THE n-INSERTIVE SUBGROUPS OF UNITS

DAVID DOLŽAN

Let \( R \) be a finite ring. Let us denote its group of units by \( G = G(R) \) and its Jacobson radical by \( J = J(R) \). Let \( n \) be an arbitrary integer. We prove that \( R \) is an \( n \)-insertive ring if and only if \( G \) is an \( n \)-insertive group and show that every \( n \)-insertive finite ring is a direct sum of local rings. We prove that if \( n \) is a unit, then the local ring \( R \) is \( n \)-insertive if and only if its Jacobson group \( 1 + J \) is \( n \)-insertive and find an example to show that this is not true if \( n \) is a non-unit.

1. INTRODUCTION

Many properties of finite rings follow from the properties of their groups of units. For example, it was shown in [1] that a finite ring is commutative if and only if its group of units is commutative. The notion of commutativity can be generalised to the notion of \( n \)-insertiveness, as shown below. In this paper, we study the link between the \( n \)-insertiveness of a finite ring and the \( n \)-insertiveness of its group of units.

So, let \( R \) be a finite ring with identity \( 1 \neq 0 \). Denote the group of units of \( R \) by \( G = G(R) \) and the Jacobson radical of \( R \) by \( J = J(R) \).

If \( n \) is an integer, we call \( R \) an \( n \)-insertive ring if, for \( a, b \in R \) and \( ab = n \), we have \( arb = nr \) for every \( r \in R \). Let \( H \) be a subgroup of \( G \). We call \( H \) an \( n \)-insertive group if, for \( a, b \in R \) and \( ab = n \), we have \( agb = ng \) for every \( g \in H \).

**Lemma 1.1.** \( G \) is \( 1 \)-insertive if and only if \( G \) is commutative.

**Proof:** Assume that \( G \) is \( 1 \)-insertive. Choose \( a \in G \) and denote \( b = a^{-1} \). Since \( G \) is \( 1 \)-insertive, we have \( ab = 1 \) and \( agb = g \) for every \( g \in G \). Therefore \( ag = gb^{-1} = ga \) for every \( g \in G \), so \( G \) is commutative.

On the other hand, if \( G \) is commutative, then \( R \) is commutative by a corollary of [1, Theorem 3.2]. This implies that \( R \), and then of course also \( G \), is \( 1 \)-insertive.

We know by [3, Lemma 1] that \( R \) is \( 1 \)-insertive if and only if \( R \) is commutative. A corollary of [1, Theorem 3.2] tells us that \( R \) is commutative if and only if \( G \) is commutative. So, the above lemma implies that \( G \) is \( 1 \)-insertive if and only if \( R \) is \( 1 \)-insertive.

We prove that for every integer \( n \) the following holds: \( G \) is \( n \)-insertive if and only if \( R \) is \( n \)-insertive. We prove this by studying the structure of \( n \)-insertive rings, showing...
that every $n$-insertive ring (for an arbitrary integer $n$) is a direct sum of local rings. We also show that the converse of this statement is false. Namely, we find a local ring that is not $n$-insertive for any integer $n$.

The group $1 + J$ is a normal subgroup of $G$, called the Jacobson group. We study whether the $n$-insertiveness of $1 + J$ is equivalent to the $n$-insertiveness of $R$. Obviously, the answer is negative in general (consider for example the full matrix ring over some finite field). However, we prove that the answer is affirmative if $R$ is a local ring and $n$ is a unit. We also find an example of a non $n$-insertive local ring $R$ with a $n$-insertive Jacobson group (for every integer non-unit $n$ in $R$), thus proving that the above equivalence does not hold for an arbitrary $n$, even in the class of local rings.

2. THE PROPERTIES OF $n$-INSERTIVE RINGS

**Theorem 2.1.** Let $n$ be an arbitrary integer. If $G$ is $n$-insertive, then $R$ is a direct sum of local rings.

**Proof:** Assume that $R$ is a directly indecomposable ring. Assume also that $R$ is not local. Then there exists a non-trivial idempotent $e_1 \in R$. Denote $e_2 = 1 - e_1$. Since $R$ is indecomposable, we either have $e_1Re_2 \neq 0$ or $e_2Re_1 \neq 0$, otherwise we would be able to decompose $R$ as $R = e_1Re_1 \oplus e_2Re_2$. We can assume without any loss of generality that $e_1xe_2 \neq 0$ for some $x \in R$. Now, $(e_1 + ne_2)(ne_1 + e_2) = n$, so by our assumption $(e_1 + ne_2)g(ne_1 + e_2) = ng$ for every $g \in G$. Clearly, $1 + e_1xe_2 \in G$, since $(e_1xe_2)^2 = 0$. But $(e_1 + ne_2)(1 + e_1xe_2)(ne_1 + e_2) = n + e_1xe_2$, therefore $(n - 1)e_1xe_2 = 0$. We can therefore conclude that $n - 1 \notin G$. However, $R$ is indecomposable, therefore it is a $p$-ring for some prime number $p$. Since $n - 1$ is a multiple of $p$, we can conclude that $n$ has to be prime to $p$, and thus $n$ must be a unit. Let us show that $G$ is then 1-insertive. Choose $a, b \in R$ such that $ab = 1$ and choose $g \in G$. Then $a(bn) = n$ and therefore $agbn = gn$, so $agb = g$, because $n$ is a unit. So, Lemma 1.1 implies that $G$ is Abelian and therefore $R$ is commutative by [1, Theorem 3.2]. This, together with the existence of $e_1$, is a contradiction with the indecomposability of $R$. Therefore, we can conclude that $R$ is indeed a local ring. □

**Example 2.2.** The converse of the above statement is false. Let $p$ be a prime number and let $R$ be a ring of all $4 \times 4$ upper triangular matrices with entries from $GF(p^2)$, such that their entries on the (main) diagonal are constant. Obviously, $G$ is a non-Abelian group. Therefore $G$ is not 1-insertive and then $G$ is also not $n$-insertive for any integer $n$, prime to $p$, by the proof of Theorem 2.1. If we take $p = 3$, we have

\[
\begin{bmatrix}
0 & 1 & 2 & 0 \\
0 & 0 & 2 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}
\begin{bmatrix}
0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0
\end{bmatrix} = 0, \text{ but}
\]

[https://doi.org/10.1017/S0004972700038958 Published online by Cambridge University Press]
The \( n \)-insertive sugroups of units

So, for \( p = 3 \), \( R \) is a local ring, but \( G \) is not \( n \)-insertive for some integers \( n \) (specifically \( n = 0, 3, 6, \ldots \)).

**Corollary 2.3.** Let \( n \) be an arbitrary integer. Then \( R \) is \( n \)-insertive if and only if \( G \) is \( n \)-insertive.

**Proof:** Since \( G(R_1 \oplus R_2) = G(R_1) \times G(R_2) \), it suffices to prove the corollary only for directly indecomposable rings. So, assume that \( R \) is directly indecomposable and that \( G \) is \( n \)-insertive. Let us prove that \( R \) is \( n \)-insertive. Assume that \( ab = n \) for some \( a, b \in R \) and choose \( r \in R \). By Theorem 2.1, \( R/J \) is a field and therefore \( R/J \) is generated by its units. But then \( R \) is also generated by its units, as was proved in [2, Lemma 4.5]. Thus, \( r = u_1 + \cdots + u_k \) and \( arb = au_1b + \cdots + au_kb = n(u_1 + \cdots + u_k) = nr \), because \( G \) is \( n \)-insertive.

**3. The \( n \)-Insertiveness of the Jacobson Group**

In this section, we examine if the \( n \)-insertiveness of \( R \) is perhaps also equivalent to the \( n \)-insertiveness of the Jacobson group \( 1 + J \). Obviously, in general, the answer is negative, because the Jacobson group of a full matrix ring over some finite field is trivial, and therefore \( 1 \)-insertive, but the ring itself is non-commutative and therefore not \( 1 \)-insertive. However, we shall examine this question in the class of all finite local rings and find that the answer is positive, at least for those integers \( n \) that are units in \( R \).

For a subset \( S \subseteq R \), let \( C(S) = \{ x \in R; xs = sx \text{ for every } s \in S \} \) denote the centraliser of \( S \) in \( R \).

**Lemma 3.1.** Let \( R \) be an arbitrary finite ring and \( n \) an arbitrary integer. If \( n \) is a unit in \( R \), then \( 1 + J \) is \( n \)-insertive if and only if \( J \subseteq C(G) \).

**Proof:** Assume \( 1 + J \) is \( n \)-insertive and choose \( a \in G \). Then \( n(aa^{-1}) = n \), therefore \( na(1 + j)a^{-1} = n(1 + j) \) for every \( j \in J \), thus \( n(aa^{-1} - j) = 0 \). Since \( n \) is a unit, we can conclude that \( aj = ja \) for every \( j \in J \).

Conversely, if \( J \subseteq C(G) \), then \( a(1 + j)b = (1 + j)ab \) for every \( a, b \in G \) and every \( j \in J \), so \( 1 + J \) is indeed \( n \)-insertive.

**Theorem 3.2.** Let \( R \) be a finite local ring and \( n \) an arbitrary integer. If \( n \) is a unit in \( R \), then the following are equivalent:

1. \( R \) is \( n \)-insertive.
2. \( 1 + J \) is \( n \)-insertive.
3. \( R \) is commutative.

https://doi.org/10.1017/S0004972700038958 Published online by Cambridge University Press
PROOF: If \( n \) is a unit and \( R \) is \( n \)-insertive, then \( R \) is also 1-insertive and thus commutative by [3, Lemma 1]. So, it suffices to prove that the \( n \)-insertiveness of \( 1 + J \) implies the commutativity of \( R \). Let us therefore assume that \( 1 + J \) is \( n \)-insertive. We know that, since \( R \) is a finite local ring, the units of the factor field \( R/J \) form a cyclic group, generated by some element \( g + J \) of order \( k \). Then \( G = \bigcup_{i=1}^{k} (g^i + J) \). By the previous lemma we conclude that all elements in \( J \) are also in the centraliser of \( G \), thus \( 1 + J \) is a commutative group, so \( J \) is commutative as well. Thus \( G \) is an Abelian group and therefore \( R \) is a commutative ring by the corollary of [1, Theorem 3.2].

The next example shows that this theorem does not hold if \( n \) is not a unit.

**Example 3.3.** If \( S \) is a ring, then let \( S\{x, y, z\} \) denote the polynomial ring over \( S \) in non-commuting variables. Let us examine the ring

\[
R = \frac{\mathbb{Z}_3\{x, y, z\}}{(x^2 + 1, y^3, z^3, yz, xz, yx - xz, zx - xy)}.
\]

Clearly, this is a finite ring, such that all of its non-units form the unique maximal ideal \( J = (y, z) \), therefore \( R \) is a local ring. We notice that \( J^3 = 0 \), therefore \( 1 + J \) is a 0-insertive group, since \( ab = 0 \) implies \( a, b \in J \). However, \( R \) is not a 0-insertive ring, because we have \( yz = 0 \), but \( yxz = xz^2 \neq 0 \), because \( x \) is a unit and \( z^2 \neq 0 \). The same argument also implies that \( 1 + J \) is \( n \)-insertive and \( R \) is not \( n \)-insertive for every integer \( n \) which is a non-unit in \( R \).

**References**