

COMPLEMENTATION OF THE JACOBSON GROUP IN A MATRIX RING

DAVID DOLŽAN

The Jacobson group of a ring R (denoted by $\mathcal{J} = \mathcal{J}(R)$) is the normal subgroup of the group of units of R (denoted by $G(R)$) obtained by adding 1 to the Jacobson radical of R ($J(R)$). Coleman and Easdown in 2000 showed that the Jacobson group is complemented in the group of units of any finite commutative ring and also in the group of units of a $n \times n$ matrix ring over integers modulo p^s , when $n = 2$ and $p = 2, 3$, but it is not complemented when $p \geq 5$. In 2004 Wilcox showed that the answer is positive also for $n = 3$ and $p = 2$, and negative in all the remaining cases. In this paper we offer a different proof for Wilcox's results and also generalise the results to a matrix ring over an arbitrary finite commutative ring. We show this by studying the generators and relations that define a matrix ring over a field. We then proceed to examine the complementation of the Jacobson group in the matrix rings over graded rings and prove that complementation depends only on the 0-th grade.

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 of X . We denote the group of units of R by $G = G(R)$ and the Jacobson radical of R by $J = J(R)$. The ring of $n \times n$ matrices over ring R is denoted by $M_n(R)$, and the ring of integers modulo m is denoted by \mathbb{Z}_m . The reader is assumed familiar with the theory of finite rings (as presented in [4]).

Let $\mathcal{J} = \mathcal{J}(R) = 1 + J(R)$ denote the Jacobson group of R . We say that the Jacobson group is complemented in $G(R)$ if $G(R)$ is a semidirect product of the normal subgroup \mathcal{J} and some other subgroup G .

It is known that the Jacobson group is complemented in finite local rings of any characteristic ([4, Theorem 18.2]) and in any finite ring of prime characteristic ([4, Corollary 21.7]). Then [1, Corollary 2.7] tells us that the Jacobson group is complemented in the group of units of any finite commutative ring. In the paper we give the answer for all matrix rings over a finite ring.

It was shown in [1] that for $s \geq 2$ the Jacobson group of $M_n(\mathbb{Z}_{p^s})$ is complemented when $n = 2$ and $p = 2$ or 3 and is not complemented when $p \geq 5$. In the first section

Received 4th July, 2005

Copyright Clearance Centre, Inc. Serial-fee code: 0004-9727/05 \$A2.00+0.00.

we show, by studying the generators and relations that define the factor ring $M_n(F)$, where F is a field, that the complementation also fails for $M_n(R)$ where R is any finite, commutative, local ring of characteristic p^s ($s \geq 2$), if $p \geq 5$, if $p = 2$ and $n \geq 4$ or, if $p = 3$ and $n \geq 3$. For the case $R = \mathbb{Z}_{p^s}$, the result was obtained in [7], but with a different proof. We show that the Jacobson group is complemented in case of $p = 2$ and $n \leq 3$ for any ring R such that $R/J(R)$ is isomorphic to \mathbb{Z}_2 and it is complemented in case of $p = 3$ and $n \leq 2$ for any ring R such that $R/J(R)$ is isomorphic to \mathbb{Z}_3 . We do this by studying the properties of the semidirect product of the two groups and the implication of the cohomology of groups to the complementation of groups.

It is worth noting that this result answers the complementation problem for all rings $M_n(R)$, where R is any finite commutative ring, since it is well known that such a ring R can be written as a direct sum of local rings, and then this case boils down to the complementation in each of the direct summands.

In the next section we turn our investigation to the ring of $n \times n$ matrices over graded rings. We prove that the complementation depends only on the 0-th grade.

2. MATRICES OVER FINITE, COMMUTATIVE, LOCAL RINGS

Let R be a finite local commutative ring of characteristic p^s , where p is a prime and s is an integer. Let n be an integer. We begin our investigation of the Jacobson group of $M_n(R)$ by the following two simple lemmas, which can be easily proved.

LEMMA 2.1. *The Jacobson radical of $M_n(\mathbb{Z}_{p^s})$ equals $M_n(p\mathbb{Z}_{p^s})$.*

LEMMA 2.2. *Let R be as above. Then $G(M_n(R))/\mathcal{J}(M_n(R))$ is isomorphic to $GL_n(F)$, where F is a finite field of characteristic p .*

As it was shown in [1], $\mathcal{J}(M_n(\mathbb{Z}_{p^s}))$ is complemented in $G(M_n(\mathbb{Z}_{p^s}))$ when $n = 2$ and $p = 2$ or 3 for every s , and is not complemented when $n \geq 2$, $s \geq 2$ and $p \geq 5$. It was shown in [4] that $\mathcal{J}(M_n(R))$, where R is a finite local commutative ring of characteristic p^s , is complemented for all p and n , when $s = 1$. So, let us assume that $s \geq 2$ and $n \geq 2$. We shall now prove that the group is complemented if and only if either $n \leq 3$, $p = 2$ and $R/J(R)$ is isomorphic to \mathbb{Z}_2 , or $n = 2$, $p = 3$ and $R/J(R)$ is isomorphic to \mathbb{Z}_3 . Due to the fact that any finite commutative ring is a direct sum of local rings and the fact that the Jacobson group is always complemented in the group of units of a commutative ring, this now yields the complete answer to the question of complementation of Jacobson group in the case of $n \times n$ matrices over R for all n and for all finite commutative rings R .

The following proposition and its immediate corollary will be useful.

PROPOSITION 2.3. *Let L be a finite commutative ring such that there exists a surjective homomorphism $f : R \rightarrow L$ with the property that its kernel is a sub-*

set of $J(R)$. Then, if $\mathcal{J}(M_n(R))$ is complemented in $GL_n(R)$, $\mathcal{J}(M_n(L))$ is also complemented in $GL_n(L)$.

PROOF: Assume that $GL_n(R) = H(1 + J(R))$, with $H \cap (1 + J(R)) = \{1\}$. Then, $GL_n(L) = f(H)f(1 + J(R))$, since f maps units into units. Now, $f(1 + J(R))$ is a subset of $1 + J(L)$, but since f is surjective and every unit is an image of a unit, we get $J(L) \subseteq f(J(R))$, so $f(1 + J(R)) = 1 + J(L)$. We now only have to prove that $f(H) \cap (1 + J(L)) = \{I\}$. Choose $\alpha \in f(H) \cap f(1 + J(R))$. Then $\alpha = f(\beta) = f(\gamma)$ for some $\beta \in H$ and some $\gamma \in 1 + J(R)$. It follows that $f(\beta^{-1}\gamma) = I$, so $I - \beta^{-1}\gamma \in \text{Ker}(f) \subseteq J(R)$. Therefore $\beta - \gamma \in J(R)$, so $\beta \in H \cap (1 + J(R)) = \{I\}$ and thus $\alpha = I$. □

COROLLARY 2.4. *If $\mathcal{J}(R)$ is complemented in $G(R)$, then $\mathcal{J}(R/J(R)^2)$ is also complemented in $G(R/J(R)^2)$.*

If we assume that G is a semidirect product of $1 + J$ and some other group H , it will be of some importance to know what properties H possesses.

LEMMA 2.5. *Let $G = H \rtimes 1 + J$. If $a \in H$ and $0 \neq j \in J$, then $a + j \notin H$.*

PROOF: Choose $a \in H$ and $0 \neq j \in J$. Then $a + j = a(1 + a^{-1}j)$, so if $a + j \in H$, we also get $1 + a^{-1}j \in H \cap (1 + J)$, therefore $j = 0$, which contradicts our assumptions. □

The following theorem is a generalisation of [1, Theorem 4.5].

THEOREM 2.6. *Let R be a finite local commutative ring of characteristic p^s , where $p \geq 5$. Then the Jacobson group of $M_n(R)$ is not complemented for any $n \geq 2$.*

PROOF: Let R be a finite local commutative ring of characteristic p^s , where $p \geq 5$. Let $S = R/J(R)^2$. By Corollary 2.4, it suffices to show that $\mathcal{J}(S)$ is not complemented. Since the characteristic of R is p^s , it follows that p is in the Jacobson radical of R , therefore we can assume that $p^2 = 0$ in S . If we suppose $\mathcal{J}(S)$ is complemented by H in $GL_n(S)$, then we can proceed in the similar way as in the proof of [1, Theorem 4.5], by taking the matrix

$$A = \begin{bmatrix} \alpha & 0 \\ 0 & I \end{bmatrix}, \quad \text{where } \alpha = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

and writing $A = BC$ for $B \in H$ and $C \in \mathcal{J}(S)$. We show that $B^p \in H \cap \mathcal{J}(S)$ and by using [1, Lemma 4.4] we show that $B^p \neq 1$. □

LEMMA 2.7. *Let $R = M_n(S)$ for some local ring S and assume that $G(R) = H \rtimes \mathcal{J}(R)$. Let $f : R \rightarrow R/J(R)$ be the canonical homomorphism. Then $f(H) \simeq GL_n(F)$, where $f \simeq S/J(S)$.*

PROOF: Clearly $f(G(R)) \simeq GL_n(F)$ and $f(\mathcal{J}(R)) = I$. □

Now, let us examine the ring $M_n(R)$, where the characteristic R is 2^s or 3^s . By Corollary 2.4 we can assume that $s = 2$.

PROPOSITION 2.8. *Suppose that the characteristic of the finite local commutative ring R is 2^s and that $J(R)^2 = 0$. Suppose also that the Jacobson group of $M_2(R)$ is complemented by a group H . If*

$$A = \begin{bmatrix} \lambda & r \\ t & \mu \end{bmatrix} \in H$$

is of the form $I + \alpha E_{ij} (i \neq j)$ modulo the Jacobson radical, then $t = 0$ and $\mu = -\lambda$.

PROOF: Since A is of the form $I + \alpha E_{ij}$ modulo the Jacobson radical, we can easily see that $A^2 \in \mathcal{J}(M_2(R)) \cap H$, so $A^2 = I$. But, since we can assume that $J(R)^2 = 0$ and we know that $\lambda, \mu \in \mathcal{J}(R)$ and $r, t \in j(R)$, we get

$$A^2 = \begin{bmatrix} 1+t & \lambda + \mu \\ 0 & 1+t \end{bmatrix} \in H. \quad \square$$

PROPOSITION 2.9. *Suppose that the characteristic of the finite local commutative ring R is 3^s and that $J(R)^2 = 0$. Suppose also that the Jacobson group of $M_2(R)$ is complemented by a group H . If*

$$A = \begin{bmatrix} \lambda & r \\ t & \mu \end{bmatrix} \in H$$

is of the form $I + \alpha E_{ij} (i \neq j)$ modulo the Jacobson radical, then $t = -3$.

PROOF: Since $A^3 \in \mathcal{J}(M_2(R)) \cap H$, we know that $A^3 = I$. But since $J(R)^2 = 0$ and since

$$A^3 = \begin{bmatrix} 1 & \lambda^2 + \lambda\mu + \mu^2 + t \\ 0 & 1 \end{bmatrix},$$

where $\lambda, \mu \in \mathcal{J}(R)$, we see that $\lambda^2 + \lambda\mu + \mu^2 = 3$, so $t = -3$. □

This now immediatley yields the following result.

COROLLARY 2.10. *Let S be a ring of upper triangular $n \times n$ matrices over a finite local commutative ring R . Then $\mathcal{J}(S)$ is complemented in $G(S)$ if and only if the characteristic of R is a power of 2 and $n = 2$.*

The following theorem is the key to obtaining our results.

THEOREM 2.11. *Let R be a finite local commutative ring $F = GF(p^r)$ its residue field and $S = M_n(R)$ for an integer n . Then $\mathcal{J}(S)$ is compemented in $G(S)$ if and only there exists a p -SyLOW subgroup H of G , such that $\mathcal{J}(S)$ is complemented by H in some subgroup of G .*

PROOF: $\mathcal{J}(S)$ is complemented in $G(S)$ if and only if thre exists a subgroup of N of G , such that N is isomorphic t $GL_n(F)$. So, N has exactly $p^{rn(n-1)/2} \prod_{i=1}^n (p^{ri} - 1)$

elements. Now, [3, Corollary 9.8.3] tells us that for an Abelian group A and a finite group N , the exact sequence $1 \rightarrow A \rightarrow X \rightarrow N \rightarrow 1$ splits if and only if for every Sylow subgroup H of N , the extension of A by H splits. Assume first that $J(S)^2 = 0$. Thus, $\mathcal{J}(S)$ is Abelian. However, for every prime $q \neq p$, the order of q -Sylow subgroups of N is relatively prime to the order of $\mathcal{J}(S)$, so therefore all those Sylow subgroups are automatically complemented by the Schur–Zassenhaus lemma (see for example, [6, Theorem 7.15]). Therefore, we only need to find the complement for one p -Sylow subgroup H of N , since every other p -Sylow subgroup is a conjugate of H and \mathcal{J} is normal. If $J(S)^2 \neq 0$, the above implies that $G(S/J(S)^2)$ contains some group isomorphic to $GL_n(F)$. Now, by our assumption $G(S)$ contains groups H_j , isomorphic to all the Sylow subgroups of $GL_n(F)$, and the group H generated by all those subgroups, is isomorphic to $GL_n(F)$ modulo $J(S)^2$. Therefore, all we need to see is that $H \cap (1 + J(S)^2) = 1$. Choose $h_1 h_2 \dots h_k \in 1 + J(S)^2$, where every h_i belongs to one of the groups H_j . Therefore $h_1^{-1} - h_2 \dots h_k \in J(S)^2$, so h_1 belongs to the same Sylow subgroup modulo $J(S)^2$ as $h_2 \dots h_k$. But all groups H_j have a trivial intersection with $1 + J(S)^2$, so h_1 and $h_2 \dots h_k$ belong to the same H_j . Therefore, their product is also in H_j and it has to equal 1 □

So, all we need to find is one subgroup of G , which is isomorphic to some p -Sylow subgroup of $GL_n(F)$.

THEOREM 2.12. *Let R be a finite local commutative ring of characteristic 2^s for some integer $s \geq 2$ and $S = M_n(R)$ for an integer n . The $\mathcal{J}(S)$ is complemented in $G(S)$ if and only if $n \leq 3$ and $R/J(R)$ is isomorphic to \mathbb{Z}_2 .*

PROOF: First, assume that $\mathcal{J}(S)$ is complemented in $G(S)$ by some group H , and prove that $R/J(R)$ has to be isomorphic to \mathbb{Z}_2 . Let $0 \neq t_1, t_2 \in R/J(R)$. Then, by Proposition 2.8, we have the following equation in H :
$$\begin{bmatrix} \lambda & t_1 \\ 0 & -\lambda \end{bmatrix} \begin{bmatrix} \mu & t^2 \\ 0 & -\mu \end{bmatrix} = \begin{bmatrix} \lambda\mu & \lambda t_2 - \mu t_1 \\ 0 & \lambda\mu \end{bmatrix}$$
, and therefore $\lambda t_2 - \mu t_1 = 0$. However, since $\lambda, \mu \in 1 + J(R)$, we have $(\lambda t_2 - \mu t_1) - (t_2 - t_1) \in J(R)$ and thus $t_1 = t_2$ by Lemma 2.5.

If $n = 2$ then, by the previous theorem, we only need to find the 2-Sylow subgroup H_2 in G . Obviously, we can choose $H_2 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} \right\}$ and by definition $\mathcal{J}(S)$ is complemented by H_2 in some subgroup of G

Assume now that $n = 3$. We have to find the 2-Sylow subgroup H_3 in G . We can construct H_3 as a semi-direct product of the group $\left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\}$

and the following group $\left\{ \begin{bmatrix} -1 & 0 & 0 \\ -\alpha - 1 & 1 & \alpha \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & \alpha \\ 0 & -1 & -\alpha - 1 \\ 0 & 0 & 1 \end{bmatrix} \right\}$, where α is an element in $1 + J(R)$ such that $a^2 + a + 2 = 0$. (Such an element exists by Hensel's lemma.) One can check that this is really a 2-Sylow subgroup in G .

Now, if $n \geq 4$ we can assume that $s = 2$ by Corollary 2.4. Should the group H_4 exist, it would be isomorphic to the semi-direct product of H_3 and the group V_4 of all 4×4 matrices that have only the last column nontrivial, modulo $J(S)^2$. But since we know the structure of H_3 , we can check that such a group V_4 cannot be imbedded as a normal group into $GL_4(R)$. For example, if we choose an element $\alpha \in V_4$ such that

$$\alpha = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \pmod{J(S)},$$

then the conjugation by the elements of H_3 should

preserve it. As a short calculation shows, this cannot be achieved, no matter how we choose to imbed V_4 into $GL_4(R)$. □

Now, the only characteristic left is a power of 3. The next theorem deals with this case.

THEOREM 2.13. *Let R be a finite local commutative ring of characteristic 3^s for some integer $s \geq 2$ and $S = M_n(R)$ for an integer $n > 1$. Then $\mathcal{J}(S)$ is complemented in $G(S)$ if and only if $n = 2$ and $R/J(R)$ is isomorphic to \mathbb{Z}_3 .*

PROOF: Let us choose an arbitrary matrix $A \in H$, which maps to the matrix $I + E_{kn}$ by the isomorphism modulo the Jacobson radical. Thus, A has the following block structure:

$$A = \begin{bmatrix} I_{n-1} + J_1 & e_k + J_2 \\ J_3 & 1 + w \end{bmatrix},$$

with $e_k, w, I_{n-1}, J_1, J_2, J_3$ as before. Lemma 2.5 this time implies that $A^3 = I$, since $A^3 = I$ holds modulo the Jacobson radical. If we calculate the cube of A , considering that by Corollary 2.4 the equation $J(R)^2 = 0$ also holds, we notice that

$$A^3 = \begin{bmatrix} * & J_1^{(k)} + \lambda e_k \\ * & * \end{bmatrix},$$

for some $\lambda \in R$, where $J_1^{(k)}$ denotes the k -th column of J_1 . This of course implies that J_1 is zero outside the diagonal. Now we can use Proposition 2.9 to establish that H_3 cannot exist, so that $n = 2$. Therefore

$$A = \begin{bmatrix} 1 + \lambda & g \\ j & 1 + \mu \end{bmatrix},$$

with $j, \lambda, \mu \in J(R)$ and $g \in G(R)$ is an arbitrary element in G_2 . So

$$A^3 = \begin{bmatrix} 1 & 3g + jg^2 \\ 0 & 1 \end{bmatrix},$$

but on the other hand $A^3 = I$. Therefore $3g + jg^2 = 0$ and since g is a unit, $jg = -3$. Now choose also

$$B = \begin{bmatrix} 1 + \lambda' & g' \\ j' & 1 + \mu' \end{bmatrix} \in G_2,$$

with some $j', \lambda', \mu' \in J(R)$ and $g' \in G(R)$. We know that $AB \in G_2$ so if $B \neq A^{-1}$, we can conclude that $(j + j')(g(1 + \lambda') + g'(1 + \mu)) = -3$. Since $j = -3g^{-1}$ and $j' = -3g'^{-1}$, this further implies that $1 + g^{-1}g' + g'^{-1}g \in J(R)$. Now, multiply the equation with gg' and examine it modulo $J(R)$. Let h and h' denote g and g' , respectively, modulo $J(R)$. We get $hh' + h'^2 + h^2 = 0$ for every $h, h' \in F = R/J(R)$. If we choose for example $h' = 1$, then we see that we can find at most two solutions h for the equation, since this is a quadratic equation over a field. Because it can also be true that $AB = I$, we find that there can really be at most three elements in F . But if $|F| = 3$, then G_2 is also a group of 3 elements, so we can choose

$$G_2 = \left\{ I, \begin{bmatrix} -5 & 7 \\ -3 & 4 \end{bmatrix}, \begin{bmatrix} 4 & -7 \\ 3 & -5 \end{bmatrix} \right\}.$$

It can be easily verified that G_2 is the desired group, not only for $s = 2$, but for an arbitrary s . □

3. MATRICES OVER GRADED RINGS

In this section we turn our investigation to rings $M_n(R)$, where $R = \bigoplus_{i=0}^{\infty} S_i$. It turns out that one can tell a lot about complementation in $M_n(R)$ just from the complementation in the ring of matrices over S_0 . The following theorem holds.

THEOREM 3.1. *Let $R = \bigoplus_{i=0}^{\infty} S_i$ be a graded ring and $n \geq 1$. Then the Jacobson group of $M_n(R)$ is complemented if and only if the Jacobson group of $M_n(S_0)$ is complemented.*

PROOF: Assume that $\mathcal{J}(M_n(S_0))$ is complemented by some group H in $GL_n(S_0)$. Therefore $\mathcal{J}(M_n(R)) = 1 + M_n(J(R))$ and $GL_n(R) = GL_n(S_0) + M_n(J(R))$. So, $\mathcal{J}(M_n(R))$ is complemented by the same group H in $GL_n(R)$. Conversely, suppose $A \in GL_n(S_0)$ has a decomposition $A = BC$, for some $B \in H$ and $C \in \mathcal{J}(M_n(R))$, where $\mathcal{J}(M_n(R))$ is complemented by H in $GL_n(R)$. Let A_0 denote the 0-th grade matrix of A . Then $A = A_0 = B_0C_0$ and it is easy to see that the matrix C_0 lies in

$\mathcal{J}(M_n(S_0))$, since the Jacobson radical of S_0 is exactly the 0-th grade of the Jacobson radical of R . Let H_0 denote the set of all such matrices B_0 for all possible decompositions of an arbitrary matrix $A \in GL_n(S_0)$. Observe that H_0 is a group. We only need to check that $H_0 \cap \mathcal{J}(M(S_0)) = \{I\}$, since then $\mathcal{J}(M(S_0))$ will be complemented by H_0 . But $\mathcal{J}(M_n(S_0)) \subseteq \mathcal{J}(M_n(R))$ and $H_0 \cap \mathcal{J}(M_n(R)) = \{I\}$, which concludes the proof of our theorem. \square

This, along with the results of the previous section, now gives us the following result.

COROLLARY 3.2. *Let $R = \bigoplus_{i=0}^{\infty} S_i$ be a graded ring, where S_0 is a finite local commutative ring of characteristic p^3 for some integers $s \geq 1$. Let $n \geq 1$. Then the Jacobson group of $M_n(R)$ is complemented if and only one of the following holds:*

1. $s = 1$,
2. $n = 2$,
3. $p = 2$, $n \leq 3$ and $S_0/J(S_0)$ is isomorphic to \mathbb{Z}_2 .
4. $p = 3$, $n = 2$ and $S_0/J(S_0)$ is isomorphic to \mathbb{Z}_3 .

PROOF: By the previous theorem we only need to examine the complementation in $M_n(S_0)$. The result now follows from the results of the previous section. \square

REMARK. Again, when S_0 is an arbitrary finite commutative ring, one can write S_0 as a direct sum of local rings and then use the above theorem to examine the complementation in that case.

REFERENCES

- [1] C. Coleman and D. Easdown, 'Complementtionin the group of units of a ring', *Bull. Austral. Math. Socl.* **62** (2000), 183–192.
- [2] M. Hall, *The theory of groups* (Macmillan, New York, 1959).
- [3] G. Karpilovsky, *Group representations, Vol 1* (Elsevier Science Publishers B.V., Amsterdam, 1992).
- [4] B.R. McDonald, *Finite rings with identity* (Marcel Dekker Inc., New York).
- [5] R. Raghavendran, 'Finite associative rings', *Compositio Math.* **21** (1969), 195–229.
- [6] J.J. Rotman, *The theory of groups, an introduction* (Allyn and Bacon, Inc., Boston, 1971).
- [7] S. Wilcox, 'Complementation in the group of units of matrix rings', *Bull. Austral. Math. Soc.* **70** (2004), 223–227.

Department of Mathematics
University of Ljubljana
Jadranska 19
Ljubljana 1000
Slovenia