*Bull. Aust. Math. Soc.* **79** (2009), 177–182
doi:10.1017/S0004972708001019

# NILPOTENCY OF THE GROUP OF UNITS OF A FINITE RING

DAVID DOLŽAN

(Received 8 April 2008)

**Abstract**

In this paper we find all finite rings with a nilpotent group of units. It was thought that the answer to this was already given by McDonald in 1974, but as was shown by Groza in 1989, the conclusions that had been reached there do not hold. Here, we improve some results of Groza and describe the structure of an arbitrary finite ring with a nilpotent group of units, thus solving McDonald's problem.

2000 *Mathematics subject classification*: primary 16P10; secondary 16U60.
*Keywords and phrases*: finite ring, group of units, nilpotent.

## 1. Introduction

In this paper let $R$ denote a ring with identity $1 \neq 0$ and for an arbitrary finite set $X$ let $|X|$ denote the number of elements in $X$. We denote the group of units of $R$ by $G$ or $G(R)$ and the Jacobson radical of $R$ by $J$ or $J(R)$. The ring of $n \times n$ matrices over a ring $R$ is denoted by $M_n(R)$ and the ring of integers modulo $m$ is denoted by $\mathbb{Z}_m$. Let $Z(I)$ denote the centre of an arbitrary ideal $I$ in $R$.

In [5, Corollary XXI.10], McDonald states that the group of units of a finite ring $R$ is nilpotent if and only if $R/J(R)$ is a direct sum of finite fields. Groza showed in [3] that this is not true because, in the case of the ring $R$ of $n \times n$ upper triangular matrices with entries from an absolute field, not of order two, the group $G(R)$ is not nilpotent, even though $R/J(R)$ is a direct sum of fields. He showed that for finite rings, such that at most one simple component of the semisimple ring $R/J(R)$ is a field of order two, $G(R)$ is a nilpotent group if and only if $R$ is a direct sum of rings that are homomorphic images of group rings $CP$, where $C$ is a homomorphic local image of the ring $\mathbb{Z}_{p^r}[X]/(X^{p^s-1} - 1)$ and $P$ is a finite $p$-group for some prime $p$.

In the first section we study the Galois coefficient ring of a finite local ring. If $R$ is a finite local ring, then by [5, Theorem XIX.1] there exists a Galois subring $S$ such that $R$ is the ring homomorphic image of the skew-polynomial ring $S\{x_1, \ldots, x_t; \sigma_1, \ldots, \sigma_t\}$, where $x_i$ are noncommuting variables and, for each $i$, $\sigma_i$

is an automorphism of $S$ satisfying $sx_i = x_i\sigma_i(s)$ for all $s \in S$. We show that the nilpotency of the group of units of the local ring $R$ is equivalent to the fact that the Galois coefficient ring is a subring of the centre of $R$, and prove that every finite local ring $R$ such that $R/J(R)$ is isomorphic to the field $\mathbb{Z}_p$, has a nilpotent group of units.

In the next section we improve the first result of [3]. By studying basic rings, we prove that for an arbitrary finite ring $R$, the group $G(R)$ is nilpotent if and only if $R$ is a direct sum of polynomial rings in noncommuting variables over Galois rings, and basic rings $S$, such that $S/J(S)$ is a direct sum of fields with two elements, and we also describe the structure of such basic rings. Finally, we describe the connection between the nilpotency of the group $G(R)$ and the action of $G(R)$ on the set of primitive idempotents of $R$, which yields a decomposition of $R$, where the only noncommutative factors are exactly the upper triangular matrices with entries from the field $\mathbb{Z}_2$ and a vector space $V$ over $\mathbb{Z}_2$.

## 2. Local rings with a nilpotent group of units

In this section we find all finite local rings with a nilpotent group of units. So, let $R$ be an arbitrary finite local ring with maximal ideal $J$ and residue field $k$. By [5, Theorem XIX.6], there exists a Galois coefficient ring $S$ of $R$ such that $R = S[a_1, \ldots, a_t; \sigma_1, \ldots, \sigma_t]$, where $t = \dim_k(J/J^2)$ for suitable automorphisms $\sigma_i$ of $S$, and $a_1 + J^2, \ldots, a_t + J^2$ determine a $k$-basis of $J/J^2$.

LEMMA 2.1. *Let $R$ be a finite local ring and let $S$ and $t$ be as above. Also, let $x = g + p(a_1, \ldots, a_t)$ and $y = h + q(a_1, \ldots, a_t)$ be two arbitrary units, where $p$ and $q$ are polynomials with coefficients in $S$ and zero constant term, and $g$ and $h$ are units in $S$. (Note that every unit in $R$ is of such form by the above remark.) If $S$ is a subring of the centre of $R$, then $[x, y] = 1 + [p', q'] + [p', q'](p' + q') + \cdots$, where $p' = g^{-1}p$ and $q' = h^{-1}q$.*

PROOF. Since $J$ is nilpotent and $p' = g^{-1}p, q' = h^{-1}q \in J$, we can write $x^{-1} = (1 - p' + p'^2 - \cdots)g^{-1}$ and $y^{-1} = (1 - q' + q'^2 - \cdots)h^{-1}$. Since $S$ is central, we can write $[x, y] = (1 + p')(1 + q')(1 - p' + p'^2 - \cdots)(1 - q' + q'^2 - \cdots)$ and now a simple calculation yields the result. □

THEOREM 2.2. *Let $R$ be a finite local ring. Let $n_H$ denote the order of nilpotency of an arbitrary nilpotent subgroup $H \leq G(R)$ and let $m$ denote the order of nilpotency of the Jacobson radical $J(R)$. Then the following two statements are equivalent:*

(1) *the Galois coefficient ring of $R$ is a subring of the centre of $R$;*
(2) *$G(R)$ is nilpotent.*

*In this case, $n_{G(R)} = n_{1+J(R)} \leq m - 1$ and $n_{G(R)} \leq \min\{k;\ J(R)^k \subseteq Z(J(R))\}$.*

https://doi.org/10.1017/S0004972708001019 Published online by Cambridge University Press

PROOF. Let $S$ denote the Galois coefficient ring of $R$.

If $G(R)$ is nilpotent, then $S$ is a subring of the centre of $R$ by [3, Theorem 1.8].

On the other hand, let us assume that $S$ is a subring of $R$ and take arbitrary elements $x = g + p(a_1, \ldots, a_t)$ and $y = h + q(a_1, \ldots, a_t)$ in $G(R)$. (Thus, $g, h \in G(R)$ and $p, q \in J(R)$.) We know, by Lemma 2.1, that

$$[x, y] = 1 + [g^{-1}p, h^{-1}q] + [g^{-1}p, h^{-1}q](g^{-1}p + h^{-1}q) + \cdots).$$

However, since $[g^{-1}p, h^{-1}q] = 0$ if and only if $[p, q] = 0$ and since $1 + J(R)$ is a $p$-group and therefore nilpotent, we can conclude that $G(R)$ is also nilpotent and the order of its nilpotency is equal to the order of nilpotency of $1 + J(R)$. Now, all of the above inequalities follow immediately. □

COROLLARY 2.3. *Let $R$ be a finite local ring such that $R/J(R)$ is isomorphic to the field $\mathbb{Z}_p$, then $G(R)$ is nilpotent.*

PROOF. By the above theorem, we only need to prove that the Galois coefficient ring $S$ is contained in the centre of $R$. This is true, because we know from [5, Theorem XIX.4] that $S$ equals $\mathbb{Z}_{p^k}$ (up to an inner automorphism of $R$). □

The proof of the following lemma can be extracted from the first paragraph of the proof of Proposition 1.4 in [3], but we include it here for the sake of completeness.

LEMMA 2.4. *Let $R$ be a ring such that at least one factor of the semisimple ring $R/J(R)$ is a proper matrix ring over a field, then $G(R)$ is not nilpotent.*

PROOF. If $G(R)$ is nilpotent, then it is solvable. The ring $R/J(R)$ is a direct sum of simple rings and each factor is isomorphic to $M_n(D)$ for some skew field $D$. Therefore, $G(D)$ is solvable, so $D$ is a field by the result of Hua in [4]. The solvability of $GL_n(D)$ now implies that either $n = 1$ or $n = 2$ and $D = GF(2)$ or $D = GF(3)$ (see, for instance, [2]). However, $GL_2(D)$ is not nilpotent, so each direct summand has to be a field. □

## 3. Basic rings with a nilpotent group of units

Recall that the ring $R$ is called basic if $R/J(R)$ is a direct sum of fields. First, we examine all such rings $R$, that at most one field of those present in the decomposition of $R/J(R)$ is isomorphic to $\mathbb{Z}_2$.

THEOREM 3.1. *Let $R$ be a basic ring such that at most one factor of the semisimple ring $R/J(R)$ is the field $\mathbb{Z}_2$. If the group of units of $R$ is nilpotent, then $R$ is a direct sum of local rings that are homomorphic images of polynomial rings $GR(p^n, r)\{x_1, \ldots, x_t\}$ in noncommuting variables.*

PROOF. The ring $R$ is a direct sum of local rings by [3, Theorem 2.2] and by [3, Theorem 1.8] each direct summand is a homomorphic image of a polynomial ring, as described above. □

https://doi.org/10.1017/S0004972708001019 Published online by Cambridge University Press

COROLLARY 3.2. *Let $R$ be a basic ring such that $R/J(R)$ is $\mathbb{Z}_{p_1} \oplus \cdots \oplus \mathbb{Z}_{p_k}$, and at most one of the factors is $\mathbb{Z}_2$. Then $G(R)$ is nilpotent if and only if $R$ is a direct sum of local rings.*

PROOF. We have one implication by the above theorem. The other follows from Corollary 2.3 since a direct sum of nilpotent groups is nilpotent. □

Now, let us examine rings $R$, such that $R/J(R)$ is isomorphic to the ring $\bigoplus_{k=1}^{n} \mathbb{Z}_2$.

THEOREM 3.3. *Let $R$ be a basic ring such that $R/J(R)$ is a direct sum of $n \geq 2$ fields with two elements, then $G(R)$ is nilpotent. Furthermore, every element of $R$ is a sum of an idempotent and an element from the group*

$$((e_1 + e_1 J(R) e_1) \ltimes ((1 - e_1) J(R) e_1)) \ldots ((e_n + e_n J(R) e_n) \ltimes ((1 - e_n) J(R) e_n)),$$

*where $\{e_1, \ldots, e_n\}$ is a set of primitive orthogonal idempotents. Also, each subring $e_i R e_i$ is a homomorphic image of a polynomial ring in noncommuting variables.*

PROOF. We note that $G(R) = 1 + J(R)$, because the group of units of $R/J(R)$ is trivial. We can assume that $R$ is indecomposable, since otherwise we can deal separately with each of the factors. So, $R$ is a $p$-ring and therefore $G(R)$ is a $p$-group, hence nilpotent. Now, [1, Theorem 9] tells us that the ring $R$ satisfies idempotent 1-stable range and therefore every element in $R$ is a sum of a unit and an idempotent. We can see this if we take an arbitrary element $x \in R$ and write $xR + (-1)R = R$, thus by the definition of idempotent 1-stable range, there exists an idempotent $e$ such that $x + (-1)e \in G(R)$. So, in our case, we have for an arbitrary $x \in R$ that $x = 1 + e + j$ for an idempotent $e$ and some $j \in J(R)$. Now, let $\{e_1, \ldots, e_n\}$ be a set of orthogonal primitive idempotents in $R$. From [6, Corollary 1.8], we have that $1 + J(R) = (1 + e_1 J(R)) \ldots (1 + e_n J(R))$ and by [6, Proposition 1.10] we know that every group $1 + e_i J(R)$ is a semidirect product of the group $e_i(1 + e_i J(R))e_i = e_i + e_i J(R) e_i$ with an abelian group

$$\begin{aligned} &\{(1 - e_i)(1 + j)e_i;\ j \in J(R),\ (1 - e_i)(1 + j)(1 - e_i) = 1 - e_i\} \\ &\quad = \{(1 - e_i) j e_i;\ j \in J(R),\ (1 - e_i) j (1 - e_i) = 0\}. \end{aligned}$$

This latter group has to be viewed as an additive subgroup of $R$, and the action of $e_i + e_i J(R) e_i$ is induced by left multiplication. Now, let us examine the ring $eRe$ for some primitive idempotent $e$. By [5, Theorem VII.4], we see that $J(eRe) = eJ(R)e$, thus $eRe/J(eRe)$ is a field with two elements. By [6, Lemma 1.4] and the fact that every idempotent preserves the group $1 + Q$ for every quasi-invertible ideal $Q$ in $R$, we know that $eG(R)e \subseteq G(eRe)$, but since $eRe$ is a local ring and its group of units is equal to $e + J(eRe) = e(1 + J(R))e$, we can conclude that $G(eRe) = eG(R)e = e + eJ(R)e$. Since $eJ(R)e$ is an additive subgroup of $J(R)$, we see that $G(eRe)$ is also a $p$-group and therefore, by Theorem 3.1, the ring $eRe$ is a homomorphic image of the polynomial ring $GR(p^n, r)\{x_1, \ldots, x_t\}$ in noncommuting variables. □

Let us now combine all of our findings into the following theorem.

https://doi.org/10.1017/S0004972708001019 Published online by Cambridge University Press

THEOREM 3.4. *Let $R$ be an arbitrary finite ring. Then $G(R)$ is nilpotent if and only if $R$ is a direct sum of either local rings that are homomorphic images of polynomial rings $GR(p^n, r)\{x_1, \ldots, x_t\}$ in noncommuting variables and their centre contains the Galois coefficient ring, or rings, described in Theorem 3.3.*

PROOF. If $R$ is a direct sum of rings, described above, then $G(R)$ is nilpotent, because the group of units of every direct summand is nilpotent by Theorems 3.3 and 2.2. Now, assume that $G(R)$ is nilpotent. We know that $R$ is a basic ring by Corollary 2.4. Let $n$ denote the number of fields in the decomposition of the ring $R/J(R)$ into a direct sum of fields. Let $n_2$ denote the number of those fields, that are isomorphic to $\mathbb{Z}_2$. If $n_2 \leq 1$ or $n_2 = n$, then the theorem holds as a direct consequence of Theorems 3.1 and 3.3. Now, let us assume that $R$ is indecomposable (otherwise we take an indecomposable component of $R$). Therefore, $R$ is a $p$-ring, so $R/J(R)$ is a direct sum of $p$-fields. If $p > 2$, then the theorem holds by Theorem 3.1. So, let us assume that $p = 2$ and $1 < n_2 < n$. If we can find a nontrivial idempotent $\overline{e} \in R/J(R)$ such that $\overline{e}$ is a sum of units in $R/J(R)$, then we can proceed as in the proof of [3, Proposition 1.4]. However, such a nontrivial idempotent exists in all cases when $n_2 < n$, since we can take 0 in a one fixed (say, last) component (that is not $\mathbb{Z}_2$) and 1 in every other component. Such an element can be written as a sum of units of the form $(1, 1, \ldots, x)$, where $x$ runs over every nonzero element of the last component, since there is an odd number of such elements and their sum equals zero in every field with more than two elements. So, we can find a nontrivial idempotent $e$ in $R$ that commutes with all units. Since the units generate all elements of $R$, except those whose cosets in $R/J(R)$ have a nontrivial element in the part that falls into the sum of fields with two elements, we only have to examine these sorts of elements. Namely, every element of $R$, taken modulo $J(R)$, is a sum of a unit and a (possibly trivial) idempotent $\overline{f}$ that only has possible nonzero elements in the components belonging to the fields $\mathbb{Z}_2$. So, let us take such an idempotent $\overline{f}$ and lift it to the idempotent $f \in R$. Let us prove that $ef(1-e) = 0$. By the definition of $e$, the element $f(1-e)$ belongs to $J(R)$ (because $1 - e$ modulo $J(R)$ has zeros at those places that belong to the sum of fields $\mathbb{Z}_2$). Therefore $ef(1-e) = f(1-e)e = 0$, since $e$ centralizes $G(R)$ and $1 + J(R)$ is a subgroup of $G(R)$. We have proved that $eR(1-e) = 0$ and similarly we see that $(1-e)Re = 0$. This now yields the following decomposition of $R$, $R = eRe \oplus (1-e)R(1-e)$, which contradicts the assumption that $R$ is indecomposable. Therefore, we either have $n_2 = n$ or $n_2 \leq 1$ and thus the theorem is proved. □

COROLLARY 3.5. *Let $R$ be a finite ring with a nilpotent group of units and a commutative Jacobson radical such that for every pair of orthogonal idempotents $e$, $f \in R$ either $eJ(R)f = 0$ or $|eJ(R)f| > |[e]|$, where by $[e]$ we denote the orbit of the conjugate action of the group $G(R)$ on the set of all idempotents of $R$. Then $R$ decomposes as a direct sum of commutative local rings and rings isomorphic to the ring*

$$\left\{ \begin{bmatrix} a & c \\ 0 & b \end{bmatrix} \,\middle|\, a, b \in \mathbb{Z}_2, c \in V \right\}$$

*for some vector space $V$ over $\mathbb{Z}_2$.*

https://doi.org/10.1017/S0004972708001019 Published online by Cambridge University Press

PROOF. By the previous theorem, we know that we can decompose $R$ into a direct sum of local rings. Now, all of those direct summands are commutative rings by [3, Corollary 1.10]. So, we can assume that $R$ is a ring, as described in Theorem 3.3. Let $e$ and $f$ denote orthogonal idempotents in $R$ that were lifted from two orthogonal idempotents in $R/J(R)$. Take an arbitrary $x \in R$. Then $e + exf = aea^{-1}$ for some $a \in G(R)$ because of [5, Theorem VII.13] and the fact that this equation holds modulo $J(R)$. So, $exf = aea^{-1}f$ and since $a = 1 + j$ and $a^{-1} = 1 + j'$ for some $j, j' \in J(R)$ and the fact that $J(R)$ is commutative,

$$exf = ea^{-1}f + jej'f = ea^{-1}f + j'fae = ea^{-1}f,$$

since $fae = 0$. If $a \neq 1$, then by assumption $fRe = 0$. If $a = 1$ for some $x \neq 0$, then by assumption $eRf = 0$. Now, if $eRf = fRe = 0$, then $R$ is directly indecomposable and $eRe$ is a local ring for a primitive idempotent $e$, therefore commutative by [3, Corollary 1.10]. Otherwise, we see that there are at most two nontrivial idempotents $e$, $f$ in $R$ such that $eJ(R)f = J(R)$ and therefore $R$ is a $2 \times 2$ matrix ring

$$\left\{ \begin{bmatrix} a & c \\ 0 & b \end{bmatrix} \middle| \, a, b \in \mathbb{Z}_2, c \in V \right\}$$

for some vector space $V$ over $\mathbb{Z}_2$. □

## References

[1] H. Chen, 'Rings with many idempotents', *Internat. J. Math. Math. Sci.* **22**(3) (1999), 547–558.
[2] J. Dieudonne, *La géométrie des groupes classiques* (Springer, New York, 1971).
[3] G. Groza, 'Artinian rings having a nilpotent group of units', *J. Algebra* **121** (1989), 253–262.
[4] L. K. Hua, 'On the multiplicative group of a field', *Acad. Sinica Sci. Record* **3** (1950), 1–6.
[5] B. R. McDonald, *Finite Rings with Identity* (Marcel Dekker, New York, 1974).
[6] P. Pavešič, 'Factorization of units and groups of stable homotopy equivalences', *J. Pure Appl. Algebra* **172**(2–3) (2002), 271–284.

DAVID DOLŽAN, Department of Mathematics, University of Ljubljana,
Jadranska 21, Ljubljana 1000, Slovenia
e-mail: david.dolzan@fmf.uni-lj.si

https://doi.org/10.1017/S0004972708001019 Published online by Cambridge University Press