Complementation in the group of units of a ring

Clare Coleman and David Easdown

August 20, 1999

Abstract

By adding 1 to elements of the nilradical and Jacobson radical of a ring with identity, normal subgroups of the group of units are obtained. In this paper we record observations about complementation of these subgroups in the group of units of a ring, identifying large classes where complementation takes place and some examples where it fails.

1 Introduction and preliminaries

Throughout let R denote a ring with identity and denote by $\mathcal{N}(R)$, $\mathcal{J}(R)$ and $G(R)$ its nilradical, Jacobson radical and group of units respectively. Observe that $N(R) = \{1 + x | x \in \mathcal{N}(R)\}$ and $J(R) = \{1 + x | x \in \mathcal{J}(R)\}$ are normal subgroups of $G(R)$, which we refer to as the *nil* and *Jacobson groups* respectively of R. Recall that R is *local* if R is commutative and has a unique maximal ideal M, in which case any field isomorphic to R/M may be referred to as the *residue field* of R.

Recall that if H is a normal subgroup of a group G then a *complement* for H in G is a subgroup K of G such that $G = HK$ and $H \cap K = \{1\}$, in which case $K \cong G/H$ and G is a semidirect product of H by K. It is natural to ask when $N(R)$ and $J(R)$ have complements in $G(R)$, thereby yielding semidirect product decompositions.

If R has characteristic $n = p_1^{t_1} \dots p_s^{t_s}$ where $p_1, \dots, p_s$ are distinct primes and $t_1, \dots, t_s \geq 1$, then it is easy to see that

$$R \cong (R/p_1^{t_1}R) \oplus \dots \oplus (R/p_s^{t_s}R) ,$$

so that R decomposes as a direct sum of rings of prime power characteristic. Consider rings R_1 and R_2, and let $\mathcal{K} = \mathcal{N}$ or $\mathcal{J}$ and $K = N$ or J respectively. If $X \subseteq R_1$, $Y \subseteq R_2$ then denote by $X \oplus Y$ the subset $\{(x, y) | x \in X, y \in Y\}$ of $R_1 \oplus R_2$. Then $\mathcal{K}(R_1 \oplus R_2) = \mathcal{K}(R_1) \oplus \mathcal{K}(R_2)$, from which it follows that, as sets, $K(R_1 \oplus R_2) = K(R_1) \oplus K(R_2)$, so that

$$K(R_1 \oplus R_2) \cong K(R_1) \times K(R_2)$$

(direct product of groups). Moreover if $K(R_i)$ has a complement H_i in $G(R_i)$ for $i = 1, 2$, then the subset $H_1 \oplus H_2$ is a subgroup of $G(R_1 \oplus R_2)$ which is easily seen to be a complement for $K(R_1) \oplus K(R_2)$. Thus for rings of positive characteristic the question of complementation of the nil or Jacobson groups is reduced to questions about rings of prime power characteristic.

If R is finite then $N(R) = J(R)$. It is known that the Jacobson group is complemented in finite local rings of any characteristic [**?**, Theorem 18.2] and in any finite ring of prime characteristic [**?**, Corollary 21.7]. In Section 2, we record some facts about binomial coefficients, which enable us to investigate complementation of the nil group for a large class of commutative rings. In Section 3, we consider complementation of the Jacobson group for a class of matrix rings over local rings, the main tool being an adaptation of Gaussian elimination. In the final section of this paper we give a class of finite matrix rings in which the Jacobson group is never complemented, and a class in which complementation always occurs, exhibiting the complement explicitly.

We complete the preliminaries by giving a lemma, the proof of which is an easy exercise, and an example of an infinite ring in which the Jacobson group is not complemented (though the nil group, being trivial, is complemented).

Lemma 1.1. *For any ring R,*

$$G(R)/J(R) \cong G(R/\mathcal{J}(R)) .$$

In particular, if R is local with residue field K, then

$$G(R)/J(R) \cong K^* .$$

Example 1.2. Let p be an odd prime and put

$$R = \{a/b \in \mathbb{Q} \mid p \text{ does not divide } b\} .$$

Then R is a local ring with unique maximal ideal

$$\mathcal{J}(R) \;=\; \{a/b \in R \mid p \text{ divides } a\}$$

and residue field $R/\mathcal{J}(R) \;\cong\; \mathbb{Z}_p$. Thus, if $J(R)$ has a complement H in $G(R)$ then, by Lemma 1.1, $H \;\cong\; G(R)/J(R) \;\cong\; \mathbb{Z}_p^*$, so that $G(R)$ contains nontrivial elements of finite order. But all nonidentity elements of $G(R)$ have infinite order. This proves that $J(R)$ has no complement in $G(R)$.

2 Commutative rings

In this section we prove that the nil group is complemented in the group of units of a commutative ring with positive characteristic under the condition that the group of units is finitely generated or periodic.

Lemma 2.1. *Suppose that* $t \geq 2$ *and* $0 \leq i < 2^{t-2}$. *Then*

$$2\binom{2^{t-1}}{2i+1} \;\equiv\; 0 \mod 2^t\,.$$

Proof. The result is clear if $i = 0$. If $i > 0$ then

$$\begin{aligned} 2\binom{2^{t-1}}{2i+1} \;&=\; \frac{2^t(2^{t-1}-2)\ldots(2^{t-1}-2i)}{(2i)(2i-2)\ldots(2)}\,\frac{k}{l} \\ &=\; \frac{2^t(2^{t-2}-1)\ldots(2^{t-2}-i)}{i!}\,\frac{k}{l} \;=\; 2^t\binom{2^{t-2}}{i}\,\frac{k}{l} \end{aligned}$$

which is divisible by 2^t, where $k = (2^{t-1}-1)(2^{t-1}-3)\ldots(2^{t-1}-(2i-1))$ and $l = (2i+1)(2i-1)\ldots(1)$, since l is odd. □

Lemma 2.2. *Let* p *be a prime and suppose that* $t \geq 1$ *and* $0 \leq i < p^{t-1}$. *Then*

$$\binom{p^t}{pi} \;\equiv\; \binom{p^{t-1}}{i} \mod p^t\,.$$

Proof. The result is clear if $i = 0$. Suppose $i > 0$. Observe that

$$\binom{p^t}{pi} \;=\; \frac{p^{t-1}(p^{t-1}-1)\dots(p^{t-1}-(i-1))}{i!}\,\frac{k}{l} \;=\; \binom{p^{t-1}}{i}\,\frac{k}{l}$$

where $\; k \;=\; \prod_{j=1\,,\,p\nmid j}^{pi-1} (p^t - j) \;$ and $\; l \;=\; \prod_{j=1\,,\,p\nmid j}^{pi-1} j \;$, and so

$$\binom{p^t}{pi} - \binom{p^{t-1}}{i} \;=\; \binom{p^{t-1}}{i}\,\frac{k-l}{l}\,.$$

But

$$k \;\equiv\; \prod_{j=1\,,\,p\nmid j}^{pi-1} -j \;=\; (-1)^{(p-1)i}\, l \qquad \bmod p^t\,.$$

If $p = 2$ and i is odd then $k \equiv -l \mod 2^t$ so

$$(k-l)\binom{p^{t-1}}{i} \;\equiv\; 2k\binom{2^{t-1}}{i} \;\equiv\; 0 \qquad \bmod\ 2^t$$

by Lemma 2.1. If p is odd or i is even then $k \equiv l \mod p^t$, so again

$$(k-l)\binom{p^{t-1}}{i} \;\equiv\; 0 \qquad \bmod\ p^t\,.$$

But l is not divisible by p, so we conclude that

$$\binom{p^t}{pi} - \binom{p^{t-1}}{i} \;\equiv\; 0 \qquad \bmod p^t\,.$$

□

Lemma 2.3. *Let* p *be a prime and suppose that* $t \geq 1$, $0 \leq i < p^{t-1}$ *and* $1 \leq k \leq p-1$. *Then*

$$\binom{p^t}{pi+k} \;\equiv\; 0 \quad \bmod p^t\,.$$

Proof. Put

$$\alpha_\ell \;=\; \begin{cases} \prod_{j=0}^{i} \; p^t - (pj+\ell) & \text{for } \; 1 \le \ell < k \;, \\[2ex] \prod_{j=0}^{i-1} \; p^t - (pj+\ell) & \text{for } \; k \le \ell \le p-1 \;, \end{cases}$$

$$\beta_\ell \;=\; \begin{cases} \prod_{j=0}^{i} \; pj+\ell & \text{for } \; 1 \le \ell \le k \;, \\[2ex] \prod_{j=0}^{i-1} \; pj+\ell & \text{for } \; k < \ell \le p-1 \;. \end{cases}$$

Then

$$\begin{aligned} \binom{p^t}{pi+k} &= \frac{p^t(p^t-p)\dots(p^t-pi)}{pi(pi-p)\dots p} \, \frac{\alpha_1\dots\alpha_{p-1}}{\beta_1\dots\beta_{p-1}} \\[2ex] &= p^t \binom{p^{t-1}-1}{i} \frac{\alpha_1\dots\alpha_{p-1}}{\beta_1\dots\beta_{p-1}} \quad \equiv \quad 0 \mod p^t \end{aligned}$$

since $\beta_1\dots\beta_{p-1}$ is not divisible by p. □

Lemma 2.4. *Let R be a ring of characteristic p^t where p is prime and $t \ge 1$. Suppose that $g \in R$ and $k \ge t$. Then, for $s = 0, \dots, k-t+1$,*

$$(1-g)^{p^k} \;=\; (1-g^{p^s})^{p^{k-s}} \;.$$

Proof. Observe, applying Lemmas 2.1, 2.2 and 2.3, that

$$\begin{aligned} (1-g)^{p^t} &= \sum_{i=0}^{p^t} (-1)^i \binom{p^t}{i} g^i \;=\; \sum_{i=0}^{p^{t-1}} (-1)^{pi} \binom{p^t}{pi} g^{pi} \\ &= \sum_{i=0}^{p^{t-1}} (-1)^i \binom{p^{t-1}}{i} g^{pi} \;=\; (1-g^p)^{p^{t-1}} \;. \end{aligned}$$

The result now follows by a straightforward induction. □

Theorem 2.5. *Let R be a commutative ring of characteristic p^t where p is prime and $t \geq 1$. Suppose that $G(R)$ is finitely generated or periodic. Then $N(R)$ has a complement in $G(R)$.*

Proof. Observe that $G(R)$ is an abelian group and put

$$P = \{g \in G(R) \mid g \text{ has order a power of } p\} .$$

Then P has a complement H in $G(R)$, by [**?**, Theorems 3.2.2 and 3.2.2]. It suffices then to prove that $P = N(R)$. If $g \in P$ then $g^{p^\alpha} = 1$ for some $\alpha \geq 1$, so, by Lemma 2.4,

$$(1-g)^{p^{\alpha+t-1}} \quad = \quad (1-g^{p^\alpha})^{p^{t-1}} \quad = \quad 0 \, ,$$

so that $1 - g \in \mathcal{N}(R)$, whence $g \in N(R)$. Conversely, if $g \in N(R)$ then $(1-g)^\beta = 0$ for some $\beta \geq 1$, so, choosing $s \geq 0$ such that $p^s \geq \beta$ gives $(1-g)^{p^s} = 0$ and, by Lemma 2.4,

$$g^{p^{s+t-1}} \quad = \quad (1-(1-g))^{p^{s+t-1}} \quad = (1-(1-g)^{p^s})^{p^{t-1}} \quad = 1 \, ,$$

so that $g \in P$. This proves $N(R) = P$. $\square$

Corollary 2.6. *The nil group is complemented in the group of units of any commutative ring of positive characteristic in which the group of units is finitely generated or periodic.*

Proof. This follows by Theorem 2.5 and the comments in Section 1 about reducing the question of complementation in rings of positive characteristic to prime power characteristic. $\square$

Corollary 2.7. *The Jacobson group is complemented in the group of units of any finite commutative ring.*

3 Matrices over a local ring

In this section we prove that the Jacobson group is complemented in the group of units of a matrix ring over a local ring such that the residue field is a subring which does not properly embed in itself. This includes, for example, matrix rings over group algebras $K[A]$, where K is a transcendental extension of a finite field F of characteristic p, where K has finite transcendence degree over F, and A is any abelian p-group.

Denote by $M_n(R)$ the ring of $n \times n$ matrices over R, and by $\iota = \iota_n$ the $n \times n$ identity matrix. Note that $\mathcal{J}(M_n(R)) = M_n(\mathcal{J}(R))$.

Lemma 3.1. *Let R be a local ring with residue field K. Then*

$$G(M_n(R))/J(M_n(R)) \;\cong\; \mathrm{GL}_n(K)\;,$$

the general linear group over K.

Proof. By Lemma 1.1,

$$\begin{aligned} G(M_n(R))/J(M_n(R)) \;&\cong\; G(M_n(R)/\mathcal{J}(M_n(R))) \;=\; G(M_n(R)/M_n(\mathcal{J}(R))) \\ &\cong\; G(M_n(R/\mathcal{J}(R))) \;\cong\; G(M_n(K)) \;=\; \mathrm{GL}_n(K)\,. \end{aligned}$$

□

Lemma 3.2. *Let R be a local ring in which the residue field K is a subring, and suppose that K does not properly embed in itself. Then K^* is a complement for $J(R)$ in $G(R)$.*

Proof. There is an isomorphism $\phi : R/\mathcal{J}(R) \to K$. Denote the natural map $: R \to R/\mathcal{J}(R)$ by ν. Clearly $\nu_{|_K} : K \to R/\mathcal{J}(R)$ is injective, so $\nu_{|_K}\phi : K \to K$ is an embedding, which, by the hypothesis, must be an isomorphism. Hence $\nu_{|_K}$ is onto. Thus, if $g \in G(R)$, then $g + \mathcal{J}(R) = k + \mathcal{J}(R)$ for some $k \in K^*$, so $k^{-1}g - 1 = k^{-1}(g - k) \in \mathcal{J}(R)$, so that $k^{-1}g \in J(R)$, yielding $g = k(k^{-1}g) \in K^*J(R)$. Thus $G(R) = K^*J(R)$. If $x \in K^* \cap J(R)$ then $x = 1 + y$ for some $y \in \mathcal{J}(R)$, so $y = x - 1 \in \mathcal{J}(R) \cap K = \{0\}$, so $x = 1$. Thus $K^* \cap J(R) = \{1\}$, which proves that K^* is a complement for $J(R)$ in $G(R)$.

□

Theorem 3.3. *Let R be a local ring in which the residue field K is a subring, and suppose that K does not properly embed in itself. Let $n \geq 1$. Then $J(M_n(R))$ is complemented in $G(M_n(R))$ by the general linear group $\mathrm{GL}_n(K)$.*

Proof. Put

$$G \;=\; G(M_n(R)) \;=\; \{\alpha \in M_n(R) \mid \det\alpha \in G(R)\}\;,$$

$$J \;=\; J(M_n(R)) \;=\; \{\iota_n + \alpha \mid \alpha \in \mathcal{J}(M_n(R)) = M_n(\mathcal{J}(R))\}\;,$$

$$H \;=\; \mathrm{GL}_n(K) \;=\; \{\alpha \in M_n(K) \mid \det\alpha \neq 0\}\;.$$

Certainly H is a subgroup of G and $H \cap J = \{\iota_n\}$. To prove the theorem it suffices to prove $G = HJ$. For $0 \le k \le n$, put

$$G_k = \left\{ \text{partitioned matrices } \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in G \;\middle|\; A \in J(M_k(R)),\ C \text{ has entries in } \mathcal{J}(R) \right\},$$

with certain data interpreted vacuously when $k = 0$ or n, so that $G_0 = G$ and $G_n = J$.

Let $0 \le k < n$. We will prove that $G_k \subseteq HG_{k+1}$. Let

$$\alpha = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in G_k$$

where $A \in J(M_k(R))$ and C has entries in $\mathcal{J}(R)$. If all of the entries in the first column of D lie in $\mathcal{J}(R)$ then it follows that $\det\alpha \in \mathcal{J}(R)$, contradicting that $\alpha \in G$. Hence at least one entry in the first column of D lies in $G(R)$, since R is local. Hence there is a permutation matrix $\beta \in H$ such that

$$\beta\alpha = \begin{pmatrix} A & B \\ C' & D' \end{pmatrix} \in G_k$$

and the first entry d of D' lies in $G(R)$. By Lemma 3.2, $d = \lambda(1 + j)$ for some $\lambda \in K^*$ and $j \in \mathcal{J}(R)$. Let τ be the diagonal elementary matrix with λ^{-1} in the $(k + 1)$th position on the diagonal. Then

$$\tau\alpha\beta = \begin{pmatrix} A & B \\ C'' & D'' \end{pmatrix} \in G_k$$

where the first entry of D'' is $1 + j$.

Denote the ith entry of the $(k+1)$th column of $\tau\alpha\beta$ by a_i, so $a_{k+1} = 1+j$. Consider $i \ne k + 1$. If $a_i \in \mathcal{J}(R)$ then put $\sigma_i = \iota_n$. If $a_i \notin \mathcal{J}(R)$ then $a_i \in G(R)$, since R is local, so, by Lemma 3.2, $a_i = \lambda_i(1 + j_i)$ for some $\lambda_i \in K^*$ and $j_i \in \mathcal{J}(R)$, in which case we define σ_i to be the elementary matrix corresponding to the elementary row operation which subtracts $\lambda_i \times ((k + 1)\text{th row})$ from the ith row. Then

$$\sigma_1 \ldots \sigma_n \beta\alpha \in G_{k+1} ,$$

so that $\alpha \in HG_{k+1}$, since $\sigma_1 \ldots \sigma_n \beta \in H$. This proves $G_k \subseteq HG_{k+1}$. It follows by induction that

$$G = G_0 = HG_n = HJ ,$$

which completes the proof that H is a complement for J in G.

$\square$

4 Matrices over $\mathbb{Z}_{p^k}$

In this section we prove that the Jacobson group of $M_n(\mathbb{Z}_{p^k})$ is complemented in the group of units when $p = 2$ or 3, $n = 2$ and $k \geq 1$. On the other hand, we prove that it is never complemented when p is a prime ≥ 5, $k \geq 2$ and $n \geq 2$. Note that, by Lemma 3.1, if a complement for $J(M_n(\mathbb{Z}_{p^k}))$ in $G(M_n(\mathbb{Z}_{p^k}))$ exists then it is a copy of $\mathrm{GL}_n(\mathbb{Z}_p)$.

Lemma 4.1. *Let p be an odd prime and $k \geq 1$. Then all elements of $1+p\mathbb{Z}_{p^k}$ are perfect squares in $\mathbb{Z}_{p^k}$.*

Proof. If $a, b \in 1 + \mathbb{Z}_{p^k}$ and $a^2 = b^2$ in $\mathbb{Z}_{p^k}$ then $(a + b)(a - b) = 0$, so that $a - b = 0$, since $a + b$ is invertible. Hence the squaring function : $1 + p\mathbb{Z}_{p^k} \to 1 + p\mathbb{Z}_{p^k}$ is one-one, and so onto. $\square$

Lemma 4.2. *Let $k \geq 1$. Then there exists an integer α such that $\alpha \equiv 2 \mod 3$ and $\alpha^2 \equiv -2 \mod 3^k$.*

Proof. By Lemma 4.1, since $-2 \in 1 + 3\mathbb{Z}$, there exists an integer β such that $\beta \equiv 1 \mod 3$ and $\beta^2 \equiv -2 \mod 3^k$. Then $\alpha = 3^k - \beta$ has the required properties. $\square$

Theorem 4.3. *The Jacobson group is complemented in the group of units of $M_2(\mathbb{Z}_{p^k})$ for $k \geq 1$ and $p = 2, 3$.*

Proof. Put $R = \mathbb{Z}_{p^k}$, $J = J(M_2(R))$ and $G = G(M_2(R))$. Then R is a local ring with residue field $\mathbb{Z}_p$. When $k = 1$, $R = \mathbb{Z}_p$, so J is trivial. We suppose then that $k > 1$. By Lemma 3.1,

$$|J|\,|\mathrm{GL}_n(\mathbb{Z}_p)| = |G| ,$$

so to find a complement for J in G, it suffices to find a subgroup H such that $H \cap J = \{\iota_n\}$ and $|H| = |\mathrm{GL}_n(\mathbb{Z}_p)|$.

If $p = 2$ then, putting

$$H = \left\{ \iota_2 \, , \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} , \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} , \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} , \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} , \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \right\} ,$$

it is easy to check that H is a subgroup of G, $H \cap J = \{\iota_2\}$ and $|H| = 6 = |\mathrm{GL}_2(\mathbb{Z}_2)|$, whence H is a complement for J in G.

Suppose that $p = 3$. By Lemma 4.2, there exists an integer α such that $\alpha \equiv 2 \mod 3$ and $\alpha^2 \equiv -2 \mod 3^{k+1}$. Put $H = \langle s, t, q \rangle$ where

$$s = \begin{pmatrix} -5 & 7 \\ -3 & 4 \end{pmatrix} \ , \ q = \begin{pmatrix} -1 & 3 \\ 0 & 1 \end{pmatrix} \ , \ t = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

for

$$a = 3(1 - \alpha) \ , \quad c = 2(1 - \alpha) \ , \quad b = (-14 + 13\alpha)/3 \ ,$$

interpreted as elements of $\mathbb{Z}_{3^k}$. Note that, as an integer, the numerator of b is divisible by 3, so that b is sensibly defined. The reader may verify immediately that

$$s^3 = q^2 = \iota \ , \quad qsq = s^2 \ , \quad qtq = t^3 \ .$$

A further, though much longer calculation, verifies that

$$t^2 = (st)^3 = (sts^2t)^2 \ .$$

By [**?**, page 95], these equations are just the relations in a presentation for $\mathrm{GL}_2(\mathbb{Z}_3)$ using generators q, s, t. Hence H is a homomorphic image of $\mathrm{GL}_2(\mathbb{Z}_3)$. Let $\Phi : M_2(\mathbb{Z}_{3^k}) \to M_2(\mathbb{Z}_3)$ where, for $\alpha \in M_2(\mathbb{Z}_{3^k})$, $\alpha\Phi$ is the matrix obtained by evaluating the entries of α in $\mathbb{Z}_3$. Then Φ is a ring epimorphism and $\iota_2\Phi^{-1} = J$. Further

$$s\Phi = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \ , \ q\Phi = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \ , \ t\Phi = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

generate $\mathrm{GL}_2(\mathbb{Z}_3)$. Thus also $\mathrm{GL}_2(\mathbb{Z}_3)$ is a homomorphic image of H under Φ, whence $\Phi_{|_H}$ is a group isomorphism. In particular $|H| = |\mathrm{GL}_2(\mathbb{Z}_3)|$. Also $H \cap J \subseteq \ker \Phi_{|_H} = \{\iota_2\}$. This proves H is a complement for J in G. $\square$

We now turn to a large class of rings where complementation fails. The following lemma may be proved by straightforward induction.

Lemma 4.4. *Let p be an integer and $a, b, c \in \mathbb{Z}_{p^2}$. Then, for $k \geq 3$, we have, evaluating entries in $\mathbb{Z}_{p^2}$,*

$$\begin{pmatrix} 1+pa & 1+pb \\ pc & 1+pd \end{pmatrix}^k = \begin{pmatrix} 1+p(ka+\binom{k}{2}c) & k+p(\binom{k}{2}a+kb+\binom{k}{3}c+\binom{k}{2}d) \\ p(kc) & 1+p(kd+\binom{k}{2}c) \end{pmatrix} .$$

Theorem 4.5. *The Jacobson group is not complemented in the group of units of $M_n(\mathbb{Z}_{p^k})$ for $n \geq 2$, $k \geq 2$ and primes $p \geq 5$.*

Proof. Put $R = \mathbb{Z}_{p^k}$, $J = J(M_n(R))$, $G = G(M_n(R))$ and suppose J is complemented by H in G. Let $\Phi : M_n(R) \to M_n(\mathbb{Z}_{p^2})$ where, for $\alpha \in R$, $\alpha\Phi$ is the matrix obtained by evaluating entries in $\mathbb{Z}_{p^2}$. Then $J\Phi = J(M_n(\mathbb{Z}_{p^2}))$ and $G\Phi = (H\Phi)(J\Phi) = G(M_n(\mathbb{Z}_{p^2}))$.

Suppose $\alpha \in H\Phi \cap J\Phi$. Then $\alpha = \beta\Phi = \gamma\Phi$ for some $\beta \in H$, $\gamma \in J$, so $\beta\gamma^{-1} - \iota \in \ker\Phi = M_n(p^2R) \subseteq \mathcal{J}(M_n(R))$, yielding $\beta\gamma^{-1} \in J$. Hence $\beta \in \gamma J \subseteq J$, so $\beta \in J \cap H = \{\iota\}$, so $\alpha = \iota$. This shows $J\Phi$ is complemented by $H\Phi$ in $G\Phi$.

Consider the partitioned matrix

$$\alpha \;=\; \begin{pmatrix} A & 0 \\ 0 & \iota_{n-2} \end{pmatrix} \qquad \text{where} \qquad A \;=\; \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

(interpreted so that $\alpha = A$ if $n = 2$), regarded as an element of $M_n(\mathbb{Z}_{p^2})$. Observe that $\alpha^p \in J\Phi$. But $\alpha \in G\Phi$, so $\alpha = \beta\gamma$ for some $\beta \in H\Phi$, $\gamma \in J\Phi$, and

$$\beta^p(J\Phi) = [\beta(J\Phi)]^p = [\beta\gamma(J\Phi)]^p = [\alpha(J\Phi)]^p = \alpha^p J\Phi = J\Phi \ .$$

Hence $\beta^p \in (J\Phi) \cap (H\Phi) = \{\iota\}$, so β has order dividing p. But

$$\gamma \;=\; \begin{pmatrix} C & D \\ E & F \end{pmatrix}$$

for some matrices C, D, E, F such that C is 2×2 and entries of D and E are over $p\mathbb{Z}_{p^2}$. Note that the product of any two matrices over $p\mathbb{Z}_{p^2}$ of appropriate dimensions is a zero matrix. Hence

$$\beta^p = (\alpha\gamma^{-1})^p = \begin{pmatrix} AC & AD \\ E & F \end{pmatrix}^p = \begin{pmatrix} (AC)^p & D' \\ E' & F' \end{pmatrix}$$

for some matrices D', E', F'. But AC is of the form

$$\begin{pmatrix} 1+pa & 1+pb \\ pc & 1+pd \end{pmatrix}$$

for some $a, b, c, d \in \mathbb{Z}_{p^2}$. By Lemma 4.4,

$$(AC)^p \quad = \quad \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \quad \neq \quad \iota_2 \ ,$$

so $\beta^p \neq \iota_n$, contradicting that the order of β divides p. This proves the theorem. $\square$

The reader might note (not unexpectedly in light of Theorem 4.3), that, for $p = 3$, the previous argument breaks down when $c = -1$ in the above expression for AC. The authors do not know whether the Jacobson group is complemented in the group of units of $M_n(\mathbb{Z}_{p^k})$ when $n > 2$, $p = 2$ or 3 and $k > 1$.

References

[1] H. S. M. Coxeter and W. O. J. Moser, *Generators and relations for discrete groups* (Springer-Verlag, Berlin, 1972).

[2] M. Hall, *The theory of groups* (Macmillan, New York, 1959).

[3] B. McDonald, *Finite rings with identity* (Marcel Dekker, Inc., New York, 1974).

School of Mathematics and Statistics
University of Sydney, NSW 2006, Australia
cec@maths.usyd.edu.au, de@maths.usyd.edu.au