FINITE RINGS IN WHICH COMMUTATIVITY IS TRANSITIVE

DAVID DOLŽAN, IGOR KLEP, AND PRIMOŽ MORAVEC

Abstract. A ring is called *CT* (*commutative transitive*) if commutativity is a transitive relation on its nonzero elements. Likewise, it is *wCT* (*weakly commutative transitive*) if commutativity is a transitive relation on its *noncentral* elements. The main topic of this paper is to describe the structure of *finite* wCT rings. It is shown that every such ring is a direct sum of an indecomposable noncommutative wCT ring of prime power order, and a commutative ring. Furthermore, finite indecomposable wCT rings are either two-by-two matrices over fields, local rings, or basic rings with two maximal ideals. We characterize finite local rings as generalized skew polynomial rings over coefficient Galois rings; the associated automorphisms of the Galois ring give rise to a *signature* of the local ring. These are then used to further describe the structure of finite local and wCT basic rings.

1. Introduction

A group G is called *commutative transitive* (CT) if for all $x, y, z \in G \setminus \{1\}$,

$$xy = yx \text{ and } yz = zy \text{ imply } xz = zx. \tag{1}$$

This notion was defined and studied by Weisner [13] in 1925. Wu [15] proved in 1998 that finite CT groups are either solvable or simple, thus fixing gaps in Weisner's proof. In the solvable case, they are either abelian or cyclic split extensions of their Fitting subgroups [15]. Finite nonabelian simple CT groups had been classified by Suzuki [12] in 1957. He proved that every finite nonabelian simple CT group is isomorphic to some $\mathrm{PSL}(2, 2^f)$, where $f > 1$. Suzuki's result is considered to have been one of the key steps in the proof of the Odd Order Theorem by Feit and Thompson [6]. Wu's and Suzuki's arguments use deep techniques from cohomology theory and the theory of group representations. On the other hand, the classification of finite-dimensional complex Lie algebras satisfying the CT property is elementary modulo the Levi-Mal'cev decomposition theorem [7].

A relaxation of the above notion is as follows. A group G is called *weakly commutative transitive* (wCT) if for all $x, y, z \in G \setminus Z(G)$, (1) holds. wCT groups are more complicated than CT groups. For a survey of known results see [1]. Finite nonnilpotent wCT groups were characterized by Schmidt [11], and Rocke [10] proved some results on finite wCT p-groups.

The aim of this note is to study these notions in the ring theoretical setting. A noncommutative ring with the commutative transitive property as in (1) has no identity. Adjoining one leads to a ring in which the property (1) holds for all *noncentral* elements, so in this paper we focus our investigation on wCT rings. Some

Date: June 23, 2009.

2000 *Mathematics Subject Classification.* 16P10, 16U80, 16L30, 16N20.

Key words and phrases. finite ring, commutative transitive, abelian centralizer, local ring.

Partial financial support from the state budget by the Slovenian Research Agency is gratefully acknowledged.

of the important examples of wCT rings include free algebras and affine domains of small Gelfand-Kirillov dimension (Example 2) indicating diversity within the class of wCT rings, so there is little hope of obtaining a unifying theory of wCT rings in general. Hence we focus on *finite* wCT rings allowing us to deploy the rich theory of finite rings as developed e.g. in [8], [9], and [14], yet some of the results of Sections 2.1 and 2.2 are valid for finite dimensional algebras over (infinite) fields.

As a sample, we prove that finite simple wCT rings are either fields or algebras of two-by-two matrices over fields. In general, finite wCT rings are direct sums of indecomposable noncommutative wCT rings of prime power order, and commutative rings. We prove that the class of wCT rings is closed under taking factor rings by the Jacobson radical. This implies that finite indecomposable wCT rings are either algebras of two-by-two matrices over fields, local rings, or basic rings with two maximal ideals.

We then focus on *local* wCT rings. Here, the wCT property is equivalent to the wCT property of the group of units of the ring in question. (This fails to hold for general wCT rings.) In order to study the wCT property for local rings, we give a characterization of finite local rings as generalized skew polynomial rings over coefficient Galois rings. The associated automorphisms of the Galois ring used in this description yield an important invariant of the local ring, the so-called *signature*. This is then used to further describe the structure of finite local wCT rings. For such rings R with Jacobson radical J satisfying $\dim J/J^2 = 1$ our results are very definitive, while for general local wCT rings only partial results are obtained. Indeed, we provide evidence supporting our belief that the class of all finite local wCT rings is too diverse to allow for a complete classification.

At the end of the paper we briefly touch upon wCT basic rings. Similar methods are used for describing the structure of these. We prove that the wCT property of a basic ring largely depends on the properties of its coefficient ring.

2. Weakly commutative transitive rings

By analogy with the group case, a ring R is said to be *weakly commutative transitive* (wCT) if for all $x, y, z \in R \setminus Z(R)$, (1) holds. Here $Z(R)$ stands for the center of R.

We start by giving a basic characterization of wCT rings.

Lemma 1. *Let R be a ring. The following are equivalent:*

(i) *R is a wCT ring.*
(ii) *For all $x, z \in R$ and $y \in R \setminus Z(R)$, $xy = yx$ and $yz = zy$ imply $xz = zx$.*
(iii) *If $xy = yx$ then $C_R(x) = C_R(y)$ for $x, y \in R \setminus Z(R)$.*
(iv) *$C_R(x)$ is commutative for all $x \in R \setminus Z(R)$.*

Proof. Let R be a wCT ring and let $x, z \in R$ and $y \in R \setminus Z(R)$ be such that $xy = yx$ and $yz = zy$. If either of x or z belongs to $Z(R)$, then x and z clearly commute. If $x, z \notin Z(R)$, then $xz = zx$ by the wCT property. This shows that (i) implies (ii), whereas (ii) clearly implies (i).

Assume now that (ii) holds. Choose $x, y \in R \setminus Z(R)$ such that $xy = yx$. Then $x \in C_R(y)$, hence $C_R(x) \subseteq C_R(y)$ by our assumption. By the symmetry we conclude that $C_R(x) = C_R(y)$, therefore (ii) implies (iii).

Suppose the ring R satisfies (iii) and choose $x \in R \setminus Z(R)$. Let $y, z \in C_R(x)$. We want to show that y and z commute, thus we may assume that $y, z \notin Z(R)$. By our assumption we get that $C_R(y) = C_R(x) = C_R(z)$, hence $yz = zy$. This yields (iv).

Let R satisfy (iv) and let $x, z \in R$ and $y \in R \setminus Z(R)$ satisfy $xy = yx$ and $yz = zy$. We have that both x and z belong to $C_R(y)$ which is commutative, therefore $xz = zx$. It follows from here that (iv) implies (ii). ∎

Example 2.

(1) Free algebras $k\langle X\rangle$ are wCT. This follows easily from the fact that the centralizer of a nonscalar element of $k\langle X\rangle$ is a polynomial ring in one variable over k; this is Bergman's centralizer theorem (see e.g. [4] or [5, Theorem 6.7.7]).
(2) For an example of a different flavor, each affine domain of Gelfand-Kirillov dimension 2 over an algebraically closed field is wCT [3].
(3) By (2), the first Weyl algebra (over, say, $\mathbb{C}$) is wCT. In contrast with that, higher Weyl algebras are not wCT. Consider the second Weyl algebra $\mathcal{A}_2(k)$ with generators p_1, p_2, q_1, q_2 and defining relations $p_ip_j = p_jp_i$ and $q_jq_i = q_iq_j$ for $i, j = 1, 2$, $p_iq_i - q_ip_i = 1$ and $p_iq_j - q_jp_i = 0$ for $i \neq j$. Then p_1 is not central, commutes with p_2 and q_2, but $p_2q_2 \neq q_2p_2$.
(4) Rings R in which centralizers (of noncentral elements) are minimal, in the sense that for all $x \in R \setminus \{0\}$ ($x \in R \setminus Z(R)$), the centralizer $C_R(x)$ is the subring generated by x, are (w)CT. Such rings were studied and characterized by Bell and Klein in [2]. In particular, they proved that if R is a ring where all noncentral elements have minimal centralizers, then R is either commutative or finite. Furthermore, finite rings with this property are, apart from two exceptions, nil.

The above examples demonstrate a certain richness of the class of general wCT rings, so we restrict our attention to an important subclass, namely finite rings with identity.

2.1. **Simple wCT rings.** In this subsection we classify finite simple wCT rings, using the Wedderburn theorem. We show that these are either fields or 2×2 matrix algebras over a field.

Proposition 3. *Let R be a nontrivial ring with identity.*

(1) *$M_2(R)$ is wCT if and only if R is commutative and zero-divisor free.*
(2) *For $n \geqslant 3$, $M_n(R)$ is not wCT.*

Proof. (1) Suppose R is commutative without zero-divisors. Suppose $xy = yx$ and $yz = yz$ for noncentral $x, y, z \in M_2(R)$. Since we can subtract central elements from x, y, z, we may assume they are of the form $\begin{bmatrix} 0 & * \\ * & * \end{bmatrix}$. In addition to that, each of the matrices x, y, z has at least one nonzero entry. Without loss of generality, replace R by its quotient field.

Case 1: Suppose x_{12} is nonzero. Let $y = \begin{bmatrix} 0 & y_{12} \\ y_{21} & y_{22} \end{bmatrix}$. As $xy = yx$, a straightforward inspection yields two cases. If $y_{12} = 0$, then $y_{21} = y_{22} = 0$ contradicting the choice of y. If $y_{12} \neq 0$, then (since x and y commute) x is a multiple of y. In particular, x commutes with z.

Case 2: Suppose x_{21} is nonzero. By transposing the matrices x, y, z, this case reduces to the previous one.

Case 3: Suppose $x = \begin{bmatrix} 0 & 0 \\ 0 & a \end{bmatrix}$. If y is as in Case 1, then $xy = yx$ implies $y_{12} = y_{21} = 0$. Hence x and z commute.

The three cases considered show that $M_2(R)$ is wCT.

For the converse implication assume $M_2(R)$ is wCT. If R has zero-divisors, i.e., $ab = 0$ for some $a, b \in R \setminus \{0\}$, then with

$$x = \begin{bmatrix} 1 & b \\ 0 & 0 \end{bmatrix}, \quad y = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}, \quad z = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},$$

we have $xy = yx$, $yz = zy$, but $xz \neq zx$. Similarly, if $ab \neq ba$ for some $a, b \in R$, then choose

$$x = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}, \quad y = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad z = \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}.$$

Again, $xy = yx$, $yz = zy$, and $xz \neq zx$.

(2) Consider

$$x = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad y = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad z = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

where the bottom right 0 is the block $(n-2) \times (n-2)$ zero matrix. Then $x, y, z \notin Z(M_n(R))$, $xy = yx$, $yz = zy$ and $xz \neq zx$. ∎

Corollary 4. *Let R be a finite simple wCT ring with identity. Then R is either a field or a 2×2 matrix algebra over a field.*

Proof. An immediate consequence of the Wedderburn theorem and Proposition 3. ∎

It is clear that Corollary 4 also holds when R is a finite dimensional simple wCT algebra.

2.2. **Indecomposable wCT rings.** In the first part of this subsection we show that every finite wCT ring is the direct sum of an indecomposable noncommutative wCT ring of prime power order, and a commutative ring. We then proceed to study indecomposable wCT rings. As the main result we prove that indecomposable finite wCT rings are either simple, local, or basic with two maximal ideals (see Theorem 10).

Proposition 5. *Let $R = R_1 \oplus R_2$ and suppose that R_1 is noncommutative. Then R is wCT if and only if R_2 is commutative and R_1 is wCT.*

Proof. ($\Rightarrow$) As R_1 is a subring of R and $Z(R_1) \subseteq Z(R)$, R_1 is wCT. Suppose that R_2 is not commutative. Choose $x, y \in R_2$ such that $xy \neq yx$. Clearly $x, y \notin Z(R)$. As R_1 is not commutative, there exists $z \in R_1 \setminus Z(R)$. We have that $xz = zx$ and $yz = zy$, and this contradicts the fact that R is a wCT ring.

($\Leftarrow$) Choose $x_i \in R \setminus Z(R)$, $i = 1, 2, 3$, such that $x_1x_2 = x_2x_1$ and $x_2x_3 = x_3x_2$. Write $x_i = r_{1,i} + r_{2,i}$, where $r_{1,i} \in R_1$ and $r_{2,i} \in R_2$, $i = 1, 2, 3$. It follows that the elements $r_{1,i}$ do not belong to the center of R_1, and that $r_{1,1}r_{1,2} = r_{1,2}r_{1,1}$

and $r_{1,2}r_{1,3} = r_{1,3}r_{1,2}$. As R_1 is a wCT ring, we conclude that $r_{1,1}r_{1,3} = r_{1,3}r_{1,1}$, therefore $x_1x_3 = x_3x_1$, as required. ∎

As an application we classify all wCT group algebras over $\mathbb{C}$.

Corollary 6. *Let G be a finite nonabelian group. The group algebra $\mathbb{C}G$ is wCT if and only if G is either isomorphic to the dihedral group D_4 of order 8, or the quaternion group Q of order 8, or the symmetric group S_3 on three letters.*

Proof. Let G be a finite nonabelian group such that $\mathbb{C}G$ is a wCT ring. By the Wedderburn theorem, $\mathbb{C}G$ is a direct sum of matrix algebras over $\mathbb{C}$. Using Proposition 3 and Proposition 5, we conclude that $\mathbb{C}G \cong \mathbb{C}^r \oplus M_2(\mathbb{C})$ for some $r \geqslant 0$. In other words, G admits r linear irreducible characters and precisely one irreducible character of degree two. It is well known that $r = |G : G'|$, and thus r divides $|G| = r + 4$. The only such possibilities are $r \in \{1, 2, 4\}$. Since G is nonabelian, $r \neq 1$. If $r = 2$, then $G \cong S_3$, and if $r = 4$, then either $G \cong Q$ or $G \cong D_4$.

For the converse note that both $\mathbb{C}D_4$ and $\mathbb{C}Q$ are isomorphic to $\mathbb{C}^4 \oplus M_2(\mathbb{C})$, whereas $\mathbb{C}S_3 \cong \mathbb{C}^2 \oplus M_2(\mathbb{C})$. These are wCT rings by Proposition 3 and Proposition 5. ∎

Another consequence of Proposition 5 is the following.

Corollary 7. *Let R be a noncommutative finite wCT ring. Then R is the direct sum of an indecomposable noncommutative wCT ring of prime power order, and a commutative ring.*

Proof. Let

$$R_p = \{x \in R \mid p^n x = 0 \text{ for some integer } n \geqslant 1\}.$$

Since R as a finite abelian group decomposes into the sum of its p-subgroups, R_p is nonempty for every prime p that divides $|R|$ and of course R_p is a subring of prime power order. But for $p \neq q$ we have $R_pR_q = 0$: if $x \in R_p$, say $p^n x = 0$, and $y \in R_q$, say $q^m y = 0$, there exist integers a and b such that $ap^n + bq^m = 1$ and therefore $xy = 0$. Thus, R is a direct sum of its prime power order subrings R_p.

Now Proposition 5 concludes the proof. ∎

We now turn to indecomposable finite wCT rings. We shall prove that these are either simple, local, or basic with two maximal ideals (see Theorem 10). A crucial step in the proof is to show that the wCT property is closed under taking quotients by the Jacobson radical.

Theorem 8. *Let R be a finite wCT ring with identity and $J = J(R)$ its Jacobson radical. Then R/J is also wCT.*

Proof. We may assume that R is directly indecomposable, since $J(R_1 \oplus R_2) = J(R_1) \oplus J(R_2)$. Because R/J is semisimple it can be written as a direct sum of fields or complete matrix algebras over fields by Wedderburn's theorem.

To prove that R/J is wCT, by Proposition 3 it suffices to check that no matrix algebra of dimension greater or equal to 3 can appear as a direct summand and that at most one of the direct summands is equal to a 2×2 matrix algebra. Assume the contrary and let $\overline{e_1}, \overline{e_2}, \overline{e_3}$ be orthogonal idempotents in R/J such that $\overline{e_1} + \overline{e_2} + \overline{e_3} = \overline{1}$. By [8, Theorem VII.11], we can lift these idempotents to orthogonal idempotents e_1, e_2, e_3 in R such that $e_1 + e_2 + e_3 = 1$. Obviously, all these idempotents are noncentral. But $[e_1, e_2] = [e_1, e_3] = 0$ and for every $x \in R$ we have $[e_1, e_2xe_3] =$

$[e_1, e_3xe_2] = 0$, therefore wCT implies that $[e_2, e_2xe_3] = e_2xe_3 = 0$ and $[e_3, e_3xe_2] = e_3xe_2 = 0$. Similarly, we prove that $e_iRe_j = 0$ for every $i \neq j$, thus yielding a decomposition $R = e_1Re_1 \oplus e_2Re_2 \oplus e_3Re_3$, which contradicts the indecomposability of R. ∎

Example 9. The converse of the above theorem does not hold. Let $1 \leqslant k < r$ and consider the ring

$$R = \left\{ \begin{bmatrix} a & b & c & d \\ 0 & a^{p^k} & b^{p^k} & c^{p^k} \\ 0 & 0 & a^{p^{2k}} & b^{p^{2k}} \\ 0 & 0 & 0 & a^{p^{3k}} \end{bmatrix} \mid a, b, c, d \in \mathrm{GF}(p^r) \right\}.$$

Observe that there exist $b, c, d \in \mathrm{GF}(p^r)$ such that

$$B = \begin{bmatrix} 0 & b & 0 & 0 \\ 0 & 0 & b^{p^k} & 0 \\ 0 & 0 & 0 & b^{p^{2k}} \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 0 & 0 & c & 0 \\ 0 & 0 & 0 & c^{p^k} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad D = \begin{bmatrix} 0 & 0 & 0 & d \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

are noncentral elements and $[B, D] = [D, C] = 0$ but $[B, C] \neq 0$.

The factor ring R/J however, is even commutative (it is isomorphic to the field $\mathrm{GF}(p^r)$).

Theorem 10. *Let R be an indecomposable finite wCT ring with identity. Then either $R = M_2(F)$ for a field F, or R/J is commutative (and therefore R/J is either a field or a direct sum of two fields).*

Proof. Since R/J is semisimple, Corollary 4 and the proof of Theorem 8 yield only three possible cases: R/J is either a field, a direct sum of two fields or a two by two matrix algebra over a field. So, assume now that $R/J = M_2(F)$. By [8, Theorem VIII.26], we know that then $R = M_2(S)$ for some local finite ring S. Assume that S is not a field. Since S is finite, it contains zero divisors, which is a contradiction with Proposition 3. Therefore, R is indeed a two by two matrix algebra over a field. ∎

2.3. **Local wCT rings.** Corollary 7 essentially reduces the study of wCT rings to the study of the indecomposable wCT rings, which in turn are either full matrix algebras, local or basic rings by Theorem 10. The focus of this subsection are local wCT rings. Remember that a ring is said to be local if it has a unique maximal ideal.

Proposition 11. *Let R be a local ring. Then R is a wCT ring if and only if R^{-1} is a wCT group.*

Proof. This is essentially a consequence of $1 + J \subseteq R^{-1}$. First observe that $Z(R) \cap R^{-1} = Z(R^{-1})$. Clearly, we have $Z(R) \cap R^{-1} \subseteq Z(R^{-1})$. For the converse inclusion, given $x \in Z(R^{-1})$ and $y \in R$ we have two cases. If $y \in R^{-1}$, then x and y commute by assumption. If $y \notin R^{-1}$, then $y \in J$ and thus $1 + y \in 1 + J \subseteq R^{-1}$. Hence $0 = [x, 1 + y] = [x, y]$, as desired.

This observation immediately implies the implication ($\Rightarrow$) of the lemma: for $x, y, z \in R^{-1} \setminus Z(R^{-1})$, we have $x, y, z \in R \setminus Z(R)$. Thus $[x, y] = 0 = [y, z]$ implies $[x, z] = 0$ by the wCT property of R. To prove ($\Leftarrow$), choose $x, y, z \in R \setminus Z(R)$ with $[x, y] = 0 = [y, z]$. If one of these elements is not in R^{-1}, say $x \notin R^{-1}$, then

we may replace it with $1 + x$ without changing any of the commutator relations. However $1 + x \in 1 + J \subseteq R^{-1}$. Thus the wCT property of R^{-1} yields the desired conclusion. ∎

In general there is no relationship between the wCT property of (the ring) R and its group of units R^{-1}.

Example 12. Let R be the ring of all upper triangular 2×2 matrices over $\mathbb{Z}_4$. Then $R/J \cong \mathrm{GF}(2) \oplus \mathrm{GF}(2)$. It is straightforward to verify that the group R^{-1} is wCT. On the other hand, the ring R is not wCT. To this end, consider the matrices

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}, \quad \text{and} \quad C = \begin{bmatrix} 0 & 2 \\ 0 & 1 \end{bmatrix}.$$

Then $B \notin Z(R)$, $AB = BA$ and $BC = CB$, but $AC \neq CA$.

To study the properties of local wCT rings, we recall the notion of a Galois ring. The ring $R = \mathrm{GR}(p^t, r)$ is said to be a *Galois ring* if it is isomorphic to the ring $\mathbb{Z}[x]/(p^t, f(x))$, where f is a monic polynomial of degree r, which is irreducible modulo $p\mathbb{Z}$. Note that the Galois ring does not depend on the choice of f by [8, Theorem XV.7 and XV.11].

The structure of finite local rings will be described using generalized skew polynomial rings, a notion which we now define. R is a *generalized skew polynomial ring* if it is defined by a subring A and a finite set of not necessarily commuting elements x_i, where there are automorphisms σ_i of A such that $x_i a = \sigma_i(a) x_i$ for all $a \in A$. We then write $R = A\{x_1, \ldots, x_n; \sigma_1, \ldots, \sigma_n\}$. For details see [8, Chapter XIX].

Theorem 13. *Let R be a finite local ring with identity, $R/J = k = \mathrm{GF}(p^r)$, $n = \dim_k(J/J^2)$ and $\mathrm{char}(R) = p^t$. Then $R = A\{x_1, x_2, \ldots, x_n; \sigma_1, \sigma_2, \ldots, \sigma_n\}$, where $A = \mathbb{Z}_{p^t}[y]$, the element $y \in R$ is an invertible element of order $p^r - 1$, the set $\{x_1, x_2, \ldots, x_n\}$ is a k-basis of J/J^2, and for every i, $\sigma_i(f(y)) = f(y^{p^{\ell_i}})$ is an automorphism of the Galois ring A.*

Proof. Choose $y_1 \in R$ such that $y_1 + J$ is a generator of the group $k \setminus \{0\}$. The order of y_1 is equal to $(p^r - 1)p^s$ for some integer s, since the order of R^{-1} is equal to $(p^r - 1)p^m$ for some integer m. Now, take $y = y_1^{p^s}$ and observe that $y + J$ is also a generator of the group $k \setminus \{0\}$. Let A be the subring of R generated by y. If $\sum_{i=0}^{t-1} p^i a_i = \sum_{i=0}^{t-1} p^i b_i$ for some elements $a_i, b_i \in \{0, y, y^2, \ldots, y^{p^r-1}\}$, we can show by induction (and by multiplying the equation by p^{t-i-1}) that $a_i = b_i$ for every i. Since the order of $y + J$ in $k \setminus \{0\}$ is r, we can therefore uniquely express every element of A as a sum $\sum_{i=0}^{r-1} n_i y^i$ for some $n_i \in \{0, 1, \ldots, p^t - 1\}$. Now let N be an A-module generated by $\{x_1, x_2, \ldots, x_n\}$. Note that $N \subseteq J$. Since $R/J(R) = A/J(A)$, we obtain the decomposition of R as an A-module, $R = A \oplus N$. The lemma now follows from the proof of [8, Theorem XIX.6] and the fact that A is a Galois ring, so every automorphism of A is a power of the automorphism that maps y into y^p. ∎

Remark 14. Note that the element y defined in Theorem 13 has the following useful property: if $y^\alpha - y^\beta \in J$, then $y^\alpha = y^\beta$. We can easily check this by considering the equation modulo the radical and keeping in mind that the image of y is the generator of $k \setminus \{0\}$.

A is called the *coefficient ring* [8, Theorem XVII.1] of R and is the local subring of R containing $\mathbb{Z}_{\mathrm{char}(R)}$, and being maximal with respect to the property $J(A) = pA$. By [8, Theorem XIX.4], a coefficient ring of a local ring R is unique up to an inner automorphism of R.

Lemma 15. *Let R_1 and R_2 be finite local rings with identity, $R_i/J_i = k = \mathrm{GF}(p^r)$, $\mathrm{char}(R_i) = p^t$ for $i = 1, 2$, and $A = \mathbb{Z}_{p^t}[y]$ a Galois ring. Suppose that $\dim_k(J_i/J_i^2) = 1$ for $i = 1, 2$. Then $R_1 = A\{x_1; \sigma\}$ is isomorphic to $R_2 = A\{x_2; \tau\}$ if and only if $\sigma = \tau$.*

Proof. If $\sigma = \tau$, the assertion is trivial, since both x_1 and x_2 are of the same order of nilpotency. Conversely, assume that f is an isomorphism from R_1 to R_2 and $f(x_1) = x_2$. The equation $yx_1 = x_1\sigma(y)$ in R_1, translates into $f(y)x_2 = x_2 f(\sigma(y))$ in R_2. Let $\sigma(y) = y^{p^{r_1}}$ and $\tau(y) = y^{p^{r_2}}$. Then $f(y)x_2 = x_2 f(y)^{p^{r_1}}$. Since f is identity on $\mathbb{Z}_{p^t}$ and its induced mapping on k is an isomorphism, we have $f(y) = y^{p^\alpha}$ for some integer α. Thus $y^{p^\alpha}x_2 = x_2 y^{p^{\alpha+r_1}}$. We also know that $yx_2 = x_2\tau(y)$, therefore $x_2 y^{p^{\alpha+r_1}} = x_2 y^{p^{\alpha+r_2}}$ and thus $y^{p^{\alpha+r_1}} - y^{p^{\alpha+r_1}} \in J$. This implies $\alpha + r_1 = \alpha + r_2 + \lambda r$ for some integer λ, by Remark 14. Hence $r_1 = r_2 + tr$, so $\sigma = \tau$. ∎

Proposition 16. *Let R be a finite local ring with identity, $R/J = k = \mathrm{GF}(p^r)$, $\mathrm{char}(R) = p^t$, $n = \dim_k(J/J^2)$ and $A = \mathbb{Z}_{p^t}[y]$ a Galois ring. Then there exists a k-basis $\{x_1, x_2, \ldots, x_n\}$ of J/J^2 such that $R = A\{x_1, x_2, \ldots, x_n; \sigma_1, \sigma_2, \ldots, \sigma_n\}$ for some automorphisms $\sigma_1, \sigma_2, \ldots, \sigma_n$ of A. Moreover, if $\tau_1, \tau_2, \ldots, \tau_n$ are automorphisms of A, and the non-ordered n-tuples $(\sigma_1, \sigma_2, \ldots, \sigma_n)$ and $(\tau_1, \tau_2, \ldots, \tau_n)$ are not equal, then R is not isomorphic to the ring $A\{x_1, x_2, \ldots, x_n; \tau_1, \tau_2, \ldots, \tau_n\}$.*

Proof. We already have the existence of x_i and σ_i by Theorem 13. Let f be an isomorphism from R to $A\{x_1, x_2, \ldots, x_n; \tau_1, \tau_2, \ldots, \tau_n\}$. Since f maps a k-basis of J/J^2 into a k-basis of J/J^2, we have $f(x_i) = \sum_k \lambda_{ik} x_k$ for all i. As in the proof of Lemma 15, we have $f(y) = y^{p^\alpha}$ for some integer α. Let also $\sigma_i(y) = y^{p^{r_i}}$ and $\tau_i(y) = y^{p^{s_i}}$ for every i. So, $yx_i = x_i\sigma_i(y)$ implies $y^{p^\alpha}(\sum_k \lambda_{ik}x_k) = (\sum_k \lambda_{ik}x_k)y^{p^{\alpha+r_i}}$, thus $\sum_k(\lambda_{ik}x_k y^{p^{\alpha+s_k}}) = \sum_k(\lambda_{ik}x_k y^{p^{\alpha+r_i}})$. However, the set $\{x_1, x_2, \ldots, x_n\}$ is linearly independent over k, therefore $y^{p^{\alpha+s_k}} = y^{p^{\alpha+r_i}}$ by Remark 14. So, whenever $\lambda_{ik} \neq 0$, we have $\tau_k = \sigma_i$. Since there is at least one nonzero λ_{ik} for every i, we conclude that the non-ordered n-tuples $(\sigma_1, \sigma_2, \ldots, \sigma_n)$ and $(\tau_1, \tau_2, \ldots, \tau_n)$ have to be equal. ∎

Definition 17. Let $R = A\{x_1, x_2, \ldots, x_n; \tau_1, \tau_2, \ldots, \tau_n\}$ be a finite local ring with identity, as above. As A is a Galois ring, each τ_i is a power map $y \mapsto y^{p^{r_i}}$. Without loss of generality, $r_1 \geqslant \cdots \geqslant r_n$. Then the n-tuple $(\tau_1, \ldots, \tau_n)$ is called the *signature* of the local ring R. By Proposition 16, the signature of a local ring is well defined and is thus an invariant of the local ring.

Theorem 18. *Let $R = A\{x_1, x_2, \ldots, x_n; \sigma_1, \sigma_2, \ldots, \sigma_n\}$, where A is a Galois ring, and suppose that $x_1, x_2, \ldots, x_n \in J$ commute. Then R is wCT if and only if the sets of fixed points of all nontrivial automorphisms $\prod_i \sigma_i^{k_i}$ with $\prod_i x_i^{k_i} \neq 0$ coincide.*

Proof. Assume that R is wCT and let $\sigma = \prod_i \sigma_i^{k_i}$ and $\tau = \prod_i \sigma_i^{\ell_i}$ be nontrivial for some $x = \prod_i x_i^{k_i} \neq 0$, $y = \prod_i x_i^{\ell_i} \neq 0$. If $x(\sigma(a)) = xa$ for every $a \in A$, then $\sigma(a) - a \in J$ for every $a \in A$. If we choose $a = y$, Remark 14 implies that $\sigma(y) = y$, whence $\sigma(a) = a$ for all $a \in A$. So $x \notin Z(R)$ and similarly, $y \notin Z(R)$. If $\sigma(a) = a$, then $[a, x] = 0$, and since $[x, y] = 0$, we have $[a, y] = 0$, thus $\tau(a) = a$. The converse is obvious. ∎

Corollary 19. *Let $R = A\{x_1, x_2, \ldots, x_n; \sigma_1, \sigma_2, \ldots, \sigma_n\}$ be a finite local ring with identity, where A is a Galois ring and $R/J = k = \mathrm{GF}(p^r)$. Assume that $J^2 = 0$. Then R is wCT if and only if the sets of fixed points of all automorphisms σ_i with $x_i \notin Z(R)$ coincide.*

Proof. Since all products of x_i and x_j are zero, we know by Theorem 18 that R is wCT if and only if the sets of fixed points of all nontrivial automorphisms σ_i coincide. The converse is obvious. ∎

Theorem 20. *Let $R = A\{x; \sigma\}$ be a finite local ring with identity, where A is a Galois ring, $x \in J$ and $R/J = k = \mathrm{GF}(p^r)$. Let m denote the nilpotency index of J and $\sigma(y) = y^{p^\ell}$. Then R is wCT if and only if $1, 2, \ldots, m-1$ are all either relatively prime to, or divisible with $r/\gcd(r, \ell)$.*

Proof. By Theorem 13, we have $R = A\{x; \sigma\}$ for $A = \mathbb{Z}_{p^t}[y]$ and $\sigma(y) = y^{p^\ell}$. Assume R is wCT. By Theorem 18, the sets of fixed points of all nontrivial automorphisms belonging to $\{\sigma, \sigma^2, \ldots, \sigma^{m-1}\}$ coincide. Since all automorphisms fix all scalars from A, we consider them modulo $J(A)$. Let F denote the algebraic closure of $\mathbb{Z}_p$. The set of fixed points of the automorphism $\sigma^j : F \to F$ is a subfield of F isomorphic to $\mathrm{GF}(p^{\ell j})$. Hence the set of fixed points of $\sigma^j : k \to k$ is the meet of $\mathrm{GF}(p^{\ell j})$ and $k = \mathrm{GF}(p^r)$ in the lattice of all field extensions of $\mathbb{Z}_p$, therefore it equals $\mathrm{GF}(p^{\gcd(j\ell, r)})$. Thus for every $j \leqslant m-1$, either $\gcd(j\ell, r) = \gcd(\ell, r)$, if the automorphism is nontrivial, or $\gcd(j\ell, r) = r$, if the automorphism is trivial. The converse is straightforward, since all nontrivial automorphisms have the same set of fixed points. ∎

Corollary 21. *Let $R = A\{x_1, x_2, \ldots, x_n; \sigma_1, \sigma_2, \ldots, \sigma_n\}$ be a finite local ring with identity, where A is a Galois ring, and $R/J = k = \mathrm{GF}(p^r)$. If J is commutative and r is a prime number, then R is wCT.*

Proof. By Theorem 18, R is wCT if and only if the sets of fixed points of all nontrivial automorphisms σ_i coincide. Let $\sigma = \prod_{i=1}^n \sigma_i^{k_i}$ and $\sigma_i(y) = y^{p^{r_i}}$. Since r is prime, we either have $\gcd(\sum_{i=1}^n k_i r_i, r) = r$ when σ is the identity, or $\gcd(\sum_{i=1}^n k_i r_i, r) = 1$. As in the proof of Theorem 20, all nontrivial automorphisms of A have the same set of fixed points. ∎

Proposition 22. *Let $R = A\{x_1, x_2, \ldots, x_n; \mathrm{id}, \mathrm{id}, \ldots, \mathrm{id}\}$ be a finite local ring with identity for a Galois ring A, where all $x_i \in J$. Then R is wCT if and only if the group $1 + J$ is wCT.*

Proof. Since A is central, R is wCT if and only if J is wCT. ∎

Example 23. Let $R = A\{x_1, x_2, \ldots, x_n; \sigma_1, \sigma_2, \ldots, \sigma_n\}$, where A is a Galois ring and $R/J = \mathrm{GF}(p^r)$. Assume there exists an integer k such that $\prod_{i=1}^k x_{\ell_i} = 0$ where $\ell_i \in \{1, 2, \ldots, n\}$ for all i. Consider two cases:

(1) There exists a noncentral element $x = \prod_{i=1}^{k-1} x_{\ell_i}$. Then $[x_i, x] = 0$ for all i, and if R is wCT, also $[x_i, x_j] = 0$ for all $i \neq j$.
(2) All elements $\prod_{i=1}^{k-1} x_{\ell_i}$ where $\ell_i \in \{1, 2, \ldots, n\}$ for all i, are central and nonzero. Let y denote the generator of the Galois ring A and let $\sigma_i(y) = y^{p^{r_i}}$. Suppose at least one automorphism is nontrivial, i.e., suppose without loss of generality that r_1 is not divisible by r. Then all automorphisms $\prod_{i=1}^n \sigma_i^{\alpha_i}$ with $\sum_{i=1}^n \alpha_i = k - 1$ coincide. Thus, $\sum_{i=1}^n \alpha_i = k - 1$ implies that $\sum_{i=1}^n \alpha_i r_i$ is

divisible by r. As in the proof of Theorem 20, if such a ring is wCT then either $\gcd(\sum_{i=1}^n \alpha_i r_i, r) = \gcd(r_1, r)$, or $\sum_{i=1}^n \alpha_i r_i$ is divisible by r for every tuple $(\alpha_1, \ldots, \alpha_n)$ with $\sum_{i=1}^n \alpha_i < k-1$. We list some of the numbers of such tuples $(r_1, \ldots, r_n)$ in the following table:

n	3	4	4	6	5	6	7
r	6	6	10	6	10	9	8
k	3	3	3	4	3	3	3
$s = \#$ of tuples $(r_1, \ldots, r_n)$	6	36	100	216	1000	6561	32768

(This data is consistent with $s = r^{n-k+1}$ and we conjecture this is true in general.) To each of these triples (n, r, k) at least one wCT ring is associated. Note that by Proposition 16, all such rings are non-isomorphic. The number of these tuples is growing rapidly, so there is little hope of finding a nice classification of wCT rings of this type in general.

2.4. **wCT basic rings.** By [8, Theorem XIX.1], a basic ring R has a similar presentation of the form $R = A\{x_1, \ldots, x_n; \sigma_1, \sigma_2, \ldots, \sigma_n\}$ for some integer n and a (local and Galois) coefficient ring A as in Theorem 13. However, not all of the elements x_i are in J.

The following theorem is an extension of Theorem 18 to the basic case. Its proof is an adaptation of the corresponding result for local rings.

Theorem 24. *Let $R = A\{x_1, x_2, \ldots, x_n; \sigma_1, \sigma_2, \ldots, \sigma_n\}$ for a Galois ring A, and suppose that $x_1, x_2, \ldots, x_n$ commute. Then R is wCT if and only if the sets of fixed points of all nontrivial automorphisms $\prod_i \sigma_i^{k_i}$ with $\prod_i x_i^{k_i} \neq 0$ coincide.*

Proof. Assume that R is wCT and let $\sigma = \prod_i \sigma_i^{k_i}$ and $\tau = \prod_i \sigma_i^{\ell_i}$ be nontrivial for some $x = \prod_i x_i^{k_i} \neq 0$, $y = \prod_i x_i^{\ell_i} \neq 0$. If $\sigma(y) - y$ is an invertible element of the field $A/J(A)$, then $\sigma(y) - y$ is also invertible in A. Hence $\sigma(y) = y$, and this implies $\sigma(a) = a$ for all $a \in A$. Therefore, $x \notin Z(R)$ and likewise, $y \notin Z(R)$. If $\sigma(a) = a$, then $[a, x] = 0$, and since $[x, y] = 0$, we have $[a, y] = 0$, thus $\tau(a) = a$. The converse is obvious. ∎

In Theorems 18, 20 and Corollary 21 we have classified local wCT rings $R = A\{x_1, x_2, \ldots, x_n; \sigma_1, \sigma_2, \ldots, \sigma_n\}$ with commuting variables $x_i \in J$. We now pass to the case of basic rings, where not all of the x_i are in J. If R is a basic ring, and all the $x_i \notin J$ are central, then the basic case essentially reduces to the local case. We thus assume that $x_1 \notin Z(R) \cup J$. In this case we have a characterization of the wCT property as follows:

Corollary 25. *Let $R = A\{x_1, x_2, \ldots, x_n; \sigma_1, \sigma_2, \ldots, \sigma_n\}$ be a basic ring for a Galois ring $A = \mathrm{GR}(p^t, r)$. Suppose that $x_1, x_2, \ldots, x_n$ commute, and that $x_1 \notin Z(R) \cup J$. If r is prime, then R is wCT. Conversely, if R is wCT, then $r/\gcd(r, \ell)$ is prime, where $\sigma_1(y) = y^{p^\ell}$ for a generator y of A.*

Proof. Following the lines of the proof of Corollary 21, we can show that R is wCT if r is prime. Conversely, if R is wCT, then R/J is a direct sum of two fields by Theorem 10. Hence $x_1 \notin J$ implies x_1 is not nilpotent. By Theorem 24, the nontrivial automorphisms σ_1^α have the same set of fixed points for every such integer α. As in the proof of Theorem 20, either $\gcd(\alpha\ell, r) = \gcd(\ell, r)$, or $\gcd(\alpha\ell, r) = r$ for all integers α as above. Hence these α have to be multiples of $r/\gcd(r, \ell)$. ∎

References

[1] Abdollahi, A., Akbari, S., and Maimani, H.R.: Non-commuting graph of a group, J. Algebra **298**, 468–492 (2006)

[2] Bell, H.E., Klein, A.A.: Extremely noncommutative elements in rings, Monatsh. Math. **153**, 19–24 (2008)

[3] Bell, J.P., Small, L.W.: Centralizers in domains of Gelfand-Kirillov dimension 2, Bull. London Math. Soc. **36**, 779–785 (2004)

[4] Bergman, G.M.: Centralizers in free associative algebras, Trans. Amer. Math. Soc. **137**, 327–344 (1969)

[5] Cohn, P.M.: Free rings and their relations (Second edition), London Math. Soc. Monographs **19**, London (1985)

[6] Feit, W., Thompson, J.G.: Solvability of groups of odd order, Pacific J. Math. **13**, 775–1029 (1963)

[7] Klep, I., Moravec, P.: Lie algebras with abelian centralizers, Algebra Colloq., to appear

[8] McDonald, B.R.: Finite rings with identity, Marcel Dekker, New York (1974)

[9] Raghavendran, R.: Finite associative rings, Compositio Math. **21**, 195–229 (1969)

[10] Rocke, D.M.: p-groups with abelian centralizers, Proc. London Math. Soc. (3) **30**, 55–75 (1975)

[11] Schmidt, R.: Zentralisatorverbände endlicher Gruppen, Rend. Sem. Mat. Univ. Padova **44**, 97–131 (1970)

[12] Suzuki, M.: The nonexistence of a certain type of simple groups of odd order, Proc. Amer. Math. Soc. **8**, 686–695 (1957)

[13] Weisner, L.: Groups in which the normaliser of every element except identity is abelian, Bull. Amer. Math. Soc. **31**, 413–416 (1925)

[14] Wilson, R.S.:, On the structure of finite rings, Compositio Math. **26**, 79–93 (1973)

[15] Wu, Y.-F.: Groups in which commutativity is a transitive relation, J. Algebra **207**, 165–181 (1998)

David Dolžan, Univerza v Ljubljani, Fakulteta za matematiko in fiziko, Jadranska 19, SI–1111 Ljubljana, Slovenia

E-mail address: david.dolzan@fmf.uni-lj.si

Igor Klep, Univerza v Mariboru, Fakulteta za naravoslovje in matematiko, Koroška 160, SI–2000 Maribor, and Univerza v Ljubljani, Fakulteta za matematiko in fiziko, Jadranska 19, SI–1111 Ljubljana, Slovenia

E-mail address: igor.klep@fmf.uni-lj.si

Primož Moravec, Univerza v Ljubljani, Fakulteta za matematiko in fiziko, Jadranska 19, SI–1111 Ljubljana, Slovenia

E-mail address: primoz.moravec@fmf.uni-lj.si