_2 = 0 \). It follows that \( R \) is canonically isomorphic to a sub-ring of the product of integral domains \( R/P_1 \) and \( R/P_2 \).

**Theorem 2.3.** Assume that \( Z(R) \) has finite girth. Then the girth of \( Z(R) \) is 4 if and only if one of the following holds.

(i) \( R \) is a sub-ring of a product of two integral domains.

(ii) \( R \) is isomorphic to \( D \times S \) where \( D \) is an integral domain and \( S \) is either \( \mathbb{Z}/4\mathbb{Z} \) or \( \mathbb{F}_2[X]/X^2\mathbb{F}_2[X] \).

**Proof:** The proof is divided in two cases, namely the case where the nil-radical \( N(R) \) is zero and the case where \( N(R) \) is non-zero. Since \( R \) must have at least 9 elements for \( Z(R) \) to have girth 4, henceforth we tacitly assume that the cardinality of \( R \) is at least 9.

First assume that \( N(R) \neq 0 \). Then, from (2.1) it follows that \( N(R) = \{0, a\} \) and the cardinality of \( (0 : a) \) is at least 5. Let \( x \) be a non-nilpotent in \( (0 : a) \). If \((0 : x) \cap (0 : a) \) contains a non-nilpotent \( y \), then \( x, a, y \) form a triangle in \( Z(R) \). Hence \((0 : x) \cap (0 : a) = N(R) \) for every non-nilpotent \( x \) in \( (0 : a) \). If every zero-divisor of \( R \) is in \( (0 : a) \), then \((0 : x) = N(R) \) for all non-nilpotents of \( Z(R) \) and hence \( Z(R) \) has infinite girth contrary to our assumption. Thus \( Z(R) \setminus (0 : a) \) must be non-empty. Pick \( y \in Z(R) \) such that \( y \) is not in \( (0 : a) \). Clearly, \((0 : y) \neq 0 \). If \((0 : y) \cap (0 : a) \) is a subset of \( N(R) \), then since \( ay \neq 0 \), we have \((0 : y) \cap (0 : a) = 0 \) and hence \( R \) is isomorphic to \( \mathbb{F}_2 \times R/(0 : y) \) (where the first factor is the field of 2 elements). But the zero-divisor graph of such a product has girth either \( \infty \) or 3. Thus it must be possible to choose a non-nilpotent \( x \) in \( (0 : y) \cap (0 : a) \). Consider the set \( C := \{zy \mid z \in (0 : a)\} \). If \( C \) has a member \( b \) not in \( \{0, x, a\} \), then \( x, b, a \) form a triangle of \( Z(R) \) contrary to our hypothesis. Therefore, \( C \) is contained in \( \{0, x, a\} \). Using the fact that \( R/(0 : a) \) is the field of two elements, we conclude that \( y - 1 \) is in \( (0 : a) \) and \( yR \) is a subset of \( \{0, x, a, y + x, y + a\} \). Now \( (y - 1)a = 0 \) implies that \( a \) is in \( yR \). So \( 0, y, a, y + a \) are 4 distinct elements of \( yR \). Using the fact that \( R/(0 : a) \) is a field, we conclude that \( y + x + a \) can not be in the set \( \{0, x, a, y + x, y + a\} \). Hence \( yR = \{0, y, a, y + a\} \). But then \( y^2 \) must belong to \( \{y, y + a = y(1 + a)\} \) (observe that \( 1 + a \) is a unit of \( R \)). Consequently, \( y^2 R = yR \) has exactly 4 elements, \( (0 : y) \cap yR = 0 \) and \( (1 - y) \) is in \( (0 : y) \). Thus \( R \) is isomorphic to \( R/yR \times R/(0 : y) \) where \( R/(0 : y) \) is a ring of cardinality 4 containing a non-zero nilpotent (namely, the image of \( a \)). In other words (ii) holds.

Finally consider the case where \( N(R) = 0 \). Let \( x \) be in \( Z(R) \). Suppose, if possible, that \((0 : x) \) has exactly 2 elements \( \{0, y\} \). Then \( yR = \{0, y\} \) and hence \((0 : y) \) is a maximal ideal having the residue field of 2 elements. Also, since \( y^2 \neq 0 \), we must have \( y^2 = y \) and \( yR \cap (0 : y) = 0 \). Hence \( R \) is isomorphic to \( \mathbb{F}_2 \times R/yR \). But such a ring has girth either \( \infty \) or 3. Thus for each \( x \) in \( Z(R) \), the cardinality of \( (0 : x) \) is at least 3 (in
the terminology of [4], the graph $Z(R)$ has no ‘ends’). Now it follows from [4, (2.2)] (see Remark 2. following the assertion [4, (2.2)]) that $Z(R)$ is a bi-partite graph. In view of the Lemma (2.2) of this article we see that (i) holds.

Conversely, if either of (i) or (ii) holds (with $Z(R)$ being non-empty of finite girth) then it is easy to verify that the girth of $Z(R)$ is exactly 4.

\textbf{Lemma 2.4.} Assume that $R$ has at least 10 elements. Let $N(R)$ be the nil-radical of $R$ and assume that $N(R) \neq 0$. Then the following are equivalent.

(i) $Z(R)$ has infinite girth.

(ii) $N(R) = \{0, y\}$ and $(0 : x) = N(R)$ for all $x \in Z(R)$.

(iii) $N(R)$ has cardinality 2 and it is a prime ideal of $R$.

\textbf{Proof:} The equivalence of (i) and (ii) follows from [4, (2.1)]. Assertion (iii) follows from (ii) in a straightforward manner. Suppose (iii) holds. Then $N(R) = \{0, y\}$ for some non-zero $y$ in $R$. Let $x \in Z(R)$ be distinct from $y$. Then $x$ is not in $N(R)$ and $(0 : x) \neq 0$. Consider $0 \neq w \in (0 : x)$. Since $0 = xw \in N(R)$ and $N(R)$ is prime, we must have $w \in N(R)$ and hence $w = y$. Hence (ii) holds.

\textbf{Definition:} Let $B$ be a ring such that its nil-radical $N(B)$ is a prime ideal of cardinality 2 and let $B[X]$ be the polynomial ring in a non-empty set of indeterminates $X$ over $B$. Let $I$ be an ideal of $B[X]$ such that

1. $I \cap B = 0$,
2. $N(B)B[X] \cdot XB[X] \subseteq I \subseteq 2B[X] + N(B)B[X] + XB[X]$ and

Then, by $\rho(B, X, I)$ we mean the ring $B[X]/I$.

\textbf{Theorem 2.5.} Assume that $R$ has at least 10 elements. Let $N(R)$ be the nil-radical of $R$ and assume that $N(R) \neq 0$. Then $Z(R)$ has infinite girth if and only if one of the following holds.

(i) $R = \rho(B, X, I)$ where $B = \mathbb{Z}[w]/(w^2, 2w)\mathbb{Z}[w]$ for an indeterminate $w$ over $\mathbb{Z}$.

(ii) $R = \rho(B, X, I)$ where $B = \mathbb{F}_2[w]/w^2\mathbb{F}_2[w]$ for an indeterminate $w$ over $\mathbb{F}_2$ and where $I$ is such that $P(B, X, I) \neq N(B)B[X] + XB[X]$.

(iii) $R = \rho(B, X, I)$ where $B = \mathbb{Z}/4\mathbb{Z}$ and $I$ is such that $P(B, X, I) \neq N(B)B[X] + XB[X]$.

Moreover, such a ring is necessarily infinite.

\textbf{Proof:} Our argument will tacitly employ Lemma (2.4). At the outset we show that under our assumptions the characteristic of $R$ is either 0 or 2 or 4. Observe that a sub-ring of $R$ does not contain $y$ if and only if it is an integral domain. On the other hand, if a sub-ring $S \subseteq R$ contains $y$, then $N(S) = N(R) \cap S$ is a prime ideal and for any $a, b \in Z(S)$ we have $ab = 0$ if and only if either $a = y$ or $b = y$. Also, it follows that
(0 : y) ∩ S is a maximal ideal of S with residue field \(\mathbb{F}_2\). In particular, the characteristic of \(R\) is an even integer. Let \(2n\) denote the characteristic of \(R\). Suppose \(n\) is neither 0 nor 1. Then \(y\) is in the prime sub-ring \(\pi\) of \(R\). Since the zero-divisors of \(\pi\) have to be contained in the maximal ideal \((0 : y) \cap \pi\), the ring \(\pi\) is a local ring that is, \(n\) is a power of 2. But the nil-radical of \(\pi\) has exactly two elements. Hence \(n = 2\). It is plain to see that the rings of the form mentioned in (i), (ii), (iii) above have characteristics 0, 2 and 4 respectively.

Suppose \(R\) satisfies any one of (i), (ii) and (iii). To simplify the notation set \(P := P(B, X, I)\). In the first two cases let \(t\) be the canonical image of \(u\) in \(B\) and in the third case let \(t = 2\). Note that \(t^2 = 2t = 0\) and \(N(B) = \{0, t\}\). We claim that \(R\) has to be infinite. This is evident in the case of (i) since \(\mathbb{Z}\) is indeed the prime sub-ring of \(R\). In the remaining two cases there is an \(x\) in \(X\) which is not in \(P = tB[X] + I\) Consider the sub-ring \(A\) of \(B[X]\) obtained by adjoining \(x\) to the prime sub-ring. Then \(A\) is a polynomial ring in one variable over the prime sub-ring and \(I \cap A \subseteq P \cap A\). If \(A\) has characteristic 2 then \(P \cap A \subseteq xA\) and consequently \(P \cap A = 0\). Thus \(A\) is (naturally) an infinite sub-ring of \(R\). If \(A\) has characteristic 4, then \(P \cap A = 2A\) and hence \(A/(I \cap A)\) is necessarily an infinite sub-ring of \(R\). Let \(y\) denote the canonical image of \(t\) in \(R\). Then \(y\) is a non-zero nilpotent of \(R\). Let \(f \in B[X]\) be in the radical of \(I\). Clearly \(f\) has to be in \(P\). Hence \(yR = P/I = N(R)\) is a prime ideal of \(R\). It is easy to verify that \(N(R) = \{0, y\}\). By Lemma (2.4), \(Z(R)\) must have infinite girth.

Conversely, suppose \(R\) has at least 10 elements, \(N(R) \neq 0\) and \(Z(R)\) has infinite girth. In view of Lemma (2.4) if we let \(N(R) := \{0, y\}\), then \(N(R)\) is a prime ideal and \((0 : y)\) is a maximal ideal with residue field \(\mathbb{F}_2\). We have already established that the characteristic of \(R\) has to be one of 0, 2, 4. Our assumption about the cardinality of \(R\) ensures that the ideal \((0 : y)\) is distinct from \(N(R)\). Let \(\pi\) denote the prime sub-ring of \(R\). Then \(B := \pi[y]\) is (isomorphic to) exactly one of the rings appearing in (i), (ii), (iii) above. Clearly, \(N(B) = N(R)\) and since for each \(r \in R\) either \(r\) or \(r + 1\) is in \((0 : y)\), the ring \(R\) is obtained by adjoining the elements of \((0 : y)\) to \(B\). Observe that \((0 : y) \cap B\) is a maximal ideal of \(B\) which equals \(J := 2B + N(B)\) and has \(\mathbb{F}_2\) as its residue field. Now the \(B\)-module \((0 : y)/J\) is in fact a vector-space over \(\mathbb{F}_2 = B/J\). Let \(T \subset (0 : y)\) be such that \(T/J\) is an \(\mathbb{F}_2\)-basis of \((0 : y)/J\) (we allow \(T\) to be the empty set). Then \(R = B[T]\). Let \(X\) be a set of indeterminates over \(B\) equipped with a bijection \(s : X \rightarrow T \cup \{0\}\). Let \(\sigma : B[X] \rightarrow R\) be the unique homomorphism of \(B\)-algebras which restricts to \(s\) on the set \(X\). Then \(\sigma\) is surjective. Let \(I\) denote the kernel of \(\sigma\). Obviously \(I \cap B = 0\) and \(I\) contains \(yx\) for all \(x \in X\). If \(f := b - g \in I\) with \(b \in B\) and \(g \in XB[X]\), then \(b = \sigma(b) = \sigma(g)\) and \(\sigma(g) \in (0 : y)\) imply that \(b\) is in \(J\). Consequently, \(I\) is contained in \(2B[X] + N(B)B[X] + XB[X]\). Finally, since \(\sigma(N(B)) = N(R)\) is a prime ideal of \(R\), its inverse image \(N(B)B[X] + I\) is also a prime ideal of \(B[X]\).\[\]

**Remarks.** 1. If \(R\) has at least 10 members, \(N(R) = 0\) and \(Z(R)\) is non-empty, then
follows from the remark at the end of [4, (2.1)] (for infinite rings $R$ see [1, Theorem 2.5]). In fact, the above Theorem, in conjunction with [4, (2.1)] provides a complete (without any cardinality restrictions) characterisation of those non-domains $R$ for which $Z(R)$ has infinite girth (that is, $V(R) = \emptyset$ in the notation used in [4]).

2. Note that in the above proof it is not essential for us to choose $T$ the way we have chosen it, that is, we did not make any particular use of the fact that $T/J$ is a vector-space basis. On the other hand, it is natural to try to get hold of a ‘smallest possible’ set $T$ with $R = B[T]$.

**Definition:** If $B$ is a ring and $M$ is a $B$-module, then by $B(+)M$ we denote the ring obtained by idealising $M$ (as defined in [5]).

**Theorem 2.6.** Assume $R$ satisfies the following. As above, $N(R)$ denotes the nil-radical of $R$.

(i) $R$ has at least 5 elements.
(ii) There is $y \in Z(R)$ such that $N(R) = \{0, y\}$ and $(0 : x) = N(R)$ for all $x \in Z(R)$.

Then the characteristic of $R$ is not 4 if and only if $R$ has a sub-domain $A$ such that $A[y] \cong A(+)F_2$ and for each $r \in R$ there exists a non-zero $a \in A$ (depending on $r$) with $ar \in A[y]$. Moreover, if $r$ is not in $N(R)$ then $ar \neq 0$. (David F. Anderson (in a private communication) asked whether a non-reduced, non-domain $R$ with $Z(R)$ having infinite girth is of the form $D(+)F_2$ for some domain $D$. The above theorem constitutes our response to his question.)

**Proof:** From the argument at the beginning of the proof of (2.5) it follows that $R$ has characteristic 0 or 2 or 4. If a ring contains a sub-ring of type $D(+)F_2$ with $D$ a domain, then obviously the characteristic can not equal 4. Henceforth, assume that the characteristic of $R$ is either 0 or 2. We proceed to show that $R$ contains an infinite integral sub-domain. This is evident if $R$ is of characteristic 0. Suppose $R$ has characteristic 2.

Condition (i) ensures that $Z(R) \setminus \{y\}$ is non-empty. Let $x$ be an element of $Z(R) \setminus \{y\}$ and $S := F_2[x]$. Note that $Z(S)$ is contained in the single maximal ideal $P := (0 : y) \cap S$ of $S$. Since $xS \subseteq P$, we must have $P = xS$. It is easy to see that $y$ is not in $xR$ and hence $y$ is not in $S$. Thus $S$ is an infinite integral sub-domain of $R$ (in fact a polynomial ring over $F_2$). Let $A$ denote a maximal sub-ring of $R$ not containing $y$. Existence of such a sub-ring can be seen in a straightforward manner. As a consequence of the above argument $A$ has to be an infinite integral domain. Since $(0 : y) \cap A$ is a maximal ideal of $A$ with residue field $F_2$, it follows that $A$ is not a field. For $r \in R$ define

$I(r, A) := \{a \in A \mid ar \in A[y]\}$.

Clearly $I(r, A)$ is an ideal of $A$ and $I(r + b, A) = I(r, A)$ for all $b \in A$.

Suppose there is an $x$ in $R$ with $I(x, A) = 0$. Then $I(bx, A) = 0$ for all non-zero $b \in A$. Replacing $x$ by $x + 1$ if needed, we may assume that $x$ is a member of $(0 : y)$. Obviously
x is not in \( N(R) \) and hence \( xR \cap N(R) = 0 \). Consider the \( A \)-algebra homomorphism \( h \) of the polynomial domain \( A[X] \) onto \( A[x] \) which maps the indeterminate \( X \) to \( x \). Let \( J(x) \) denote the kernel of \( h \). Our choice of \( A \) ensures that \( y \in A[x] \). Thus \( J(x) \) is not a radical ideal of \( A[X] \). In particular, \( J(x) \neq 0 \). Let \( f \in J(x) \) be a non-zero polynomial of least degree. Let \( f := a_0X^d + \cdots + a_d \) where \( d \geq 2 \) is the degree of \( f \) and \( a_0 \neq 0 \). Replacing \( x \) by \( a_0x \) if needed, we may assume \( a_0 = 1 \) that is, \( x \) is integral over \( A \). The minimality of \( d \) allows us to conclude that \( J(x) = fA[X] \). More generally, we observe that \( J(bx) = b^df(X/b)A[X] \) for all non-zero \( b \in A \). Consequently, for each non-zero \( b \in A \), the ring \( A[bx] \) contains \( y \) and it is a free \( A \)-sub-module of \( A[x] \) with basis \( \{1, bx, \cdots, (bx)^{d-1}\} \). Now, \( A \) is an integral domain which is not a field and hence the intersection of all non-zero principal ideals of \( A \) is necessarily zero. Thus the intersection of all the sub-modules \( A[bx] \) of \( A[x] \), as \( b \) ranges over non-zero elements of \( A \) is exactly \( A \). This is absurd since \( y \) is certainly not in \( A \). Therefore we must have \( I(r,A) \neq 0 \) for all \( r \in R \). It is easy to see that \( A[y] \cong A(+\bar{F}_2) \).

**Remarks.** 1. The above theorem allows us to think of \( R \) as a “blow-up” of \( A(+\bar{F}_2) \).

2. A ring \( R \) is of the form \( S(+)M \) for some non-zero \( S \)-module \( M \) if and only if \( R \) has a non-zero ideal \( N \) and a derivation \( \delta : R \to N \) such that \( N^2 = 0, N \cap Ker(\delta) = 0 \) and the set-theoretic map \( R \to R/N \oplus N \) sending \( r \in R \) to \( \sigma(r) \oplus \delta(r) \) (here \( \sigma \) is the canonical map) is surjective. Now any derivation of \( R \) is identically 0 on the prime subring of \( R \). Suppose \( R \) satisfies the conditions of the above Theorem and the characteristic of \( R \) is 4. Then \( N(R) = \{0,2\} \) and it is the only non-zero ideal of \( R \) whose square is zero. Since \( N(R) \) is contained in the kernel of every derivation of \( R \), it follows that \( R \) is not of the form \( S(+)M \) with \( M \neq 0 \).

3. Consider the 3-variable polynomial ring \( B := \bar{F}_2[X_1, X_2, X_3] \) with ideal \( I \) generated by \( \{X_1f, X_2f, X_3f\} \) where \( f := X_1X_3 + X_2^2 \). Let \( R := B/I \) and let \( u, v, w, y \) denote the canonical images of \( X_1, X_2, X_3, f \) (respectively) in \( R \). It is easy to see that \( R \) satisfies the hypotheses of the above Theorem. We leave it to the reader to verify that for \( A \) (as in the conclusion of the Theorem) we may take the sub-ring \( \bar{F}_2[u,v,w^2, vw] \). Further, it is simple to check that \( \delta(y) = 0 \) for any derivation \( \delta : R \to \{0,y\} \). Hence \( R \) is not of the form \( S(+)M \) with \( M \neq 0 \). One can construct a similar example in characteristic 0.

**References**


Department of Mathematics  
The University of Tennessee  
Knoxville, TN 37996  
United States of America  
e-mail: mulay@math.utk.edu