PDMI PREPRINT — 8/2001

Characterization of cyclotomic schemes on a finite field and normal Schur rings over a cyclic group

Sergei Evdokimov
St. Petersburg Institute
for Informatics and Automation RAS
evdokim@pdmi.ras.ru *

Ilia Ponomarenko
Steklov Institute of Mathematics
at St. Petersburg
inp@pdmi.ras.ru †

13.09.2001

Abstract

It is well known that in general a cyclotomic scheme $\mathcal{C}$ on a finite field $\mathbb{F}$ cannot be characterized up to isomorphism by its intersection numbers. We show that the set of intersection numbers of some scheme $\widehat{\mathcal{C}}^{(b)}$ on the b-fold Cartesian product of $\mathbb{F}$ where b is the base number of the group $\mathrm{Aut}(\mathcal{C})$ forms a full set of invariants of $\mathcal{C}$. A key point here is that the scheme $\widehat{\mathcal{C}}^{(b)}$ can be defined for an arbitrary scheme $\mathcal{C}$ in a purely combinatorial way. The proof is based on the complete description of normal Cayley and Schur rings (introduced in this paper) over a finite cyclic group. The developed technique enables us to show that a Schur ring over a cyclic group that is different from the group ring has a nontrivial automorphism.

*Partially supported by RFFI, grants 96-15-96060, 99-01-00098, 01-01-00219
†Partially supported by RFFI, grants 96-15-96060, 99-01-00098, 01-01-00219

1 Introduction

In the end of the 1960's in studying permutation representations of classical groups D. G. Higman [9] came to the following notion playing a key role in the present paper. Let V be a finite set and $\mathcal{R}$ a set of binary relations on V. A pair $\mathcal{C} = (V, \mathcal{R})$ is called a *coherent configuration* or a *scheme* on V if the following conditions are satisfied:

(C1) $\mathcal{R}$ forms a partition of the set V^2,

(C2) the diagonal of V^2 is a union of elements of $\mathcal{R}$,

(C3) if $R \in \mathcal{R}$, then $R^T \in \mathcal{R}$,

(C4) if $R, S, T \in \mathcal{R}$, then the number $|\{v \in V :\ (u,v) \in R,\ (v,w) \in S\}|$ does not depend on the choice of $(u,w) \in T$.

The elements of V, the relation of $\mathcal{R}$ and the numbers from (C4) are called the *points*, the *basis relations* and the *intersection numbers* of $\mathcal{C}$, respectively. Obviously, the latters are invariants of the scheme $\mathcal{C}$ with respect to isomorphism of schemes, i.e. a bijection of the point sets respecting the basis relations.

The main source of schemes are finite groups. Namely, any permutation group $\Gamma \leq \mathrm{Sym}(V)$ defines a scheme $\mathrm{Con}(\Gamma) = (V, \mathcal{R})$ where $\mathcal{R}$ is the set of all orbits of Γ on $V \times V$. This enables us to consider Γ as a group of automorphisms of $\mathcal{C} = \mathrm{Con}(\Gamma)$, i.e. as a subgroup of the group

$$\mathrm{Aut}(\mathcal{C}) = \{g \in \mathrm{Sym}(V) :\ R^g = R,\ R \in \mathcal{R}\}$$

called the *automorphism group* of $\mathcal{C}$. Extending this definition to an arbitrary scheme $\mathcal{C}$ we come to the mappings $\Gamma \mapsto \mathrm{Con}(\Gamma)$ and $\mathcal{C} \mapsto \mathrm{Aut}(\mathcal{C})$ between the schemes and the permutation groups on V. These mappings are not inverse to each other but define a Galois correspondence with respect to the natural partial orders on these sets. A scheme $\mathcal{C}$ is called *Schurian* if it is a closed object under this correspondence (the name "Schurian" is explained by the fact that I. Schur was probably the first who explicitly used the centralizer ring of a permutation group which is none other than the adjacency ring of its scheme). It should be noted that Schurian schemes are rather rare. For example, the scheme associated in a natural way to a finite projective plane is Schurian iff the plane is Desarguesian (see [6]).

In this paper we study cyclotomic schemes introduced by P. Delsarte and defined as follows. Let $\mathbb{F}$ be a finite field with q elements and H a subgroup of the group $\mathbb{F}^\times$ of index m. For $a \in \mathbb{F}$ set

$$R_a = \{(x,y) \in \mathbb{F}^2 :\ x - y \in aH\}.$$

Then the pair $(\mathbb{F}, \{R_a :\ a \in \mathbb{F}\})$ is a scheme on $\mathbb{F}$ called a *cyclotomic* one (see [1]). One can see that the intersection number of this scheme corresponding to the relations R_a, R_b, R_c with $a, b, c \neq 0$ equals the number of solutions $\xi, \eta \in \{0, 1, \ldots, (q-1)/m - 1\}$ of the equation $ag^{m\xi} + b = cg^{m\eta}$ where g is a primitive element of $\mathbb{F}$. The explicite evaluation of these integers called the cyclotomic numbers is a hard number-theoretic problem (see [12, p.305]). Moreover, in contrast to many classical schemes the intersection numbers of a cyclotomic scheme do not determine it up to isomorphism. For example, there is a great variety of pairwise non-isomorphic schemes coming from the conference matrices as well as the Hadamard matrices and having the same intersection numbers as the Payley schemes, i.e. cyclotomic schemes with $m = 2$. The aim of this paper is to find a full set of invariants of a cyclotomic scheme by enlarging the set of its intersection numbers. To do this we use the approach developed by the authors in a series of papers [3]-[6] and outlined below (as for exact definitions see Sections 2 and 3).

The natural one-to-one correspondence between the binary relations on a set V and the {0,1}-matrices of the full matrix ring $\mathrm{Mat}_V = \mathrm{Mat}_V(\mathbb{Z})$ induces a one-to-one correspondence between the schemes on V and the cellular rings [1] on V which are by definition subrings of Mat_V closed under the Hadamard (componentwise) multiplication and the transposition and containing the identity matrix and the all-one matrix. In particular, for a permutation group Γ the scheme $\mathrm{Con}(\Gamma)$ goes to the centralizer ring $\mathcal{Z}(\Gamma)$ of Γ. Let $\mathcal{C}$ be a scheme on V and W the corresponding cellular ring (the adjacency ring of $\mathcal{C}$). For a positive integer m we define a scheme $\widehat{\mathcal{C}}^{(m)}$ as the scheme corresponding to the smallest cellular ring $\widehat{W}^{(m)}$ on the set V^m containing the m-fold tensor product W^m and the adjacency matrix of the reflexive relation corresponding to the diagonal of V^m. We are interested in the minimal m such that the set of intersection numbers of the scheme $\widehat{\mathcal{C}}^{(m)}$ determines $\mathcal{C}$ up to isomorphism. We call this number the *separability number* of $\mathcal{C}$, denote it by $s(\mathcal{C})$ and set $s(W) = s(\mathcal{C})$. Thus $s(\mathcal{C}) \le m$ iff $\mathcal{C}$ is characterized by the intersection numbers of $\widehat{\mathcal{C}}^{(m)}$, or in other words, the set of intersection numbers of $\widehat{\mathcal{C}}^{(m)}$ is a full set of invariants of $\mathcal{C}$. The separability number was introduced and studied in [6]; therein this number was evaluated for several families of classical schemes.

The above discussion shows that there exist cyclotomic schemes $\mathcal{C}$ with $s(\mathcal{C}) \ge 2$. On the other hand, from [6, Theorem 5.1] it follows that $s(\mathcal{C}) \le 2$ for any imprimitive cyclotomic scheme. Finally, if $\mathcal{C}$ is a primitive cyclotomic scheme on a prime number of points, then $s(\mathcal{C}) \le 4$ (see [6, Theorem 5.4]). In the present paper we estimate the separability number of an arbitrary cyclotomic scheme by the base number of its automorphism group. (By the base number $b(\Gamma)$ of a permutation group Γ we mean the minimum number of points leaved fixed only by the identity permutation of Γ.) From [13] it follows that if $\mathcal{C}$ is a proper cyclotomic scheme (i.e. $H \ne \mathbb{F}^\times$), then

$$\mathrm{Aut}(\mathcal{C}) \le \{x \mapsto ax^\sigma + b,\ x \in \mathbb{F} :\ a \in H,\ \sigma \in \mathrm{Aut}(\mathbb{F}),\ b \in \mathbb{F}\}. \tag{1}$$

In particular, the base number of $\mathrm{Aut}(\mathcal{C})$ is at most 3. The following theorem is the main result of the paper.

Theorem 1.1 *Let $\mathcal{C}$ be a proper [2] cyclotomic scheme on a finite field. Then $s(\mathcal{C}) \le b(\mathrm{Aut}(\mathcal{C}))$.*

The proof of Theorem 1.1 is postponed to the end of this section. As it follows from the theorem, $s(\mathcal{C}) \le 3$ for all cyclotomic scemes $\mathcal{C}$. We do not know if this estimate is sharp.

[1] In [17, 18] and [2]-[7] the theory of cellular algebras over $\mathbb{C}$ was developed. This theory except for its representation aspects can be completely transferred to the cellular rings

[2] If $\mathcal{C}$ is not proper, then, obviously, $s(\mathcal{C}) = 1$

Let W be the adjacency ring of a proper cyclotomic scheme on a finite field $\mathbb{F}$. Our approach to estimate $s(W)$ consists in studying for $v_1, \ldots, v_l \in \mathbb{F}$ the structure of a ring $W_{v_1,\ldots,v_l}$ which is by definition the smallest cellular ring on $\mathbb{F}$ containing W and the matrix unit corresponding to v_i for all i. (In fact for our purpose the case $l \le 2$ is sufficient.) It turns out that one can associate in a natural way to the ring W_u where $u = 0_{\mathbb{F}}$ a cellular ring W^* on the cyclic group $G = \mathbb{F}^{\times}$ (see (22)) such that $G \le \mathrm{Aut}(W^*) \le G \cdot \mathrm{Aut}(G)$. In our terminology this means that W^* is a *normal Caley ring* over G (see Subsections 4.2 and 4.3). The complete characterization of normal Cayley rings over a cyclic group is given in Theorem 6.1. It is based on the Leung-Man description of the Schur rings over a cyclic group (see [10, 11]) and on a one-to-one correspondence between the Schur rings and the Cayley rings (see Theorem 4.2). This characterization in particular implies that the rings W^* and $(W^*)_v$ where $v = 1_{\mathbb{F}}$ are Schurian. The latter enables us to prove that the cellular rings W_u and $W_{u,v}$ are also Schurian and after taking into account (1) ultimately to estimate the number $s(W)$. A series of results about Schur rings over a cyclic group not connected directly with the main result of the paper is of independent interest. In particular, we completely identify the automorphism groups of normal Schur rings (Theorem 6.1). For each of these rings we also find the groups of its weak and strong isomorphisms (Theorem 6.6). Finally, we mention Theorem 5.7 stating that the only Schur ring over a cyclic group having trivial automorphism group is the group ring.

The structure of the above rings $W_{v_1,\ldots,v_l}$ is revealed in Theorem 1.2 below. This enables us in particular to find the base number $b(W)$ of the cellular ring W, which is by definition the minimal l such that $W_{v_1,\ldots,v_l}$ is the full matrix ring. It turned out that the developed technique made it possible to explicitly describe also the cellular rings $\widehat{W}^{(l)}$ for all l. The results obtained show that it is not necessary to have $\Gamma = \mathrm{Aut}(W)$ in hand to find efficiently the rings $\mathcal{Z}(\Gamma_{v_1,\ldots,v_l})$ and $\mathcal{Z}_l(\Gamma)$ where $\Gamma_{v_1,\ldots,v_l}$ is the pointwise stabilizer of the set $\{v_1, \ldots, v_l\}$ in Γ and $\mathcal{Z}_l(\Gamma) = \mathcal{Z}(\widehat{\Gamma}^{(l)})$ with $\widehat{\Gamma}^{(l)}$ being the permutation group induced by the action of Γ on the l-tuples of points. This seems to be of interest because in general the situation is not so good (see Subsections 2.6 and 3.1). It also explains why Theorem 1.2 is formulated in a more general form than it is necessary for proving the main result.

Theorem 1.2 *Let W be the adjacency ring of a cyclotomic scheme on a finite field $\mathbb{F}$. Then*

(1) $b(W) = b(\mathrm{Aut}(W))$,

(2) $W_{v_1,\ldots,v_{m-1}} = \mathcal{Z}(\mathrm{Aut}(W)_{v_1,\ldots,v_{m-1}})$ *for all $m \ge 1$ and any points $v_1, \ldots, v_{m-1}$ of W,*

(3) $\widehat{W}^{(m)} = \mathcal{Z}_m(\mathrm{Aut}(W))$ *for all $m \ge 1$.*

Proof. Statement (1) immediately follows from statement (2). If the scheme is not a proper one, then the second statement is obvious whereas the third one follows from the equality $\widehat{\mathcal{Z}(\mathrm{Sym}(V))}^{(m)} = \mathcal{Z}_m(\mathrm{Sym}(V))$ (see [5, formula 2]). Suppose without loss of generality that the scheme is proper and $m \ge 2$. The rings W^* and $\widehat{W}^*$as defined in (22) are Schurian by Theorem 8.1. So the rings W_u and $\widehat{W}^{(2)}$ are also Schurian by statement (3) of Theorem 4.8 where $u = 0_{\mathbb{F}}$. This implies for $m = 2$ statement (3) and after taking into account that the group $\mathrm{Aut}(W)$ is transitive also statement (2). Let $m \geq 3$. Then from Corollary 6.2 it follows that the ring $(W^*)_{v_2,\ldots,v_{m-1}}$ and hence by Lemma 9.2 the ring $(W')_{v_2,\ldots,v_{m-1}}$ are 1-regular for any points $v_2, \ldots, v_{m-1}$ of W different from u where W' is the ring defined in (21). So $W_{v_1,v_2,\ldots,v_{m-1}}$ is a 1-regular ring for $v_1 = u$ and the same $v_2, \ldots, v_{m-1}$. This proves both statement (2) (by Theorem 9.3 and the transitivity of $\mathrm{Aut}(W)$) and statement (3) (by Theorem 9.6). ∎

The case $m = 2$ of statement (3) is rather labor-consuming (difficulties arise if $\mathrm{Aut}(W) \cap \mathrm{Aut}(\mathbb{F}) \neq \{1\}$, i.e. $b(\mathrm{Aut}(W)) = 3$). Its proof takes most of Section 8 and involves Schur rings over non-Abelian groups. In this case we associate to the ring $\widehat{W}^{(2)}$ a Cayley ring $\widehat{W}^*$ over the group Γ equal to the semidirect product of the additive group of the finite field $\mathbb{F}$ by its multiplicative group. From Theorem 4.8 it follows that the ring $\widehat{W}^*$ is normal and $\mathrm{Aut}(\widehat{W}^*) \leq \Gamma \cdot \mathrm{Aut}(\mathbb{F})$. Moreover, the Schur ring $\widehat{\mathcal{A}}^*$ over Γ correponding to $\widehat{W}^*$ contains p pairwise isomorphic subrings one of which corresponds to the normal Cayley ring W^* over $\mathbb{F}^\times$ (see above) where $p = \mathrm{char}(\mathbb{F})$. Using these facts, Theorem 6.1 and the properties of finite fields we prove that $\widehat{\mathcal{A}}^*$ is an orbit Schur ring (Theorem 8.2) and consequently that the cellular rings $\widehat{W}^*$ and $\widehat{W}^{(2)}$ are Schurian.

Proof of Theorem 1.1. [3] Let W be the adjacency ring of the scheme $\mathcal{C}$ and $b = b(\mathrm{Aut}(\mathcal{C})$. Then from statement (2) of Theorem 1.2 and implication (1)⇒(2) of Lemma 9.1 it follows that there exist points $v_1, \ldots, v_{b-1}$ of W such that $W_{v_1,\ldots,v_{b-1}}$ is a 1-regular ring. So $s(W_{v_1,\ldots,v_{b-1}}) = 1$ by Theorem 9.3 and consequently $s(W) \leq b$ by statement (1) of Theorem 3.2.∎

The paper consists of nine sections. Section 2 contains the main definitions and the notation concerning cellular rings. In Section 3 we define the separability number and give a brief exposition of the theory of m-extended rings and m-isomorphisms. In Section 4 the definitions and notations concerning Schur rings over a finite group are presented. Next we introduce Cayley rings and indicate a relationship between them and Schur rings. Finally, we define normal Cayley rings and Schur rings, describe their elementary properties and give examples of normal Cayley rings derived from cyclotomic schemes. Section 5 is devoted to Schur rings over a cyclic group. In Section 6 a powerful criterion of normality for Cayley and Schur rings over a cyclic group is formulated and its various corollaries are deduced. Section 7 contains the proof of Theorem 6.1. The Schurity of the cellular rings W^* and $\widehat{W}^*$ used in the proof of Theorem 1.2 is established in Section 8. Finally, in Section 9 (Appendix) we define and study 1-regular cellular rings used in the proof of the main results.

Notation. As usual by $\mathbb{C}$ and $\mathbb{Z}$ we denote the complex field and the ring of integers.

Throughout the paper V denotes a finite set with $n = |V|$ elements. A subset of $V \times V$ is called a relation on V. For a relation R on V we define its support V_R to be the smallest set $U \subset V$ such that $R \subset U \times U$. If $u \in V$, then by the neighbourhood of u in R we mean the set $R(u) = \{v \in V : \ (u, v) \in R\}$.

By an equivalence E on V we always mean an ordinary equivalence relation on a subset of V (coinciding with V_E). The set of equivalence classes of E will be denoted by V/E.

The ring of all integral matrices whose rows and columns are indexed by the elements of V is denoted by Mat_V, its unity element (the identity matrix) by I_V and the all-one matrix by J_V.

[3] Another proof is based on statement (3) of Theorem 1.2. In this case one should use implication (1)⇒(3) (instead of implication (1)⇒(2)) of Lemma 9.1 and statement (2) (instead of statement (1)) of Theorem 3.2.

For $U \subset V$ the ring Mat_U can be treated in a natural way as a subring of Mat_V. If $A \in \mathrm{Mat}_V$, then A_U will denote the submatrix of A corresponding to U.

The adjacency matrix of a relation R is denoted by $A(R)$; this is a $\{0,1\}$-matrix of Mat_V such that its (u,v)-entry equals 1 iff $(u,v) \in R$.

The transpose of a matrix A is denoted by A^T. If R is a relation on V, then R^T denotes the relation with adjacency matrix $A(R)^T$.

Each bijection $g : V \to V'$ $(v \mapsto v^g)$ defines a natural ring isomorphism from Mat_V onto $\mathrm{Mat}_{V'}$. The image of a matrix A under it will be denoted by A^g. If R is a relation on V, then we set R^g to be the relation on V' with adjacency matrix $A(R)^g$.

The group of all permutations of V is denoted by $\mathrm{Sym}(V)$. If $\Gamma \le \mathrm{Sym}(V)$, then $\mathrm{Orb}(\Gamma) = \mathrm{Orb}(\Gamma, V)$ denotes the set of all orbits of Γ on V.

Let G be a group. The permutation group on G defined by the right (resp. left) multiplications is denoted by G_{right} (resp. G_{left}). If a group K faithfully acts on G as a group of its automorphisms, then we identify the semidirect product $G \cdot K$ with the permutation group on the set G generated by G_{right} and the subgroup of $\mathrm{Sym}(G)$ induced by the action of K.

2 Cellular rings

All undefined terms below concerning permutation groups can be found in [19, 20].

2.1. Let V be a finite set. By a *cellular* ring on V we mean a subring W of Mat_V satisfying the following conditions:

(A1) $I_V, J_V \in W$,

(A2) $\forall A \in W: \quad A^T \in W$,

(A3) $\forall A, B \in W: \quad A \circ B \in W$,

where $A \circ B$ is the Hadamard (componentwise) product of the matrices A and B. The elements of V are called the *points* and the set V is called the *point set* of W. The number $\mathrm{rk}(W) = \dim_{\mathbb{Z}}(W)$ is called the *rank* of W.

Each cellular ring W on V has a uniquely determined $\mathbb{Z}$-base $\mathcal{M} = \mathcal{M}(W)$ consisting of $\{0,1\}$-matrices such that

$$\sum_{A \in \mathcal{M}} A = J_V \quad \text{and} \quad A \in \mathcal{M} \ \Rightarrow \ A^T \in \mathcal{M}. \tag{2}$$

The linear base $\mathcal{M}$ is called the *standard basis* of W and its elements the *basis matrices*. The structure constants of W with respect to $\mathcal{M}$ are called the *structure constants* of W. Denote by $\mathcal{M}^* = \mathcal{M}^*(W)$ the set of all sums of different elements of $\mathcal{M}$, i.e. the set of all $\{0,1\}$-matrices belonging to W.

We say that cellular rings W on V and W' on V' are *strongly isomorphic*, if $W^g = W'$ for some bijection $g : V \to V'$ called a *strong isomorphism* from W to W'. The set of all of them is denoted by $\mathrm{Iso}(W, W')$. The group $\mathrm{Iso}(W) = \mathrm{Iso}(W, W)$ contains a normal subgroup

$$\mathrm{Aut}(W) = \{g \in \mathrm{Sym}(V) : \ A^g = A, \ A \in W\}$$

called the *automorphism group* of W. Conversely, for any permutation group $\Gamma \le \mathrm{Sym}(V)$ its *centralizer ring*

$$\mathcal{Z}(\Gamma) = \{A \in \mathrm{Mat}_V :\ A^g = A,\ g \in \Gamma\}$$

is a cellular ring on V. If a group Γ' acts on V, then we set $\mathcal{Z}(\Gamma', V) = \mathcal{Z}(\Gamma)$ where Γ is the permutation group on V induced by Γ'. A cellular ring W is called *Schurian* if $W = \mathcal{Z}(\mathrm{Aut}(W))$.

The set of all cellular rings on V is partially ordered by inclusion. The largest and the smallest elements of the set are respectively the full matrix ring Mat_V and the ring $\mathcal{Z}(\mathrm{Sym}(V))$ with the linear base $\{I_V, J_V\}$. We write $W \le W'$ if $W \subset W'$. One can easily see that for cellular rings $W_1, W_2 \le \mathrm{Mat}_V$ the set $W_1 \cap W_2$ is also a cellular ring on V. This implies that there exists the smallest cellular ring W on V such that $W_1 \le W$, $W_2 \le W$. Thus the set of all cellular rings on V is a lattice.

2.2. Let $W \le \mathrm{Mat}_V$ be a cellular ring, $\mathcal{M} = \mathcal{M}(W)$ and $\mathcal{M}^* = \mathcal{M}^*(W)$. Set

$$\mathrm{Cel}(W) = \{U \subset V :\ I_U \in \mathcal{M}\}, \quad \mathrm{Cel}^*(W) = \{U \subset V :\ I_U \in \mathcal{M}^*\}.$$

Each element of $\mathrm{Cel}(W)$ (resp. $\mathrm{Cel}^*(W)$) is called a *cell* of W (resp. a *cellular set* of W). Obviously,

$$V = \bigcup_{U \in \mathrm{Cel}(W)} U \qquad \text{(disjoint union)}.$$

The ring W is called *homogeneous* if $|\mathrm{Cel}(W)| = 1$.

For $U_1, U_2 \in \mathrm{Cel}^*(W)$ set $\mathcal{M}_{U_1,U_2} = \{A \in \mathcal{M} :\ I_{U_1} A I_{U_2} = A\}$. Then

$$\mathcal{M} = \bigcup_{U_1,U_2 \in \mathrm{Cel}(W)} \mathcal{M}_{U_1,U_2} \qquad \text{(disjoint union)}.$$

For $A \in \mathcal{M}_{U_1,U_2}$ where $U_1, U_2 \in \mathrm{Cel}(W)$ let $d_{out}(A)$ (resp. $d_{in}(A)$) be the coefficient of I_{U_1} (resp. I_{U_2}) in the decomposition of AA^T (resp. $A^T A$) with respect to the standard basis $\mathcal{M}$ of W. It is easily seen that this positive integer equals the number of 1's in the row (res. column) of the matrix A corresponding to any element of U_1 (resp. U_2). If W is homogeneous, then $d_{out}(A) = d_{in}(A)$ for all $A \in \mathcal{M}$ and we use the notation $d(A)$ for this number and call it the *degree* of A[4]. A cellular ring W is called *semiregular* if $d_{in}(A) = d_{out}(A) = 1$ for all $A \in \mathcal{M}$. A homogeneous semiregular ring is called *regular*. From [6, Theorem 4.4] it follows that the semiregular (regular) rings are Schurian and so coincide with the centralizer rings of semiregular (regular) permutation groups.

Sometimes it is convenient for us to deal with binary relations R on V for which $A(R) \in W$. We define $\mathcal{R}$ (resp. $\mathcal{R}^*$, $\mathcal{R}_{U_1,U_2}$) to be the set of all R such that $A(R)$ belongs to $\mathcal{M}$ (resp. $\mathcal{M}^*$, $\mathcal{M}_{U_1,U_2}$). The elements of $\mathcal{R}$ are called *basis relations* of W. We use all notions and notations introduced for basis matrices of a cellular ring (degree, $d(A), \ldots$) also for basis relations. In fact, the pair $\mathcal{C} = (V, \mathcal{R})$ is the coherent configuration corresponding to W (see Section 1). It is easy to see that the intersection numbers of $\mathcal{C}$ coincide with the structure constants of W.

[4]The mapping $A \mapsto d(A)$ induces by linearity a ring homomorphism from W to $\mathbb{Z}$.

2.3. Let W be a cellular ring on V and E be an equivalence on V. We say that E is an *equivalence* of W if $E \in \mathcal{R}^*$. In this case its support V_E is obviously a cellular set of W. The set of all equivalences of W is denoted by $\mathcal{E}(W)$. Set $\mathcal{B}(W) = \bigcup_{E \in \mathcal{E}(W)} V/E$. An element of this set is called a *block* of W. It immediately follows from the definition that $\mathrm{Cel}^*(W) \subset \mathcal{B}(W)$.

Given $U \in \mathcal{B}(W)$ the set $W_U = \{A_U : \ A \in W\}$ is a subring of Mat_U. It is obviously closed with respect to the transposition and the Hadamard multiplication and contains the matrices I_U and J_U. Thus W_U is a cellular ring on U called the *restriction* of W to U. Moreover,

$$\mathcal{M}(W_U) = \{A_U \ : \ A \in \mathcal{M}, \ I_U A I_U \neq 0\}. \tag{3}$$

From the first part of (2) it follows that each basis matrix of W_U can be uniquely represented in the form A_U for $A \in \mathcal{M}(W)$. If $U \in \mathrm{Cel}^*(W)$, then (3) implies that the basis matrices of W_U are in a one-to-one correspondence to the matrices of $\mathcal{M}_{U,U}$.

2.4. Along with the notion of a strong isomorphism we consider for cellular rings also weak isomorphisms (see [6]). Cellular rings W on V and W' on V' are called *weakly isomorphic* if there exists a $\mathbb{Z}$-module isomorphism $\varphi : W \to W'$ such that

$$\varphi(A \cdot B) = \varphi(A) \cdot \varphi(B), \quad \varphi(A \circ B) = \varphi(A) \circ \varphi(B) \quad \text{ for all } \ A, B \in W. \tag{4}$$

Any such φ is called a *weak isomorphism* from W to W'. It immediately follows from the definition that φ takes {0,1}-matrices to {0,1}-matrices and also that $\varphi(I_V) = I_{V'}$, $\varphi(J_V) = J_{V'}$. It was proved in [5, Lemma 4.1] that $\varphi(A^T) = \varphi(A)^T$ for all $A \in \mathcal{M}(W)$. Besides, φ induces a natural bijection $U \mapsto U^\varphi$ from $\mathrm{Cel}^*(W)$ onto $\mathrm{Cel}^*(W')$ preserving cells such that $\varphi(I_U) = I_{U^\varphi}$ and $|U| = |U^\varphi|$. In particular, $|V| = |V'|$. Finally, $\varphi(\mathcal{M}) = \mathcal{M}'$ and, moreover,

$$\varphi(\mathcal{M}_{U_1,U_2}) = \mathcal{M}'_{U_1^\varphi, U_2^\varphi} \quad \text{for all } \ U_1, U_2 \in \mathrm{Cel}^*(W) \tag{5}$$

where $\mathcal{M} = \mathcal{M}(W)$ and $\mathcal{M}' = \mathcal{M}(W')$. In this case the structure constants of W equal the corresponding structure constants of W'.

We observe that the composition of weak isomorphisms and the inverse of a weak isomorphism are also weak isomorphisms. The set of all weak isomorphisms from W to W' is denoted by $\mathrm{Isow}(W, W')$. Evidently each strong isomorphism from W to W' induces a weak isomorphism between these rings. Given $\varphi \in \mathrm{Isow}(W, W')$ set

$$\mathrm{Iso}(W, W', \varphi) = \{f \in \mathrm{Iso}(W, W') : \ \varphi_f = \varphi\}$$

where φ_f is the weak isomorphism induced by f. If $W = W'$ we write $\mathrm{Isow}(W)$ instead of $\mathrm{Isow}(W, W)$ and $\mathrm{Iso}(W, \varphi)$ instead of $\mathrm{Iso}(W, W, \varphi)$.

The following statement from [6, Lemma 2.2] describes the behavior of the relations of a cellular ring under weak isomorphisms.

Lemma 2.1 *Let $W \leq \mathrm{Mat}_V$ and $W' \leq \mathrm{Mat}_{V'}$ be cellular rings and $\varphi \in \mathrm{Isow}(W, W')$. Then φ induces a bijection $R \mapsto R^\varphi$ from the set $\mathcal{R}^*(W)$ onto the set $\mathcal{R}^*(W')$ such that $\varphi(A(R)) = A(R^\varphi)$. Moreover, this bijection maps $\mathcal{R}(W)$ onto $\mathcal{R}(W')$ and also*

(1) $(R^\varphi)^T = (R^T)^\varphi$, $d_{in}(R) = d_{in}(R^\varphi)$, $d_{out}(R) = d_{out}(R^\varphi)$, $|R| = |R^\varphi|$ *for all* $R \in \mathcal{R}(W)$,

(2) $E \in \mathcal{E}(W)$ *iff* $E^\varphi \in \mathcal{E}(W')$, *and also* $|V_E| = |V'_{E^\varphi}|$ *and* $|V/E| = |V'/E^\varphi|$.■

2.5. Let $W \le \mathrm{Mat}_V$ be a cellular ring and Φ a subgroup of $\mathrm{Isow}(W)$. Then according to [3, Lemma 3.1] the set $W^\Phi = \{A \in W : \varphi(A) = A, \varphi \in \Phi\}$ is a cellular ring on V. If G is a subgroup of $\mathrm{Iso}(W)$, then we set $W^G = W^\Phi$ where $\Phi = \{\varphi_f : f \in G\}$. Obviously, $G \le \mathrm{Aut}(W^G)$. The following statement will be used in proving Theorem 4.8.

Theorem 2.2 *Let* W *be a cellular ring,* G *a subgroup of* $\mathrm{Iso}(W)$ *and* $\rho : G \to \mathrm{Sym}(\mathrm{Cel}(W))$ *the homomorphism induced by the action of* G *on the set* $\mathrm{Cel}(W)$*. Suppose that the following conditions are satisfied:*

(1) $\mathrm{im}(\rho)$ *is a regular subgroup of* $\mathrm{Sym}(\mathrm{Cel}(W))$,

(2) $\ker(\rho) \le \mathrm{Aut}(W)$

Then $\mathrm{Aut}(W^G) = G\,\mathrm{Aut}(W)$*. Furthermore, the ring* W *is Schurian iff so is* W^G.

Proof. The first statement of the theorem is the consequence of Lemma 2.3 below: condition (1) of this lemma is satisfied because any regular group is 2-closed (see [20, Corollary 5.4]) whereas condition (2) follows from the observation that in this case the subgroup of G leaving fixed any cell of W equals $\ker(\rho)$.

Lemma 2.3 *In the notation of the theorem* $\mathrm{Aut}(W^G) = G\,\mathrm{Aut}(W)$ *whenever*

(1) $\mathrm{im}(\rho)$ *is a 2-closed subgroup of* $\mathrm{Sym}(\mathrm{Cel}(W))$,

(2) *for any* $U_1, U_2 \in \mathrm{Cel}(W)$ *the induced action of the group* $\{g \in G : U_1^g = U_1, U_2^g = U_2\}$ *on the set* $\mathcal{R}_{U_1,U_2}$ *is trivial.*

Proof. Since $G \le \mathrm{Aut}(W^G)$, we have $\mathrm{Aut}(W^G) \ge G\,\mathrm{Aut}(W)$. To prove the converse inclusion let $R \in \mathcal{R}(W^G)$. Then by the definition of W^G we have $R = \bigcup_{g\in G} S^g$ for some $S \in \mathcal{R}(W)$. So

$$R = \bigcup_{(U_1,U_2)\in O} R_{U_1,U_2}, \quad R_{U_1,U_2} = R \cap (U_1 \times U_2), \tag{6}$$

for some 2-orbit O of the group $\mathrm{im}(\rho)$. From the condition (2) it follows that

$$R_{U_1,U_2} \in \mathcal{R}(W) \quad \text{for all} \quad (U_1,U_2) \in O. \tag{7}$$

From the definition of W^G it follows that the equivalence with the set of classes $\mathrm{Cel}(W)$ belongs to $\mathcal{E}(W^G)$. Denote by $\rho' : \mathrm{Aut}(W^G) \to \mathrm{Sym}(\mathrm{Cel}(W))$ the homomorphism induced by the action of $\mathrm{Aut}(W^G)$ on $\mathrm{Cel}(W)$. Clearly, $\rho'|_G = \rho$. Moreover, by formula (6) the groups $\rho(G)$ and $\rho'(\mathrm{Aut}(W^G))$ have the same 2-orbits. Therefore, condition (1) implies that $\rho(G) = \rho'(\mathrm{Aut}(W^G))$.

On the other hand, formula (7) shows that $\ker(\rho') \le \mathrm{Aut}(W)$. Thus, $\mathrm{Aut}(W^G) \le G\,\mathrm{Aut}(W)$ and we are done.■

It is easy to see that the ring W^G is Schurian whenever W is. Conversely, suppose that W^G is Schurian. Let $S \in \mathcal{R}(W)$. Then $S = R_{U_1,U_2}$ for some $R \in \mathcal{R}(W^G)$ and $U_1, U_2 \in \mathrm{Cel}(W)$ (see (6), (7)). Since $\mathrm{Aut}(W^G)$ transitively acts on R, the subgroup of it leaving fixed U_1 and U_2 as sets transitively acts on S. However the latter group equals in $\ker(\rho)$ by condition (1) and hence is contained in $\mathrm{Aut}(W)$ by condition (1). Thus W is a Schurian ring.■

2.6. Given subsets $X_1, \ldots, X_s$ of Mat_V, their *cellular closure*, i.e. the smallest cellular ring on V containing all of them is denoted by $[X_1, \ldots, X_s]$. If $X_i = \{A_i\}$, we omit the braces. For a cellular ring $W \le \mathrm{Mat}_V$ and points $v_1, \ldots, v_s \in V$ we set $W_{v_1,\ldots,v_s} = [W, I_{v_1}, \ldots, I_{v_s}]$ where $I_{v_i} = I_{\{v_i\}}$ and call this ring the *extension* of W with respect to $v_1, \ldots, v_s$ or $(v_1, \ldots, v_s)$-extension of W. It is easy to see that

$$W_{v_1,\ldots,v_s} \le \mathcal{Z}(\mathrm{Aut}(W)_{v_1,\ldots,v_s}), \quad \mathrm{Aut}(W_{v_1,\ldots,v_s}) = \mathrm{Aut}(W)_{v_1,\ldots,v_s}. \tag{8}$$

We note that there exist cellular rings for which the first inclusion is strict. In the nonhomogeneous case a simple example is obtained by adding extra point to any non-Schurian ring. The smallest homogeneous ring with non-Schurian one-point extension we know is given by the cellular ring of rank 4 on 182 points coming from the Hall projective plane of order 9. Formulas (8) imply that if W is Schurian, then the cells of a one-point extension W_v of W coincide with the orbits of the group $\mathrm{Aut}(W)_v$, i.e. with the neighbourhoods of v in the basis relations of W. In the general case, we can only state that the latter sets are cellular sets of W_v.

3 Separability number of a cellular ring

In this section we outline the theory of m-extended rings and m-isomorphisms developed in [3]-[6] we need to define the separability number.

3.1. Let $\Gamma \le \mathrm{Sym}(V)$ be a permutation group. Given a positive integer m, denote by $\widehat{\Gamma}^{(m)}$ the permutation group on V^m induced by the action of Γ on the m-tuples of points. It is easy to see that $\widehat{\Gamma}^{(m)}$ coincide with the setwise stabilizer of the set $\Delta = \Delta^{(m)}(V) = \{(v, \ldots, v) \in V^m :\ v \in V\}$ in the m-fold direct product of Γ acting coordinatewise on V^m. It follows that the ring $\mathcal{Z}_m(\Gamma) = \mathcal{Z}(\widehat{\Gamma}^{(m)})$ contains both the m-fold tensor product of $\mathcal{Z}(\Gamma)$ and the matrix I_Δ. This suggest the following definition. For a cellular ring $W \le \mathrm{Mat}_V$ set

$$\widehat{W}^{(m)} = [W^m, I_\Delta] \tag{9}$$

where W^m is the m-fold tensor product of W. The cellular ring $\widehat{W}^{(m)} \le \mathrm{Mat}_{V^m}$ is called the *m-extended ring* of W. Clearly, $\widehat{W}^{(1)} = W$. It was proved in [5, Theorem 3.2] that

$$\widehat{W}^{(m)} = [W^m,\ \mathcal{Z}_m(\mathrm{Sym}(V))]^5 \tag{10}$$

[5]In papers [3]-[6] the ring $\widehat{W}^{(m)}$ was defined by formula (10).

It follows that the set $\mathcal{R}^*(\widehat{W}^{(m)})$ contains all binary relations on V^m invariant with respect to $\mathrm{Sym}(V)$, in particular, those defined by equalities of coordinates.

From (9) it follows that $\mathrm{Aut}(\widehat{W}^{(m)}) = \widehat{\mathrm{Aut}(W)}^{(m)}$. So $\widehat{W}^{(m)} \leq \mathcal{Z}_m(\mathrm{Aut}(W))$. We note that the equality does not always hold (even for $W = \mathcal{Z}(\Gamma)$); the smallest example we know is the homogeneous cellular ring of rank 4 on 62 points corresponding to the projective plane of order 5. Nevertheless the equality does hold whenever $m \geq n$ where $n = |V|$. This follows from Corollary 9.7 of this paper because $b(W) \leq n-1$.

The following statement showing the relationship between point extensions of W and some parts of $\widehat{W}^{(m)}$ will be used in the next sections.

Lemma 3.1 *Let $W \leq \mathrm{Mat}_V$ be a cellular ring, m a positive integer and $\widehat{W} = \widehat{W}^{(m)}$. For $v_1, \ldots, v_{m-1} \in V$ set $U = \{\overline{u} \in V^m : \ u_i = v_i, \ i = 1, \ldots, m-1\}$. Then $U \in \mathcal{B}(\widehat{W})$ and*

$$\widehat{W}_U \geq (W_{v_1,\ldots,v_{m-1}})^\zeta$$

where $\zeta : V \to U$ is the bijection taking v to $(v_1, \ldots, v_{m-1}, v)$.

Proof. Follows from [4, Lemma 3.1] after taking into account that U is a class of the equivalence $\{(\overline{u}, \overline{v}) \in V^m \times V^m : \ u_i = v_i, \ i = 1, \ldots, m-1\}$ belonging to $\mathcal{E}(\widehat{W})$.■

3.2. Let $\varphi : W \to W'$ be a weak isomorphism from a cellular ring $W \leq \mathrm{Mat}_V$ to a cellular ring $W' \leq \mathrm{Mat}_{V'}$. We say that a weak isomorphism $\psi : \widehat{W}^{(m)} \to \widehat{W'}^{(m)}$ is an *m-extension* of φ if $\psi(I_\Delta) = I_{\Delta'}$ and $\psi(A) = \varphi^m(A)$ for all $A \in W^m$ where $\Delta = \Delta^{(m)}(V)$, $\Delta' = \Delta^{(m)}(V')$ and φ^m is the weak isomorphism from W^m to $(W')^m$ induced by φ. Clearly, any weak isomorphism has a 1-extension coinciding with itself. However, for $m \geq 2$ the m-extension does not always exist. For example, a straightforward computation shows that the weak isomorphism of the adjacency ring of the unique conference graph type scheme on 15 points induced by the transposition does not have a 2-extension. It can be proved that the existence of the m-extension implies the existence of the l-extension for $l \leq m$. Certainly, the m-extension is uniquely determined (if it exists).

A weak isomorphism φ is called an *m-isomorphism* if there exists an m-extension of φ. The set of all m-isomorphisms from W to W' will be denoted by $\mathrm{Isow}_m(W, W')$. It was proved in [5, Theorem 4.5 and formula (7)] that

$$\mathrm{Isow}(W, W') = \mathrm{Isow}_1(W, W') \supset \ldots \supset \mathrm{Isow}_n(W, W') = \ldots = \mathrm{Isow}_\infty(W, W') \tag{11}$$

where $\mathrm{Isow}_\infty(W, W')$ is the set of all weak isomorphisms from W to W' induced by strong isomorphisms. A cellular ring W is called *m-separable* if $\mathrm{Isow}_m(W, W') = \mathrm{Isow}_\infty(W, W')$ for any cellular ring W'. This means that any m-isomorphism from W to another cellular ring is induced by a strong isomorphism. A scheme is called m-separable if so is its adjacency ring. From (11) it follows that an m-separable ring is l-separable for all $l \geq m$. We set

$$s(W) = \min\{m : \ W \text{ is } m-\text{separable}\}.$$

and call this positive integer the *separability number* of W. The separability number $s(\mathcal{C})$ of a scheme $\mathcal{C}$ is defined to be the separability number of its adjacency ring.

In some cases the separability number can easily be computed. For instance, $s(W) = 1$ whenever W is of rank 2 or a semiregular ring. In particular, $s(\mathrm{Mat}_V) = 1$. It is less trivial that all the Johnson, Hamming and Grassmann schemes are 2-separable. Moreover, for the schemes belonging to the first two families the exact value of the separability number can be found. In the general case the situation is more complicated. Namely, it was proved in [5, Theorem 1.3] that there exist cellular rings with arbitrarily large separability number. More exactly,

$$\liminf_{n(W)\to\infty} \frac{s(W)}{n(W)} > 0$$

where W runs over all cellular rings and $n(W)$ is the number of points of W. However, it can be proved that $s(W) \le \lceil n/3 \rceil$ for any cellular ring on n points.

The following theorem gives some upper bounds for the separability number of a cellular ring via the separability numbers of some rings associated with it.

Theorem 3.2 ([6, Theorem 4.6]) *Let $W \le \mathrm{Mat}_V$ be a cellular ring. Then*

(1) $s(W) \le s(W_v) + 1$ *for all* $v \in V$,

(2) $s(W) \le m\, s(\widehat{W}^{(m)})$ *for all* $m \ge 1$.■

We complete the section by making some remarks on the relations between the separability number and the characterization of schemes. Let $\mathcal{C}$ be a scheme. Saying that the intersection numbers of $\mathcal{C}$ and another scheme $\mathcal{C}'$ are the same we mean that a weak isomorphism $\varphi : W \to W'$ where W and W' are the adjacency rings of $\mathcal{C}$ and $\mathcal{C}'$, respectively, is given. Thus $\mathcal{C}$ is characterized by the intersection numbers iff $s(\mathcal{C}) = 1$. This understanding of characterization is adequate to the point of view of [1]. Next, we could call the intersection numbers of the scheme $\widehat{\mathcal{C}}^{(m)}$ (the structure constants of $\widehat{W}^{(m)}$) by the m-dim intersection numbers of $\mathcal{C}$. Then it is natural to say that the m-dim intersection numbers of $\mathcal{C}$ and $\mathcal{C}'$ are the same if the intersection numbers of $\mathcal{C}$ and $\mathcal{C}'$ are the same and the corresponding weak isomorphism φ has an m-extension. Thus $\mathcal{C}$ is characterized by the intersection numbers of $\widehat{\mathcal{C}}^{(m)}$ (the m-dim intersection numbers of $\mathcal{C}$) iff $s(\mathcal{C}) \le m$.

4 Schur rings and Cayley rings. Normality

4.1. Let G be a finite group. On the free $\mathbb{Z}$-module $\mathbb{Z}[G]$ spanned by G we define the involution, the group multiplication and the Hadamard multiplication by the formula

$$\xi^* = \sum_{g\in G} a_g g^{-1}, \quad \xi \cdot \eta = \sum_{g,h\in G} a_g b_h gh, \quad \xi \circ \eta = \sum_{g\in G} a_g b_g g$$

where $\xi = \sum_{g\in G} a_g g$ and $\eta = \sum_{g\in G} b_g g$. Obviously, $\xi(X^{-1}) = \xi(X)^*$ and $\xi(X \cap Y) = \xi(X) \circ \xi(Y)$ for all $X, Y \subset G$, where $\xi(X) = \sum_{x\in X} x$.

In accordance with [19] (see also [8]), a submodule $\mathcal{A}$ of $\mathbb{Z}[G]$ is called a *Schur ring* (briefly an *S-ring*) over G if it is closed under the involution and under the group and Hadamard multiplications, and contains the unity elements 1 and $\xi(G)$ with respect to the multiplications. The number $\mathrm{rk}(\mathcal{A}) = \dim_{\mathbb{Z}}(\mathcal{A})$ is called the *rank* of $\mathcal{A}$. We say that S-rings $\mathcal{A}$ over G and $\mathcal{A}'$ over G' are *Cayley isomorphic* if there exists a group isomorphism $f : G \to G'$ such that $\mathcal{A}'$ equals the image of $\mathcal{A}$ with respect to the homomorphism from $\mathbb{Z}[G]$ to $\mathbb{Z}[G']$ induced by f.

It is easy to show that each S-ring $\mathcal{A}$ has a uniquely determined $\mathbb{Z}$-base consisting of the elements $\xi(X)$ with X running over a family $\mathcal{S} = \mathcal{S}(\mathcal{A})$ (also uniquely determined by $\mathcal{A}$) of pairwise disjoint nonempty subsets of G such that

$$\{1\} \in \mathcal{S}, \quad \bigcup_{X\in\mathcal{S}} X = G \quad \text{and} \quad X \in \mathcal{S} \;\Rightarrow\; X^{-1} \in \mathcal{S}.$$

We call the elements of $\mathcal{S}(\mathcal{A})$ *basic sets* of $\mathcal{A}$ and denote by $\mathcal{S}^*(\mathcal{A})$ the set of all unions of them. The basic set of $\mathcal{A}$ containing $x \in G$ is denoted by $[x]$. The set of all subgroups of G belonging to $\mathcal{S}^*(\mathcal{A})$ is denoted by $\mathcal{H}(\mathcal{A})$. One can show that $\mathcal{H}(\mathcal{A})$ contains the subgroup $\langle X\rangle$ generated by a set $X \in \mathcal{S}^*(\mathcal{A})$.

The set of all S-rings over a group G is ordered by inclusion. The largest and the smallest elements of this set are $\mathbb{Z}[G]$ and $\mathbb{Z}1 + \mathbb{Z}\xi$ with $\xi = \xi(G \setminus \{1\})$. Next, let K be a subgroup of the group $\mathrm{Aut}(G)$. Then, obviously, the set $\mathcal{A}$ of all K-invariant elements of $\mathbb{Z}[G]$ is an S-ring over G. It is easily seen that $\mathcal{S}(\mathcal{A})$ coincides with the set of all orbits of the group K on G. Such an S-ring is called an *orbit* S-ring and is denoted by $\mathcal{O}(K, G)$.

Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be S-rings over groups G_1 and G_2 respectively. Then the tensor product $\mathcal{A}_1\otimes\mathcal{A}_2$ is obviously an S-ring over the group $G_1 \times G_2$ and we have $\mathcal{S}(\mathcal{A}_1 \otimes \mathcal{A}_2) = \{X_1 \times X_2 :\ X_1 \in \mathcal{S}(\mathcal{A}_1), X_2 \in \mathcal{S}(\mathcal{A}_2)\}$. In the case of orbit S-rings the following equality holds:

$$\mathcal{O}(K_1 \times K_2, G_1 \times G_2) = \mathcal{O}(K_1, G_1) \otimes \mathcal{O}(K_2, G_2) \tag{12}$$

where $K_i \le \mathrm{Aut}(G_i)$, $i = 1, 2$.

Let $\mathcal{A}$ be an S-ring over a group G, H a subgroup of G belonging to $\mathcal{H}(\mathcal{A})$, and $i : H \to G$ the natural injection. Then it is easy to see that the $\mathbb{Z}$-module $\mathcal{A}_H = i^{-1}(\mathcal{A})$ is an S-ring over H, and

$$\mathcal{S}(\mathcal{A}_H) = \{i^{-1}(X) :\ X \in \mathcal{S}(\mathcal{A}),\ X \subset \mathrm{im}(i)\}.$$

Suppose, moreover, that H is normal in G. Then, in a similar way, the $\mathbb{Z}$-module $\mathcal{A}_{G/H} = \pi(\mathcal{A})$ (where $\pi : G \to G/H$ is the natural surjection) is an S-ring over the group G/H and

$$\mathcal{S}(\mathcal{A}_{G/H}) = \{\pi(X) :\ X \in \mathcal{S}(\mathcal{A})\}. \tag{13}$$

Given $X \subset G$ the set

$$\mathrm{rad}(X) = \{g \in G :\ gX = Xg = X\} \tag{14}$$

is obviously a subgroup of G called the *radical* of X. Thus, $\mathrm{rad}(X)$ is the largest subgroup of G such that X is a union of left as well as right cosets by it. From the definition it follows that $\mathrm{rad}(\pi(X)) = \pi(\mathrm{rad}(X))$ for any normal subgroup H of G contained in $\mathrm{rad}(X)$. In particular, if $\mathrm{rad}(X)$ is normal in G and $H = \mathrm{rad}(X)$, then $\mathrm{rad}(\pi(X)) = \{1\}$. If $X \in \mathcal{S}^*(\mathcal{A})$, then it is easy to see that $\mathrm{rad}(X) \in \mathcal{H}(\mathcal{A})$.

4.2. S-rings naturally lead to cellular rings of special kind defined as follows.

Definition 4.1 *Let G be a group. A cellular ring $W \leq \mathrm{Mat}_G$ is called a Cayley ring over G if the group G_{right} is contained in* $\mathrm{Aut}(W)$.

From the definition it follows that every Cayley ring is homogeneous. The smallest and the largest Cayley rings over G are $\mathcal{Z}(\mathrm{Sym}(G))$ and $\mathcal{Z}(G_{right})$ respectively. We note that each basis relation of a Cayley ring over G can be considered as the edge set of a Cayley graph on G whereas the scheme corresponding to it as a colored Cayley graph on G.

Given a group G the mapping

$$\rho_G : \mathbb{Z}[G] \to \mathrm{Mat}_G(\mathbb{Z}), \qquad g \mapsto P_g, \tag{15}$$

where P_g is the permutation matrix corresponding to the left multiplication by g, is obviously a ring injection the image of which is the enveloping ring of the group G_{left}, i.e. $\mathcal{Z}(G_{right})$. Moreover, it takes the Hadamard multiplication and the involution in $\mathbb{Z}[G]$ to the Hadamard multiplication and the involution in Mat_G. It is easy to see that the injection (15) induces a bijection $X \mapsto X^{\rho_G}$ between the subsets of G and the binary relations on G invariant with respect to G_{right} such that $A(X^{\rho_G}) = \rho_G(\xi(X))$. The following statement immediately follows from the definitions.

Theorem 4.2 *The mapping (15) defines a bijection $\mathcal{A} \mapsto W$ between the S-rings over G and the Cayley rings over G. Moreover, $\mathcal{S}(\mathcal{A})^{\rho_G} = \mathcal{R}(W)$, $\mathcal{S}^*(\mathcal{A})^{\rho_G} = \mathcal{R}^*(W)$, $\mathcal{H}(\mathcal{A})^{\rho_G} = \mathcal{E}(W)$, and given $H \in \mathcal{H}(\mathcal{A})$ we have $G/H^{\rho_G} = \{Hg : \ g \in G\}$ and $\rho_H(\mathcal{A}_H) = W_H$.*■

Theorem 4.2 enables us to transfer the notions of weak isomorphism and strong isomorphism from cellular rings to S-rings. Namely, S-rings $\mathcal{A}$ over G and $\mathcal{A}'$ over G' are said to be *weakly isomorphic* (see (4)) if there exists a $\mathbb{Z}$-module isomorphism $\varphi : \mathcal{A} \to \mathcal{A}'$ (called a *weak isomorphism* from $\mathcal{A}$ to $\mathcal{A}'$) such that

$$\varphi(\xi \cdot \eta) = \varphi(\xi) \cdot \varphi(\eta), \quad \varphi(\xi \circ \eta) = \varphi(\xi) \circ \varphi(\eta) \quad \text{ for all } \ \xi, \eta \in \mathcal{A}. \tag{16}$$

From Lemma 2.1 it follows that φ induces a bijection $X \mapsto X^\varphi$ from $\mathcal{S}^*(\mathcal{A})$ onto $\mathcal{S}^*(\mathcal{A}')$ such that $\varphi(\xi(X)) = \xi(X^\varphi)$ (this bijection takes $\mathcal{S}(\mathcal{A})$ to $\mathcal{S}(\mathcal{A}')$ and $\mathcal{H}(\mathcal{A})$ to $\mathcal{H}(\mathcal{A}')$). Also, it can be proved that $(X^{-1})^\varphi = (X^\varphi)^{-1}$ and $|X^\varphi| = |X|$ for all $X \in \mathcal{S}^*(\mathcal{A})$.

Similarly, by a strong isomorphism from $\mathcal{A}$ to $\mathcal{A}'$ we mean a strong isomorphism of the corresponding Cayley rings taking 1_G to $1_{G'}$ (we note that if Cayley rings are strongly isomorphic, then obviously there exists a strong isomorphism of this kind). It follows that any strong isomorphism of S-rings induces a weak isomorphism of them coming from that of the corresponding Cayley rings.

Lemma 4.3 *A bijection $f : G \to G'$ is a strong isomorphism from $\mathcal{A}$ to $\mathcal{A}'$ iff*

$$f([x]y) = [f(x)]f(y), \quad x, y \in G. \tag{17}$$

In particular, any Cayley isomorphism of S-rings is a strong one.

Proof. Let f be a strong isomorphism from $\mathcal{A}$ to $\mathcal{A}'$. Then $f \in \mathrm{Iso}(W, W')$ where $W = \rho_G(\mathcal{A})$ and $W' = \rho_{G'}(\mathcal{A}')$, and $f(1) = 1$. Given $X \in \mathcal{S}(\mathcal{A})$ set $R = X^{\rho_G}$, $R' = R^f$, $X' = (R')^{\rho_{G'}^{-1}}$. From the definitions it follows that given $x, y \in G$ we have

$$x \in X \;\Leftrightarrow (y, xy) \in R \;\Leftrightarrow (f(y), f(xy)) \in R' \;\Leftrightarrow f(xy)f(y)^{-1} \in X'.$$

Since f is a bijection, this implies that $f(Xy)f(y)^{-1} = X'$. This equality shows that $X' = f(X)f(1)^{-1} = f(X)$ and so it can be rewritten in the form $f([x]y)f(y)^{-1} = [f(x)]$ where $x \in X$, which completes the proof.∎

By analogy with cellular rings we use the notations $\mathrm{Isow}(\mathcal{A}, \mathcal{A}')$, $\mathrm{Isow}(\mathcal{A})$, $\mathrm{Iso}(\mathcal{A}, \mathcal{A}')$, $\mathrm{Iso}(\mathcal{A}, \mathcal{A}', \varphi)$, $\mathrm{Iso}(\mathcal{A})$, $\mathrm{Iso}(\mathcal{A}, \varphi)$ and $\mathrm{Aut}(\mathcal{A})$. The latter group is called the *automorphism group* of $\mathcal{A}$. It follows that

$$\mathrm{Aut}(\mathcal{A}) = \mathrm{Aut}(W)_v, \qquad \mathrm{Aut}(W) = G_{right}\,\mathrm{Aut}(\mathcal{A}) \tag{18}$$

where W is the Cayley ring corresponding to $\mathcal{A}$ and $v = 1_G$. Obviously, $\mathrm{Aut}(\mathcal{A})$ equals $\{1\}$ if $\mathcal{A} = \mathbb{Z}[G]$ and equals $\mathrm{Sym}(G)_v$ if $\mathrm{rk}(\mathcal{A}) = 2$. It is easy to show that $\mathrm{Aut}(\mathcal{A}_1 \otimes \mathcal{A}_2) = \mathrm{Aut}(\mathcal{A}_1) \times \mathrm{Aut}(\mathcal{A}_2)$. The S-ring $\mathcal{A}$ is called *Schurian* if so is W, i.e. $\mathcal{S}(\mathcal{A}) = \mathrm{Orb}(\mathrm{Aut}(\mathcal{A}))$. We note that an orbit S-ring is obviously Schurian.

Let $\varphi \in \mathrm{Isow}(\mathcal{A}, \mathcal{A}')$. If $H \in \mathcal{H}(\mathcal{A})$, then following [8] denote by φ_H the weak isomorphism from $\mathcal{A}_H$ to $\mathcal{A}_{H'}$ induced by φ. If, moreover, H is normal in G, then denote by $\varphi_{G/H}$ the weak isomorphism from $\mathcal{A}_{G/H}$ to $\mathcal{A}'_{G'/H'}$ induced by φ. For $f \in \mathrm{Iso}(\mathcal{A}, \mathcal{A}')$ we use similar notations f_H and $f_{G/H}$. If $f \in \mathrm{Iso}(\mathcal{A}, \mathcal{A}', \varphi)$, then obviously $f_H \in \mathrm{Iso}(\mathcal{A}_H, \mathcal{A}'_{H'}, \varphi_H)$ and $f_{G/H} \in \mathrm{Iso}(\mathcal{A}_{G/H}, \mathcal{A}'_{G/H'}, \varphi_{G/H})$.

4.3. A Cayley ring W over a group G is called *normal* if G_{right} is a normal subgroup of $\mathrm{Aut}(W)$. Since a regular group is 2-closed, a regular Cayley ring is normal. More generally, $\mathcal{Z}(\Gamma)$ is a normal Cayley ring whenever Γ is a 2-closed subgroup of $\mathrm{Sym}(G)$ such that $G \le \Gamma \le G \cdot \mathrm{Aut}(G)$. In fact, every Schurian normal Cayley ring can be obtained in this way (see Corollary 4.6). However, there exist non-Schurian normal Cayley rings. A simple example comes from a non-Schurian S-ring over an elementary Abelian group of order p^2, $p \ge 5$ (see [15, 19]).

In this paper we completely identify normal Cayley rings over a cyclic group. In the general case we confine ourselves to citing some simplest properties.

Lemma 4.4 *The following statements hold:*

(1) *a Cayley ring containing a normal Cayley ring over the same group is also normal,*

(2) *the tensor product of Cayley rings is normal iff each factor is normal.*∎

The following statement gives a simple characterization of normal Cayley rings.

Theorem 4.5 *Let W be a Cayley ring over a group G. Then W is normal iff* $\mathrm{Aut}(W) \le G \cdot \mathrm{Aut}(G)$.

Proof. The sufficiency is obvious. Conversely, let the ring W be normal. It suffices to verify that $\mathrm{Aut}(W)_v \le \mathrm{Aut}(G)$ where $v = 1_G$. Since $\mathrm{Aut}(W)_v$ normalizes G_{right}, given $f \in \mathrm{Aut}(W)_v$ there exists $\sigma_f \in \mathrm{Aut}(G)$ such that

$$f^{-1} g_{right} f = (g^{\sigma_f})_{right}, \quad g \in G, \tag{19}$$

where g_{right} is the permutation of G induced by the right multiplication by g. The images of v under the permutations on the left-hand and right-hand sides of (19) equal $(v^{f^{-1}}g)^f = g^f$ and $vg^{\sigma_f} = g^{\sigma_f}$ respectively. So by (19) we have $g^f = g^{\sigma_f}$ for all $g \in G$. This means that $f = \sigma_f$ and we are done.■

As a corollary we have the following statement which will be made for a cyclic group considerably more precise in Section 6 (see Corollary 6.3).

Corollary 4.6 *The automorphism groups of normal Cayley rings over G are exactly the 2-closed subgroups of the holomorph $G \cdot \mathrm{Aut}(G)$ of G containing G.*■

We say that an S-ring is normal if so is the corresponding Cayley ring. Certainly, for normal S-rings the analog of Lemma 4.4 holds. Moreover, as a corollary of Theorem 4.5 and equalities (18) we obtain the following statement.

Theorem 4.7 *Let $\mathcal{A}$ be an S-ring over a group G. Then $\mathcal{A}$ is normal iff $\mathrm{Aut}(\mathcal{A}) \le \mathrm{Aut}(G)$.*■

4.4. An important example of a normal Cayley ring is given by a proper cyclotomic ring W on a finite field $\mathbb{F}$, i.e. the adjacency ring of a proper cyclotomic scheme $\mathcal{C}$ on $\mathbb{F}$ (see Section 1). Indeed, since $\mathrm{Aut}(W) = \mathrm{Aut}(\mathcal{C})$, equality (1) shows that W is a normal Cayley ring over the addiive group of $\mathbb{F}$. Let us describe two more natural constructions of normal Cayley rings also coming from cyclotomic schemes. They will be used in proving the main results of the paper.

Denote by A and G the additive and multiplicative groups of the field $\mathbb{F}$ and by $\Gamma = A \cdot G$ the semidirect product of A and G with G acting on A by multiplications, so that $(a_1 \cdot g_1)(a_2 \cdot g_2) = (a_1 g_2 + a_2) \cdot (g_1 g_2)$. We note that the group $\mathrm{Aut}(\mathbb{F})$ faithfully acts on the groups A, G and Γ as a group of their automorphisms. Below we shall identify $\mathrm{Aut}(\mathbb{F})$ with the corresponding subgroups of $\mathrm{Aut}(A)$, $\mathrm{Aut}(G)$ and $\mathrm{Aut}(\Gamma)$. The semidirect product $\Gamma \cdot \mathrm{Aut}(\mathbb{F})$ acts on the field $\mathbb{F}$ by

$$x^{\gamma \cdot \sigma} = a + x^\sigma g, \quad \gamma = a \cdot g \in \Gamma, \ \sigma \in \mathrm{Aut}(\mathbb{F}), \ x \in \mathbb{F}. \tag{20}$$

It is easy to see that the mapping

$$\widehat{f} : \mathbb{F}^2 \setminus \Delta \to \Gamma, \ (x, y) \mapsto x \cdot (y - x)$$

with $\Delta = \Delta^{(2)}(\mathbb{F})$, is a bijection. Moreover, $\widehat{f}$ takes the componentwise action of $\Gamma \cdot \mathrm{Aut}(\mathbb{F})$ on $\mathbb{F}^2 \setminus \Delta$ to the natural action of $\Gamma \cdot \mathrm{Aut}(\mathbb{F})$ on Γ (Γ acts on itself by right multiplications).

Let W be a cyclotomic ring on $\mathbb{F}$. Set

$$W' = ((W_u)_{\mathbb{F}^\times})^f, \quad \widehat{W}' = (\widehat{W}_{\widehat{\mathbb{F}}^\times})^{\widehat{f}} \tag{21}$$

where $u = 0_{\mathbb{F}}$, $\mathbb{F}^{\times} = \mathbb{F} \setminus \{u\}$, $f : \mathbb{F}^{\times} \to G$ is the identity map, $\widehat{\mathbb{F}}^{\times} = \mathbb{F}^2 \setminus \Delta$ and $\widehat{W} = \widehat{W}^{(2)}$. Since obviously $\mathrm{AGL}(1, \mathbb{F}) \le \mathrm{Iso}(W)$, it follows that $G_{right} \le \mathrm{Iso}(W')$ and $\Gamma_{right} \le \mathrm{Iso}(\widehat{W}')$. So according to the end of Subsection 2.5 one can consider cellular rings

$$W^* = (W')^{G_{right}}, \quad \widehat{W}^* = (\widehat{W}')^{\Gamma_{right}}. \tag{22}$$

Thus W^* is a Cayley ring over G and $\widehat{W}^*$ is a Cayley ring over Γ. Let us describe the properties of the ring $\widehat{W}^*$ to be used in the next theorem as well as in Theorem 8.1.

A straightforward computation shows that the equivalence on $\widehat{\mathbb{F}}^{\times}$ defined by the equality of the first coordinates and the relation of degree 1 on the same set defined by interchanging the coordinates (obviously belonging to $\mathcal{R}^*(\widehat{W})_{\widehat{\mathbb{F}}^{\times}}$ and invariant with respect to Γ) are taken by $\widehat{f}$ to $E_G = G^{\rho_\Gamma}$ and to $R_s = \{s\}^{\rho_\Gamma}$ respectively where s is the element of Γ with A-component $1_{\mathbb{F}}$ and G-component $-1_{\mathbb{F}}$. So

$$E_G \in \mathcal{E}(\widehat{W}^*), \quad R_s \in \mathcal{R}(\widehat{W}^*). \tag{23}$$

We also observe that $s^2 = 1_\Gamma$ and the equivalence $E_{G_1} = (G_1)^{\rho_\Gamma}$ with $G_1 = sGs$ is the image of the equivalence on $\widehat{\mathbb{F}}^{\times}$ defined by the equality of the second coordinates. Thus $E_{G_1} \in \mathcal{E}(\widehat{W}^*)$.

Theorem 4.8 *Let W be a proper cyclotomic ring on a finite field $\mathbb{F}$. Then in the above notation the following statements hold:*

1. $\mathrm{Aut}(W^*) \le G \cdot \mathrm{Aut}(\mathbb{F})$ *and* $\mathrm{Aut}(\widehat{W}^*) \le \Gamma \cdot \mathrm{Aut}(\mathbb{F})$*; in particular, the Cayley rings W^* and $\widehat{W}^*$ are normal,*
2. $G \in \mathcal{B}(\widehat{W}^*)$ *and* $(\widehat{W}^*)_G \ge W^*$*,*
3. *the cellular rings W_u and W^* (resp. $\widehat{W}$ and $\widehat{W}^*$) are Schurian or not simultaneously.*

Proof. Let us prove statements (1) and (3). First we observe that the hypothesis of Lemma 9.4 of Section 9 is satisfied for W with $X = \mathbb{F}^{\times}$ and for $\widehat{W}$ with $X = \widehat{\mathbb{F}}^{\times}$ (in the latter case $\Delta \in \mathrm{Cel}(\widehat{W})$ and we set $R_\Delta = (\widehat{\mathbb{F}}^{\times} \times \Delta) \cap E$ where E is the equivalence of $\widehat{W}$ defined by the equality of the first coordinates). So by statement (1) of this lemma

$$\mathrm{Aut}((W_u)_{\mathbb{F}^{\times}}) = \mathrm{Aut}(W)_{\mathbb{F}^{\times}}, \quad \mathrm{Aut}((\widehat{W}_{\widehat{\mathbb{F}}^{\times}}) = \mathrm{Aut}(\widehat{W})_{\widehat{\mathbb{F}}^{\times}}$$

and also the cellular rings W_u, $(W_u)_{\mathbb{F}^{\times}}$ and W' (resp. $\widehat{W}$, $\widehat{W}_{\widehat{\mathbb{F}}^{\times}}$ and $\widehat{W}'$) are Schurian or not simultaneously. From (1) it follows that the group $\mathrm{Aut}(W)_{\mathbb{F}^{\times}}$ (resp. $\mathrm{Aut}(\widehat{W})_{\widehat{\mathbb{F}}^{\times}}$) is contained in the permutation group defined according to (20) by the natural action of $G \cdot \mathrm{Aut}(\mathbb{F})$ (resp. $\Gamma \cdot \mathrm{Aut}(\mathbb{F})$) on the set $\mathbb{F}^{\times}$ (resp. $\widehat{\mathbb{F}}^{\times}$). Thus

$$\mathrm{Aut}(W') \le G \cdot \mathrm{Aut}(\mathbb{F}), \quad \mathrm{Aut}(\widehat{W}') \le \Gamma \cdot \mathrm{Aut}(\mathbb{F}).$$

Now to complete the proof of statements (1) and (3) it suffices to verify that the hypothesis of Lemma 2.2 is satisfied for the ring W' and the group G_{right} as well as for the ring $\widehat{W}'$ and the group Γ_{right}. To do this we observe that the neighbourhood of the point u in a basis relation of the cellular ring W is a cellular set of W_u whereas the basis relation itself is a cellular set of $\widehat{W}$ (the first is obvious whereas the second follows from [4, Proposition 3.6, Statement (1)]). Since W is a Schurian ring the both cellular sets are in fact cells. So any cell of $(W_u)_{\mathbb{F}^\times}$ is of the form Hg whereas any cell of $\widehat{W}_{\widehat{\mathbb{F}}^\times}$ is of the form $\{(x,y) \in \widehat{\mathbb{F}}^\times : \; x - y \in Hg\}$ where the group H is as in the definition of a cyclotomic scheme. Thus

$$\mathrm{Cel}(W') = \{Hg : \; g \in G\}, \quad \mathrm{Cel}(\widehat{W}') = \{AH\gamma : \; \gamma \in \Gamma\}.$$

It follows that G_{right} regularly acts on $\mathrm{Cel}(W')$ whereas Γ_{right} regularly acts on $\mathrm{Cel}(\widehat{W}')$. Since the kernels of these actions equal $H \le \mathrm{Aut}(W')$ and $AH \le \mathrm{Aut}(\widehat{W}')$ respectively, the hypothesis of Lemma 2.2 is satisfied and we are done.

Let us prove statement (2). First $G \in \mathcal{B}(\widehat{W}^*)$ because the equivalence $E_G = G^{\rho_\Gamma}$ belongs to $\mathcal{E}(\widehat{W}^*)$ (see formula (23) and Theorem 4.2). Next, since the group Γ_{right} regularly acts on the set $\Gamma/E_G = \{G\gamma : \; \gamma \in \Gamma\}$ and the setwise stabilizer of G in Γ_{right} equals G_{right}, we have

$$(\widehat{W}^*)_G = ((\widehat{W}')^{\Gamma_{right}})_G = (\widehat{W}'_G)^{G_{right}}. \tag{24}$$

On the other hand, denote by $\widehat{f}_1 : U \setminus \{(u,u)\} \to G$ and $\zeta_1 : \mathbb{F}^\times \to U \setminus \{(u,u)\}$ the bijections induced by $\widehat{f}$ and ζ where $U = \{u\} \times \mathbb{F}$. Then obviously $\zeta_1 \circ \widehat{f}_1 = f$. So by Lemma 3.1 with $m = 2$ and $v_1 = u$ we obtain that

$$\widehat{W}'_G = ((\widehat{W}_{\mathbb{F}^\times})^{\widehat{f}})_G = ((\widehat{W}_U)_{U \setminus \{(u,u)\}})^{\widehat{f}_1} \ge (((W_u)_{\mathbb{F}^\times})^{\zeta_1})^{\widehat{f}_1} = ((W_u)_{\mathbb{F}^\times})^f = W'. \tag{25}$$

Thus statement (2) follows from (24), (25) and the definition of W^*.■

5 S-rings over a cyclic group

5.1. We recall basic facts concerning finite cyclic groups (see e.g.[16]). Let G be a finite cyclic group of order n and $\mathcal{P}(G)$ the set of all prime divisors of n. Given $p \in \mathcal{P}(G)$ denote by G_p the Sylow p-subgroup of G. Then there are canonical decompositions

$$G = \prod_{p \in \mathcal{P}(G)} G_p, \quad \mathrm{Aut}(G) = \prod_{p \in \mathcal{P}(G)} \mathrm{Aut}(G_p). \tag{26}$$

We observe that each automorphism of G is of the form $\sigma_m = \sigma_{m,G} : x \mapsto x^m$ for some integer m relatively prime to n.

Let $p \in \mathcal{P}(G)$ and $|G_p| = p^k$, $k \ge 1$. Then $\mathrm{Aut}(G_p)$ is a cyclic group of order $(p-1)p^{k-1}$ whenever p is odd. If $p = 2$, then $\mathrm{Aut}(G_p)$ is trivial for $k = 1$ and is the direct product of a cyclic group of order 2 and a cyclic group of order 2^{k-2} for $k \ge 2$. More exactly,

$$\mathrm{Aut}(G_p) = A_{1,p} \times A_{2,p} \tag{27}$$

N	$K=\{\sigma_m:\ m\in M\}$	k	$\lvert\mathrm{rad}(K)\rvert$	$\lvert K\rvert$
1	$M=\{1\}$	$k\geq 0$	1	1
2	$M=\{1,n/2\}$	$k\geq 2$	2	2
3	$M=\{1,-1\}$	$k\geq 3$	1	2
4	$M=\{1,1+n/2,-1,-1+n/2\}$	$k\geq 4$	2	4
5	$M=\{1,-1+n/2\}$	$k\geq 3$	1	2
6	$M=\{1,1+n/2,-1+n/4,-1+3n/4\}$	$k\geq 4$	2	4

Table 1:

where the groups $A_{1,p}$ and $A_{2,p}$ are defined as follows. If p is odd, then $A_{1,p}$ is the subgroup of $\mathrm{Aut}(G_p)$ of order $p-1$ whereas $A_{2,p}=\{\sigma_m:\ m\equiv 1\,(\mathrm{mod}\,p)\}$. If $p=2$, then $A_{1,p}=\{\sigma_1,\sigma_{-1}\}$ and $A_{2,p}=\{\sigma_m:\ m\equiv 1\,(\mathrm{mod}\,4)\}$.

Let $K\leq\mathrm{Aut}(G)$. If g is a generator of G, then obviously the radical of the set $\{g^\sigma:\ \sigma\in K\}$ does not depend on the choice of g. We call this subgroup of G the *radical* of K and denote it by $\mathrm{rad}(K)$. The following statement in fact characterizes those K for which $|\,\mathrm{rad}(K)|\leq 2$ assuming that G is a p-group.

Lemma 5.1 *Let G be a cyclic p-group of order p^k and $K\leq\mathrm{Aut}(G)$. Then*

(1) *if p is odd, then $|\,\mathrm{rad}(K)|=1$ iff $K\leq A_{1,p}$,*

(2) *if $p=2$, then $|\,\mathrm{rad}(K)|\leq 2$ iff K belongs to one of the six families as listed in Table 1.*

Proof. Let p be odd. Then obviously $K\cap A_{2,p}=\{\sigma_m:\ m\equiv 1\,(\mathrm{mod}\,p^r)\}$ for a uniquely determined positive integer $r\leq k$. So $\mathrm{rad}(K)$ is the subgroup of G of index p^r. Thus $|\,\mathrm{rad}(K)|=1$ iff $K\cap A_{2,p}=\{1\}$. This proves statement (1) due to (27). If $p=2$, then by (27) we have $|K\cap A_{2,p}|\geq 4$ (and hence $|\,\mathrm{rad}(K)|\geq 4$) whenever $|K|\geq 8$. So $|\,\mathrm{rad}(K)|\leq 2$ implies that $|K|\leq 4$. Now statement (2) follows by a straightforward computation.∎

We complete the subsection by citing one more fact about the automorphism groups of cyclic groups. Let H be a subgroup of a cyclic group G. Then the natural homomorphisms

$$\pi_H:\mathrm{Aut}(G)\to\mathrm{Aut}(H),\quad \pi_{G/H}:\mathrm{Aut}(G)\to\mathrm{Aut}(G/H) \tag{28}$$

are surjections.

5.2. To describe the structure of S-rings over a finite cyclic group we need the following definition.

Definition 5.2 *Let $\mathcal{A}$ be an S-ring over a group G and let L,U be subgroups of G. We say that $\mathcal{A}$ satisfies the U/L-condition if the following three conditions hold:*

(1) *$L\leq U$ and L is normal in G,*

(2) *$L,U\in\mathcal{H}(\mathcal{A})$,*

(3) $L \le \mathrm{rad}(X)$ *for all* $X \in \mathcal{S}(\mathcal{A})$ *with* $X \subset G \setminus U$.

If, moreover, $L \ne \{1\}$ *and* $U \ne G$, *we say that* $\mathcal{A}$ *satisfies the* U/L*-condition nontrivially.*

An S-ring $\mathcal{A}$ satisfying the U/L-condition was called in [10, 11] the wedge product of the S-rings $\mathcal{A}_U$ and $\mathcal{A}_{G/L}$. It should be noted that in [8] we independently introduced the operation of taking the generalized wreath product of two S-rings which exactly produces all S-rings satisfying the U/L-condition.

The description of all S-rings over a cyclic group was obtained in [10, 11]. In the following two theorems we reformulate these results in the form convenient for us. Below an S-ring $\mathcal{A}$ over G is called *dense* if the set $\mathcal{H}(\mathcal{A})$ contains all subgroups of G. Obviously, any orbit S-ring is dense.

Theorem 5.3 *Let* $\mathcal{A}$ *be an S-ring over a finite cyclic group* G. *Suppose that* $\mathcal{A}$ *is not dense. Then at least one of the following two statements holds:*

(1) $\mathcal{A}$ *nontrivially satisfies the* U/L*-condition for some subgroups* L, U *of* G *such that the product of* $|L|$ *and* $|G/U|$ *is not a prime square,*

(2) $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$ *where* $\mathcal{A}_1$ *is the S-ring of rank 2 over a subgroup of* G *of composite order.*

Proof. First we observe that in the context of the theorem statement (2) can be replaced by the following one: either $\mathrm{rk}(\mathcal{A}) = 2$ or $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$ with $\mathcal{A}_1 \ne \mathcal{A}$ and $\mathcal{A}_2 \ne \mathcal{A}$. Indeed, if $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$, then $\mathcal{A}_1 = \mathcal{A}_{G_1}$, $\mathcal{A}_2 = \mathcal{A}_{G_2}$ for some subgroups $G_1, G_2 \in \mathcal{H}(\mathcal{A})$ such that $G = G_1 \times G_2$. Since $\mathcal{A}$ is not dense, at least one of the S-rings $\mathcal{A}_1$, $\mathcal{A}_2$, say $\mathcal{A}_1$, is not dense and so by induction we can assume that for $\mathcal{A}_1$ statement (1) or statement (2) holds. In the latter case we are done. In the former case $\mathcal{A}_1$ nontrivially satisfies the U_1/L_1-condition for some subgroups L_1, U_1 of G_1 such that the product of $|L_1|$ and $|G_1/U_1|$ is not a prime square. Then obviously $\mathcal{A}$ nontrivially satisfies the U/L-condition with $U = U_1 \times G_2$ and $L = L_1$. Since $|G/U| = |G_1/U_1|$, our claim is proved.

We will deduce the theorem from the results of paper [11] the numeration of the statements of which we use below. Without loss of generality we assume that $\mathrm{rk}(\mathcal{A}) > 2$. Suppose that some Sylow subgroup of G does not belong to $\mathcal{H}(\mathcal{A})$. Then one can see that the hypothesis of Corollary 4.3 or Theorem 4.5 is satisfied. In the former case by Corollary 4.3 either $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$ where $\mathcal{A}_1 \ne \mathcal{A}$, $\mathcal{A}_2 \ne \mathcal{A}$, or $\mathcal{A}$ nontrivially satisfies the U/L-condition with composite $|G/U|$, and we are done. In the latter case by Theorem 4.5 the S-ring $\mathcal{A}$ nontrivially satisfies the U/L-condition with $|G/U| = p$ where p is a prime. According to Proposition 4.4 the subgroup L can be chosen in such a way that $|L|$ is not a power of p, and we are also done. Let now $\mathcal{H}(\mathcal{A})$ contains all Sylow subgroups of G. Then by Theorem 5.2 either $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$ where $\mathcal{A}_1 \ne \mathcal{A}$, $\mathcal{A}_2 \ne \mathcal{A}$, or $\mathcal{A}$ nontrivially satisfies the U/L-condition with $|L|$ or $|G/U|$ divided by p^2 for some prime p. Thus the theorem is proved.∎

To formulate the second theorem we need one more definition. Let $\mathcal{A}$ be an S-ring over an Abelian group G. Then by the well-known Schur theorem (see [19, Theorem 23.9]) we have

$$\mathrm{Aut}(G) \le \mathrm{Iso}(\mathcal{A}) \tag{29}$$

Suppose now that G is cyclic. Then the group $\mathrm{Aut}(G)$ acts transitively on the set of generators of G. So the group $\mathrm{rad}(X)$ does not depend on the choice of $X \in \mathcal{S}(\mathcal{A})$ such that $\langle X \rangle = G$. We call it the *radical* of $\mathcal{A}$ and denote by $\mathrm{rad}(\mathcal{A})$. From Definition 5.2 it follows that if $\mathcal{A}$ satisfies the U/L-condition, then $\mathrm{rad}(\mathcal{A}) \geq L$. It is easy to see that $\mathrm{rad}(\mathcal{A}) = \mathrm{rad}(K)$ whenever $\mathcal{A} = \mathcal{O}(K, G)$ for some $K \leq \mathrm{Aut}(G)$.

Theorem 5.4 *Let $\mathcal{A}$ be a dense S-ring over a finite cyclic group G. Then exactly one of the following two statements holds:*

(1) $|\,\mathrm{rad}(\mathcal{A})| \geq 2$ *and $\mathcal{A}$ satisfies the U/L-condition for some subgroups L, U of G such that $|L| = |G/U| = p$ where p is the maximal prime divisor of* $|\,\mathrm{rad}(\mathcal{A})|$,

(2) $|\,\mathrm{rad}(\mathcal{A})| = 1$ *and $\mathcal{A}$ is an orbit S-ring.*

Proof. Follows from [10, Theorems 3.4, 3.6].■

5.3. In this subsection we give in the terms of the U/L-condition a powerful necessary condition for an S-ring over a cyclic group to be normal.

Let G (resp. G') be a group and L, U (resp. L', U') subgroups of G (resp. G') such that $L \leq U$ and L is normal in G (resp. $L' \leq U'$ and L' is normal in G'). Let next $f_1 : U \to U'$ and $f_2 : G/L \to G'/L'$ be group isomorphisms coinciding on U/L. For each left coset T of G by U let us choose a bijection $f_T : T \to T'$ compatible with f_2 such that $f_T(ux) = f_1(u)f_T(x)$ for all $u \in U$, $x \in T$, where T' is the image of T with respect to the bijection from the set of all left cosets of G by U onto the set of all left cosets of G' by U' induced by f_2. Assume that $f_U = f_1$. Then the mapping

$$f : G \to G', \quad x \mapsto f_T(x)$$

where $T = T(x)$ is the coset containing x, is a bijection. Denote by $\mathcal{F} = \mathcal{F}(f_1, f_2)$ the set of all such f. Then it is easy to see that $|\mathcal{F}| = |L|^{[G:U]-1}$.

Lemma 5.5 *Let $\mathcal{A}$ (resp. $\mathcal{A}'$) be an S-ring over a group G (resp. G') satisfying the U/L-condition (resp. the U'/L'-condition) and $f_1 : \mathcal{A}_U \to \mathcal{A}'_{U'}$, $f_2 : \mathcal{A}_{G/L} \to \mathcal{A}'_{G'/L'}$ be Cayley isomorphisms. Then $\mathcal{F} \subset \mathrm{Iso}(\mathcal{A}, \mathcal{A}')$ and $f_U = f_1$, $f_{G/L} = f_2$ for all $f \in \mathcal{F}$.*

Proof. Let $f \in \mathcal{F}$. Then from the definition of $\mathcal{F}$ it immediately follows that $f(xy) = f(x)f(y)$ for $x \in U$, $y \in G$, and $f(LxLy) = f(Lx)f(Ly)$ for all x, y. The first of these statements shows that equality (17) holds for all $x \in U$ and $y \in G$. If $x \notin U$, then by the assumption on $\mathcal{A}$ and $\mathcal{A}'$ the sets $[x]$ and $[f(x)]$ are unions of cosets by L and L' respectively (see Definition 5.2). So the second statement shows that equality (17) holds for all $x \notin U$ and $y \in G$. Thus $f \in \mathrm{Iso}(\mathcal{A}, \mathcal{A}')$ by Lemma 4.3. Obviously, $f_U = f_1$ and $f_{G/L} = f_2$.■

Let us apply Lemma 5.5 for studying normal S-rings over a cyclic group.

Theorem 5.6 *Let $\mathcal{A}$ be a normal S-ring over a cyclic group G. Suppose that $\mathcal{A}$ nontrivially satisfies the U/L-condition for some subgroups L and U of G. Then $|L| = |G/U| = 2$.*

Proof. From Lemma 5.5 with $\mathcal{A} = \mathcal{A}'$ and f_1, f_2 being the identity maps it follows that for any $l \in L \setminus \{1\}$ the group $\mathrm{Aut}(\mathcal{A})$ contains an automorphism f identical on U and taking x to lx if $x \in G \setminus U$. Since $\mathcal{A}$ is normal, $f \in \mathrm{Aut}(G)$ by Theorem 4.7. So for $x \in G \setminus U$ we obtain that

$$x^2l^2 = f(x)^2 = f(x^2) = \begin{cases} x^2l, & \text{if } x^2 \notin U, \\ x^2, & \text{otherwise.} \end{cases} \tag{30}$$

On the other hand, if $|G/U| \neq 2$, then the cyclicity of G implies that there exists $x \in G$ with $x^2 \notin U$. Thus $l = 1$ by (30), which contradicts the choice of l. Similarly, if $|L| \neq 2$, then there exists $l \in L$ such that $l^2 \neq 1$, which contradicts (30).∎

As a byproduct of the results of this subsection and the previous section we have the following statement.

Theorem 5.7 *Let $\mathcal{A}$ be an S-ring over a cyclic group G. Then* $\mathrm{Aut}(\mathcal{A}) = \{1\}$ *iff* $\mathcal{A} = \mathbb{Z}[G]$.

Proof. The sufficiency is obvious. Let $\mathrm{Aut}(\mathcal{A}) = \{1\}$. Then Lemma 5.5 shows that $\mathcal{A}$ cannot nontrivially satisfy any U/L-condition. Thus by Theorem 5.3 and Theorem 5.4 either $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$ where $\mathcal{A}_1$ is an S-ring of rank 2 over a group of composite order or $\mathcal{A} = \mathcal{O}(K, G)$ where $K \leq \mathrm{Aut}(G)$. However, in the first case obviously $|\mathrm{Aut}(\mathcal{A})| \geq |\mathrm{Aut}(\mathcal{A}_1)| > 1$. In the second case $\mathrm{Aut}(\mathcal{A}) \geq K$ and so $|K| = 1$. This means that $\mathcal{A} = \mathbb{Z}[G]$.∎

6 Criterion of normality and its corollaries

6.1. Let us formulate the main result of the section to be proved in Section 7. To do this, given a cyclic group G and $K \leq \mathrm{Aut}(G)$ set

$$\mathcal{P}^*(K) = \{p \in \mathcal{P}(G) : \ |G_p| = p, \ \mathrm{Aut}(G_p) \leq K\}.$$

Clearly, the condition $\mathrm{Aut}(G_p) \leq K$ means that $K = \mathrm{Aut}(G_p) \times \pi_{G_{p'}}(K)$ where $G_{p'} = \prod_{q \in \mathcal{P}(G) \setminus \{p\}} G_q$ (see (28)).

Theorem 6.1 *Let W be a Cayley ring over a cyclic group G and $\mathcal{A}$ the corresponding S-ring. Then the following statements are equivalent:*

1. *W is a normal Cayley ring (equivalently, $\mathcal{A}$ is a normal S-ring),*
2. *$W_v = \mathcal{Z}(K, G)$ for some $K \leq \mathrm{Aut}(G)$, where $v = 1_G$,*
3. *$\mathcal{A} = \mathcal{O}(K, G)$ for some $K \leq \mathrm{Aut}(G)$ such that $|\mathrm{rad}(K)| \leq 2$ and $\mathcal{P}^*(K) \subset \{2, 3\}$.*

Let W be a normal Cayley ring over a cyclic group G. Then by Theorem 6.1 we have $W_v = \mathcal{Z}(K, G)$ for some $K \leq \mathrm{Aut}(G)$. Since any generator of G is obviously a regular point of $\mathcal{Z}(K, G)$, the ring W_v is 1-regular (see Section 9). By the transitivity of $\mathrm{Aut}(W)$ this implies that any one-point extension of W is 1-regular. Thus by Lemma 9.2 any extension of W with respect to $v_1, \ldots, v_s \in G$, $s \geq 1$, is 1-regular and we come to the following statement.

Corollary 6.2 *Any s-points extension of a normal Cayley ring over a cyclic group is 1-regular for $s \geq 1$.*$\blacksquare$

From Theorem 6.1 ((1) $\Rightarrow$ (3)), it follows that a normal Cayley ring over a cyclic group is Schurian. Thus Corollary 4.6 implies the following statement.

Corollary 6.3 *Let G be a cyclic group. Then the mappings*

$$\Gamma \mapsto \mathcal{Z}(\Gamma), \quad W \mapsto \mathrm{Aut}(W)$$

define a one-to-one correspondence between the 2-closed subgroups of the holomorph of G containing G and the normal Cayley rings over G.$\blacksquare$

Since obviously an S-ring with trivial radical cannot nontrivially satisfy any U/L-condition, Theorem 5.3, Theorem 5.4 and Theorem 6.1 ((3) $\Rightarrow$ (1)) imply due to (12) the following statement.

Corollary 6.4 *Any S-ring with trivial radical over a cyclic group equals the tensor product of a normal S-ring with trivial radical and S-rings of rank 2.*$\blacksquare$

From Theorem 6.1 ((1) $\Rightarrow$ (3)), it follows that the order of the radical of a normal S-ring over a cyclic group is at most 2. If it equals 2 the structure of the corresponding S-rings is described as follows.

Corollary 6.5 *Let $\mathcal{A}$ be a normal S-ring over a cyclic group G. Suppose that $|\mathrm{rad}(\mathcal{A})| = 2$. Then $\mathcal{A}$ satisfies the U/L-condition where L and U are subgroups of G such that $|L| = |G/U| = 2$ (in particular, 4 divides $|G|$). Moreover, $\mathcal{A}_U$ and $\mathcal{A}_{G/L}$ are Cayley isomorphic normal S-rings with trivial radical.*

Proof. By Theorem 6.1 $\mathcal{A}$ is an orbit S-ring and hence dense. Since $|\mathrm{rad}(\mathcal{A})| = 2$, Theorem 5.4 implies that $\mathcal{A}$ satisfies the U/L-condition with $|L| = |G/U| = 2$. Let $\mathcal{A} = \mathcal{O}(K, G)$ where $K \leq \mathrm{Aut}(G)$. Then $\mathcal{A}_U = \mathcal{O}(\pi_U(K), U)$ and $\mathcal{A}_{G/L} = \mathcal{O}(\pi_{G/L}(K), G/L)$ (see (28)). The isomorphism $G/L \to U$ taking Lg to g^2 where g is a generator of G, induces the isomorphism $\mathrm{Aut}(G/L) \to \mathrm{Aut}(U)$ taking $\pi_{G/L}(K)$ to $\pi_U(K)$. So it is a Cayley isomorphism from $\mathcal{A}_{G/L}$ to $\mathcal{A}_U$. To complete the proof it suffices to verify that $\mathcal{A}_{G/L}$ is a normal S-ring with trivial radical. However, since $\mathrm{rad}(\mathcal{A}) = L$, we have $\mathrm{rad}(\mathcal{A}_{G/L}) = \{1\}$. Next, if $\pi_{G/L}(K) = \mathrm{Aut}((G/L)_p) \times K'$ where p is an odd prime and $K' \leq \mathrm{Aut}((G/L)_{p'})$, then

$$K = \pi_{G/L}^{-1}(\pi_{G/L}(K)) = \pi_{G/L}^{-1}(\mathrm{Aut}((G/L)_p) \times K') = \mathrm{Aut}(G_p) \times \pi_{G/L}^{-1}(K')$$

and $|G_p| = |(G/L)_p|$. So $\mathcal{P}^*(\pi_{G/L}(K)) \setminus \{2\} \subset \mathcal{P}^*(K)$. Thus the normality of $\mathcal{A}_{G/L}$ follows from the normality of $\mathcal{A}$ by Theorem 6.1 ((1) $\Leftrightarrow$ (3)).$\blacksquare$

6.2. It was proved in [8] that not every weak isomorphism of S-rings over a cyclic group is induced by a strong isomorphism. As the following theorem shows the situation is different for normal S-rings. Moreover, in this case statement (2) of this theorem can be regarded as the refinement of inclusion (29). Since weakly isomorphic S-rings over a cyclic group are Cayley isomorphic (see [14]), we can confine ourselves to isomorphisms of an S-ring to itself.

Theorem 6.6 *Let $\mathcal{A}$ be a normal S-ring over a cyclic group G. Then*

(1) *any weak isomorphism of $\mathcal{A}$ is induced by a strong isomorphism,*

(2) $[\mathrm{Iso}(\mathcal{A}) : \mathrm{Aut}(G)] \le 2$*; moreover,* $\mathrm{Iso}(\mathcal{A}) = \mathrm{Aut}(G)$ *iff either* $|\operatorname{rad}(\mathcal{A})| = 1$ *or* $|\operatorname{rad}(\mathcal{A})| = 2$ *and the order of the Sylow 2-subgroup of G equals 4.*

Proof. From Theorem 6.1 ((1) $\Leftrightarrow$ (3)) it follows that $\mathcal{A}$ is an orbit S-ring and $|\operatorname{rad}(\mathcal{A})| \le 2$. If $|\operatorname{rad}(\mathcal{A})| = 1$, then it suffices to prove the following statement.

Lemma 6.7 *In the notation and the assumptions of Theorem 6.6 let* $\operatorname{rad}(\mathcal{A}) = \{1\}$*. Then*

(1) *any weak isomorphism of $\mathcal{A}$ is induced by a Cayley isomorphism,*

(2) $\mathrm{Iso}(\mathcal{A}) = \mathrm{Aut}(G)$.

Proof. Let us fix a basic set X of $\mathcal{A}$ containing a generator of G. We will show that the smallest S-ring $\mathcal{A}'$ containing $\xi(X)$ coincides with $\mathcal{A}$. To do this we observe that $\operatorname{rad}(X) = \operatorname{rad}(\mathcal{A}) = \{1\}$. Since obviously $X \in \mathcal{S}(\mathcal{A}')$, we have $\operatorname{rad}(\mathcal{A}') = \operatorname{rad}(X) = \{1\}$. So $\mathcal{A}'$ does not nontrivially satisfy any U/L-condition. This implies by Theorem 5.3 that $\mathcal{A}'$ is dense. Indeed, otherwise for $\mathcal{A}'$ statement (2) of this theorem is true. Then X is not an orbit of any subgroup of $\mathrm{Aut}(G)$ and so $\mathcal{A}$ is not an orbit S-ring, which contradicts the normality of $\mathcal{A}$ by Theorem 6.1 ((1) $\Rightarrow$ (3)). Now by Theorem 5.4 the ring $\mathcal{A}'$ is an orbit one and hence coincides with $\mathcal{A}$.

To prove statement (1) let $\varphi \in \mathrm{Isow}(\mathcal{A})$. Since $\langle X \rangle = G$, by Lemma 2.1 and Theorem 4.2 we have $X^\varphi \in \mathcal{S}(\mathcal{A})$ and $\langle X^\varphi \rangle = G$. This and the fact that $\mathcal{A}$ is an orbit S-ring imply that X^φ contains a generator of G. So $X^\varphi = X^\sigma$ for some $\sigma \in \mathrm{Aut}(G)$. Thus φ coincides on $\mathcal{A}'$ with the weak isomorphism of $\mathcal{A}$ induced by σ. Since $\mathcal{A}' = \mathcal{A}$, statement (1) is proved. To prove statement (2) let $f \in \mathrm{Iso}(\mathcal{A})$. Then from statement (1) it follows that there exists $\sigma \in \mathrm{Aut}(G)$ such that $f\sigma^{-1} \in \mathrm{Aut}(\mathcal{A})$, and we are done by the normality of $\mathcal{A}$.$\blacksquare$

Let now $|\operatorname{rad}(\mathcal{A})| = 2$. Then by Corollary 6.5 there exist subgroups L and U of G for which all statements of this corollary hold. Let $\varphi \in \mathrm{Isow}(\mathcal{A})$. Then since $\mathcal{A}_U$ and $\mathcal{A}_{G/L}$ are normal S-rings with trivial radical, by statement (1) of Lemma 6.7 the weak isomorphisms φ_U and φ_G/L are induced by $\sigma_1 \in \mathrm{Aut}(U)$ and $\sigma_2 \in \mathrm{Aut}(G/L)$ respectively. Due to the surjectivity of the homomorphisms π_U and $\pi_{G/L}$ (see (28)), we assume without loss of generality that σ_1 and σ_2 coincide on U/L. Now by Lemma 5.5 one can find $f \in \mathrm{Iso}(\mathcal{A})$ such that $f_U = \sigma_1$ and $f_{G/L} = \sigma_2$. Since obviously f induces φ, statement (1) is completely proved. To prove statement (2) we observe first that 4 divides n where $n = |G|$. Let $f \in \mathrm{Iso}(\mathcal{A})$. By statement (2) of Lemma 6.7 we have $f_U \in \mathrm{Aut}(U)$ and $f_{G/L} \in \mathrm{Aut}(G/L)$. So $f_{U/L} \in \mathrm{Aut}(U/L)$ where $f_{U/L} = (f_U)_{U/L} = (f_{G/L})_{U/L}$. From the surjectivity of mappings (28) it follows that there exists $\sigma \in \mathrm{Aut}(G)$ such that $\sigma_{U/L} = f_{U/L}$. Thus after replacing f by $f\sigma^{-1}$ we can assume without loss of generality that

$$f_{U/L} = \mathrm{id}_{U/L}, \quad f_U \in \mathrm{Aut}(U), \quad f_{G/L} \in \mathrm{Aut}(G/L). \tag{31}$$

If $n/4$ is odd, then this implies that $f_U = \mathrm{id}_U$ and $f_{G/L} = \mathrm{id}_{G/L}$. So $f \in \mathrm{Aut}(\mathcal{A})$ and hence $f \in \mathrm{Aut}(G)$ by the normality of $\mathcal{A}$ (in fact, $f \in \Gamma_0$ where $\Gamma_0 = \{\sigma_{1+in/2} : i = 0, 1\}$). Suppose that 8 divides n. Then (31) shows that $f_U \in \Gamma_1$ and $f_{G/L} \in \Gamma_2$ where $\Gamma_1 = \{\sigma_{1+in/4,U} :\ i = 0, 1\}$, $\Gamma_2 = \{\sigma_{1+in/4,G/L} :\ i = 0, 1\}$. Denote by Γ the group of all $f \in \mathrm{Iso}(\mathcal{A})$ satisfying the last condition. To complete the proof it suffices to verify that $[\Gamma : \Gamma \cap \mathrm{Aut}(G)] = 2$. To do this, using once more the normality of $\mathcal{A}$ we obtain that

$$\Gamma = \{f_{\gamma_1,\gamma_2}\gamma_0 :\ \gamma_j \in \Gamma_j,\ j = 0, 1, 2\}$$

where f_{γ_1,γ_2} is a fixed element of $\mathrm{Iso}(\mathcal{A})$ such that $(f_{\gamma_1,\gamma_2})_U = \gamma_1$ and $(f_{\gamma_1,\gamma_2})_{G/L} = \gamma_2$ (we made use of Lemma 5.5 and the fact that $(\gamma_1)_{U/L} = (\gamma_2)_{U/L} = \mathrm{id}_{U/L}$ for all $\gamma_1 \in \Gamma_1$ and $\gamma_2 \in \Gamma_2$). It is easy to see that $\Gamma_0 \le \mathrm{Aut}(G)$ and that $f_{\gamma_1,\gamma_2} \in \mathrm{Aut}(G)$ iff $\gamma_1 = \sigma_{1+in/4,U}$, $\gamma_2 = \sigma_{1+in/4,G/L}$, $i = 0, 1$. Thus $[\Gamma : \Gamma \cap \mathrm{Aut}(G)] = 2$ and we are done.■

7 Proof of Theorem 6.1

We will show that (2) $\Rightarrow$ (1) $\Rightarrow$ (3) $\Rightarrow$ (2). To prove the implication (2) $\Rightarrow$ (1) suppose that $W_v = \mathcal{Z}(K, G)$ where $K \le \mathrm{Aut}(G)$. The stabilizer of any generator of G is obviously trivial. So K is a 2-closed subgroup of $\mathrm{Sym}(G)$ by [20, Theorem 5.12]. This implies that $\mathrm{Aut}(W_v) = \mathrm{Aut}(\mathcal{Z}(K, G)) = K$. Thus $\mathrm{Aut}(\mathcal{A}) = K$ due to (18) and $\mathcal{A}$ is normal by Theorem 4.7.

Let us prove the implication (1) $\Rightarrow$ (3). We need the following lemma.

Lemma 7.1 *Any normal S-ring over a cyclic group is an orbit one with radical of order at most* 2.

Proof. Let $\mathcal{A}$ be a normal S-ring over a cyclic group G. Then it is dense. (Indeed, otherwise by Theorem 5.3 at least one of its two statements holds. However, $\mathcal{A}$ cannot be normal in the first case by Theorem 5.6 whereas in the second one by Theorem 4.7.) If $\mathrm{rad}(\mathcal{A}) = \{1\}$ then $\mathcal{A}$ cannot nontrivially satisfy any U/L-condition. So $\mathcal{A}$ is an orbit S-ring by Theorem 5.4 and we are done. Let $\mathrm{rad}(\mathcal{A}) \ne \{1\}$. Then by Theorem 5.4 $\mathcal{A}$ satisfies the U/L-condition for some subgroups L, U of G such that $|L| = |G/U| = p$ where p is the maximal prime divisor of $|\,\mathrm{rad}(\mathcal{A})|$. So by Theorem 5.6 we conclude that $p = 2$ and hence $\mathrm{rad}(\mathcal{A})$ is a nontrivial 2-group.

Let us prove that the S-rings $\mathcal{A}_{G/L}$ and $\mathcal{A}_U$ are orbit S-rings with trivial radical. Since $\mathcal{A}$ is dense, these S-rings are also dense. So by Theorem 5.4 it only suffices to prove that each of them has trivial radical. Suppose $\mathrm{rad}(\mathcal{A}_{G'}) \ne \{1\}$ where $G' = G/L$. Then since $\mathrm{rad}(\mathcal{A})$ is a nontrivial 2-group, so is $\mathrm{rad}(\mathcal{A}_{G'})$. By Theorem 5.4 this implies that $\mathcal{A}_{G'}$ satisfies the U'/L'-condition with $|L'| = |G'/U'| = 2$. So $\mathcal{A}$ satisfies the $U/\pi^{-1}(L')$-condition where $\pi : G \to G'$ is the natural surjection. Since $|\pi^{-1}(L')| = 4$, this contradicts the normality of $\mathcal{A}$ by Theorem 5.6. Thus $\mathrm{rad}(\mathcal{A}_{G'}) = \{1\}$. To prove our claim for the S-ring $\mathcal{A}_U$ it suffices to verify that $\mathrm{rad}(\mathcal{A}_U$ is a 2-group. Indeed, if in this case $\mathrm{rad}(\mathcal{A}_U) \ne \{1\}$ then by Theorem 5.4 the S-ring $\mathcal{A}_U$ satisfies the U_1/L-condition with $|U/U_1| = 2$. So $\mathcal{A}$ also satisfies the U_1/L-condition. Since $|G/U_1| = 4$, this contradicts the normality of $\mathcal{A}$ by Theorem 5.6. Let us now prove that $\mathrm{rad}(\mathcal{A}_U)$ is a 2-group. To do this let X be a basic set of $\mathcal{A}$ containing a generator of G. Then by (13) the set $X' = \pi(X)$ is a basic set of $\mathcal{A}_{G'}$ containing a generator of G'. Since the ring $\mathcal{A}_{G'}$ is an orbit one, we conclude that the set $Y' = \{(x')^2 :\ x' \in X'\}$ belongs to $\mathcal{S}(\mathcal{A}_{G'})$. This implies that $\pi^{-1}(Y') = Y \cup Yh$ where Y is a basic set of $\mathcal{A}_U$ containing a generator of U and h is the element of G of order 2. Since obviously

$\mathrm{rad}(Y) = \mathrm{rad}(Yh)$, we obtain that $\mathrm{rad}(Y) \le \mathrm{rad}(\pi^{-1}(Y')$. Thus it suffices to prove that $\mathrm{rad}(Y')$ is a 2-group. However, if $a'Y' = Y'$ for some element $a' \in G'$ of odd order, then obviously $b'X' \subset Z'$ where $Z' = X' \cup h'X'$, b' is the element of G' such that $(b')^2 = a'$ and h' is the element of G' of order 2. Then $H' = \langle b' \rangle$ is a subgroup of $\mathrm{rad}(Z')$. So Z' is a disjoint union of cosets by H'. Since X' and $h'X'$ are orbits of the same subgroup of $\mathrm{Aut}(G')$ and $\sigma_{1+n'/2}(X') = h'X'$ where $n' = |G'$, the cardinality of nonempty intersections $g'H' \cap X'$ and $g'H' \cap h'X'$ do not depend on the choice of $g' \in G'$ and these numbers are equal. This implies due to the oddness of $|H'|$ that X' is a union of cosets by H', i.e. $H' \le \mathrm{rad}(X')$. Using the fact that $\mathrm{rad}(X') = \{1\}$, we conclude that $H' = \{1\}$ and hence $a' = b' = 1$.

As it was proved above $\mathrm{rad}(\mathcal{A})$ is a nontrivial 2-group and $\mathrm{rad}(\mathcal{A}_{G/L}) = \{1\}$. So $|\,\mathrm{rad}(\mathcal{A})| = 2$. Now to complete the proof it suffices to verify that the S-ring $\mathcal{A}$ is Schurian (then due to the normality it is an orbit one). Since the S-rings $\mathcal{A}_{G/L}$ and $\mathcal{A}_U$ are orbit ones, we have $\mathcal{A}_U = \mathcal{O}(K_1, U)$ and $\mathcal{A}_{G/L} = \mathcal{O}(K_2, G/L)$ for some groups $K_1 \le \mathrm{Aut}(U)$ and $K_2 \le \mathrm{Aut}(G/L)$. Denote by Γ the group generated by the set $\bigcup_{f_1,f_2} \mathcal{F}(f_1, f_2)$ where the union is taken over all pairs $(f_1, f_2) \in K_1 \times K_2$ with $(f_1)_{U/L} = (f_2)_{U/L}$ (see Lemma 5.5). Since the homomorphisms π_U and $\pi_{G/L}$ are surjective (see (28)), Γ acts on U as K_1 and on G/L as K_2. Besides, it is easy to see that outside of U the orbits of the subgroup $\mathcal{F}(1,1)$ of Γ coincide with the cosets by L. Thus $\mathrm{Orb}(\Gamma, G) = \mathcal{S}(A)$ and hence $\mathcal{A}$ is Schurian.∎

Let $\mathcal{A}$ be a normal S-ring. Then it follows from Lemma 7.1 that $\mathcal{A} = \mathcal{O}(K, G)$ for some group $K \le \mathrm{Aut}(G)$ with $|\,\mathrm{rad}(K)| \le 2$. Let $p \in \mathcal{P}^*(K)$. Then $K = \mathrm{Aut}(G_p) \times \pi_{G_{p'}}(K)$. By formula (12) this implies that $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$ where $\mathcal{A}_1$ is the S-ring of rank 2 over G_p and $\mathcal{A}_2$ is an S-ring over $G_{p'}$. So $\mathrm{Aut}(\mathcal{A}) \ge \mathrm{Aut}(\mathcal{A}_1)$. Since $\mathrm{Aut}(\mathcal{A}_1)$ is isomorphic to the symmetric group of degree $p-1$ and $\mathrm{Aut}(\mathcal{A})$ is an Abelian group due to the normality of $\mathcal{A}$, we conclude that $p \le 3$. This proves that (1) $\Rightarrow$ (3).

Let us prove that (3) $\Rightarrow$ (2). The proof is based on two statements (Theorem 7.3 and Theorem 7.4). The first of them shows that this implication is in fact true proved in the prime power case, whereas the second one enables us to reduce the general case to it. Let $\mathcal{A} = \mathcal{O}(K, G)$ where $K \le \mathrm{Aut}(G)$. Then $W = \mathcal{Z}(G \cdot K, G)$. The lemma below reduces statement (2) to verifying the 1-regularity of a one-point extension of W.

Lemma 7.2 *$W_v = \mathcal{Z}(K, G)$ iff W_v is a 1-regular cellular ring.*

Proof. The necessity follows from Lemma 9.1 ($m = 1$, $\Gamma = K$). Conversely, let W_v be a 1-regular ring and let x be a regular point of it. Then obviously $\mathrm{Aut}(W_v)_x = \{1\}$. So $|\,\mathrm{Aut}(W_v)| = |X|$ where X is the orbit of $\mathrm{Aut}(W_v)$ containing x. From the Schurity of W it follows that X is the neighbourhood of the point v in a basis relation of W and so $X \in \mathrm{Orb}(K, G)$. This implies that $|X| \le |K|$. Therefore, $|\,\mathrm{Aut}(W_v)| \le |K|$. Since obviously $K \le \mathrm{Aut}(W_v)$, we conclude that $\mathrm{Aut}(W_v) = K$. On the other hand, from Theorem 9.3 it follows that the ring W_v is Schurian. Thus $W_v = \mathcal{Z}(\mathrm{Aut}(W_v)) = \mathcal{Z}(K, G)$.∎

Theorem 7.3 *Suppose G is a p-group G and the group K satisfies the following two conditions:*

(1) $|\,\mathrm{rad}(K)| = 1$ *for* $p \ge 3$, *and* $|\,\mathrm{rad}(K)| \le 2$ *for* $p = 2$,

(2) *if* $p \geq 5$ *and* $|G| = p$, *then* $K \neq \mathrm{Aut}(G)$.

Then the ring W_v *is 1-regular.*

Proof. Let g be a generator of G. We will show that g is a regular point of W_v. To do this let $|G| = n = p^k$.

Let $p = 2$. It follows from condition (1) and Lemma 5.1 that the group K belongs to one of the six families as listed in Table 1. Therefore $\mathcal{R}(W) = \{R_c : \ c \in \mathbb{Z}\}$ and $\mathrm{Cel}(W) = \{X_c : \ c \in \mathbb{Z}\}$ where

$$R_c = \{(g^a, g^b) : \ b - a = mc \,(\mathrm{mod}\, n), \ m \in M, \ a, b \in \mathbb{Z}\}, \quad X_c = \{g^a : \ a = mc \,(\mathrm{mod}\, n), \ m \in Mc\}$$

with M being as in Table 1. Now a straightforward computation shows that $|R_c(g) \cap X_d| \leq 1$ for all the groups K and $c, d \in \mathbb{Z}$ except for K belonging to families 4 or 6 and pairs (R_c, X_d) with $(c, d) \in \{(n/4, 1 + n/4), (-1 + n/4, n/4)\}$. Since any relation $R_c \cap (X_1 \times X_d)$ obviously belongs to $\mathcal{R}^*(W_v)$, we see that g is a regular point of W_v for K belonging to families $1, 2, 3, 5$. In the remaining cases

$$R_{n/4}(g) \cap X_{1+n/4} = \{g^{1+n/4}, g^{1+3n/4}\}, \quad R_{-1+n/4}(g) \cap X_{n/4} = \{g^{n/4}, g^{3n/4}\}.$$

However by the above $R_2(g) \cap X_3 = \{g^3\}$ and $R_{-2+n/4}(g^3) \cap X_{1+n/4} = \{g^{1+n/4}\}$. So $\{g^{1+n/4}\} = S(g)$ for some basis relation S of W_v. Similarly, $R_1(g) \cap X_2 = \{g^2\}$ and $R_{-2+n/4}(g^2) \cap X_{n/4} = \{g^{n/4}\}$, and so $\{g^{n/4}\} = T(g)$ for some basis relation T of W_v. Thus g is a regular point of W_v also for families 4 and 6.

Let $p > 2$. Then it follows from condition (1) and Lemma 5.1 that the cellular ring W is $3/2$-homogeneous, i.e. that any two nonreflexive basis relations of it have the same degree ($|K|$ in our case). Moreover, if $k \geq 2$, then the set $\mathcal{E}(W)$ contains a nontrivial equivalence (e.g. one with classes of cardinality p), i.e. W is an imprimitive cellular ring in sense of [3]. However, the restriction of a one-point extension of any imprimitive $3/2$-homogeneous cellular ring to the set of all its points different from the fixed one is semiregular (see [3, Lemma 5.13]). So any element of G different from v is a regular point of W_v for $k \geq 2$. If $k = 1$, we identify W with a normal cyclotomic ring over the field $\mathbb{F}$ with p elements using an isomorphism of G onto the additive group of $\mathbb{F}$. It follows from condition (2) that $\mathrm{rk}(W) \geq 3$ unless $p = 3$. If $p = 3$, then the required statement is obvious. Otherwise, according to statement (1) of Theorem 4.8 the cellular ring W^* defined there is a normal Cayley ring over the group $G = \mathbb{F}^\times$ and also $\mathrm{Aut}(W^*) = G$. So by Lemma 7.1 and equalities (18) the S-ring corresponding to W^* equals $\mathbb{Z}[G]$. Thus the ring W^* is regular. Since $(W_v)_G \geq W^*$, g is a regular point of W_v.■

For $p \in \mathcal{P}(G)$ and $R \subset G^2$ set

$$\mathrm{pr}_p(R) = \{(g_p, h_p) : \ (g, h) \in R\} \tag{32}$$

where g_p and h_p are p-components of g and h. Let $E_p = (G_p)^{\rho_G}$ and $E_{p'} = (G_{p'})^{\rho_G}$. If W is a cellular ring on G such that $E_{p'} \in \mathcal{E}(W)$, then any two of the sets $\mathrm{pr}_p(R)$, $R \in \mathcal{R}(W)$, are pairwise disjoint or coincide and, moreover, the set of all of them forms the standard basis of some cellular ring on G_p denoted here by $\mathrm{pr}_p(W)$. Indeed, by [2, Lemma 2.1] under the natural identification of G_p and $G/E_{p'}$ this set equals the standard basis of the factorring of W modulo $E_{p'}$ as defined in [2, Section 2.2].

Theorem 7.4 *Let $p \in \mathcal{P}(G)$, $K_p = K \cap \mathrm{Aut}(G_p)$ and $W_p = \mathcal{Z}(K_p, G_p)$. Then*

$$(W_p)_v = \mathcal{Z}(K_p, G_p) \ \Rightarrow \ \mathrm{pr}_p(W_v) = \mathcal{Z}(\pi_p(K), G_p).$$

where $\pi_p = \pi_{G_p}$.

Proof. Let g be a generator of $G_{p'}$. Suppose that $(W_p)_v = \mathcal{Z}(K_p, G_p)$. First we prove that

$$(W_v)_{G_p g} = \mathcal{Z}(K_p, G_p g). \tag{33}$$

To do this we observe that obviously $K_p \leq \mathrm{Aut}(W_v)$ and $(G_p g)^{K_p} = G_p g$. So $(W_v)_{G_p g} = \mathcal{Z}(K_p, G_p g)$. On the other hand from the assumption it follows that $\mathcal{Z}(K_p, G_p g) = \widetilde{W}_{\widetilde{v}}$ where $\widetilde{W} = \mathcal{Z}(G_p \cdot K_p, G_p g)$ and $\widetilde{v} = g$. Thus equality (33) is the consequence of the following inclusion

$$\widetilde{W}_{\widetilde{v}} \leq (W_v)_{G_p g}. \tag{34}$$

To prove (34) let $\widetilde{R} \in \mathcal{R}(\widetilde{W})$. Then $\widetilde{R}$ is a 2-orbit of the group $G_p \cdot K_p$ on the set $G_p g$. This implies that the set $\{(x_p, y) : \ (x, y) \in \widetilde{R}\}$ is an orbit of the same group on $G_p \times G_p g$. As it follows from equality

$$\{R \cap G_p \times G_p g : \ R \in \mathcal{R}(W), \ R \cap G_p \times G_p g \neq \emptyset\} = \mathrm{Orb}(G_p \cdot K_p, G_p \times G_p g) \tag{35}$$

proved below, this set is of the form $R \cap (G_p \times G_p g)$ for some $R \in \mathcal{R}(W)$. A straightforward computation shows that

$$A(\widetilde{R}) = (A(E_{p'}) I_{G_p} A(R))_{G_p g}. \tag{36}$$

Since obviously $G_p \in \mathrm{Cel}^*(W_v)$ and $E_{p'} \in \mathcal{E}(W)$, the matrix $A(E_{p'}) I_{G_p} A(R)$ belongs to W_v. So the matrix on the right-hand belongs to $(W_v)_{G_p g}$. Thus $\widetilde{R} \in \mathcal{R}((W_v)_{G_p g}$. To complete the proof of (34) let us prove (35). To do this it suffices to verify that the inclusion "$\subset$". Let $R \in \mathcal{R}(W)$ and $R \cap G_p \times G_p g \neq \emptyset$. Then $R = \{(x^\sigma, y^\sigma g^\sigma) : \ \sigma \in G \cdot K\}$ where $x, y \in G_p$. So repesenting $\sigma \in G \cdot \mathrm{Aut}(G)$ as $\sigma = \sigma_p \cdot \sigma_{p'}$ with $\sigma_p \in G_p \cdot \mathrm{Aut}(G_p)$ and $\sigma_{p'} \in G_{p'} \cdot \mathrm{Aut}(G_{p'})$, we have

$$R \cap (G_p \times G_p g) = \{(x^\sigma, y^\sigma g) : \ \sigma \in G \cdot K, \ 1^{\sigma_{p'}} = 1, \ g^{\sigma_{p'}} = g\} =$$

$$\{(x^\sigma, y^\sigma g) : \ \sigma \in G \cdot K, \ \sigma_{p'} = 1\} = \{(x^\sigma, y^\sigma g) : \ \sigma \in G_p \cdot K_p\}.$$

(We use the definition of K_p and the fact that the only element of the group $G_{p'}\,\mathrm{Aut}(G_{p'})$ leaving fixed both 1 and g equals its neutral element.) This proves the required inclusion.

Let us turn to the proof of the theorem. Set $W' = (W_v)^{\pi_p(K)}$. From (33) and the obvious inclusion $K_p \leq \pi_p(K)$ it follows that

$$W'_{G_p g} = ((W_v)^{\pi_p(K)})_{G_p g} = ((W_v)_{G_p g})^{\pi_p(K)} = \mathcal{Z}(K_p, G_p g)^{\pi_p(K)} = \mathcal{Z}(\pi_p(K), G_p g). \tag{37}$$

Let us show that

$$\mathrm{pr}_p(W') = \mathrm{pr}_p(W'_{G_p x}), \quad x \in G_{p'}. \tag{38}$$

Let $X \in \mathrm{Orb}(\pi_{p'}(K), G_{p'})$ where $\pi_{p'} = \pi_{G_{p'}}$. The set G_pX is the neighbourhood of the point v in the relation $\{(a,b) \in G^2 :\ a^{-1}b \in G_pX\}$ obviously belonging to $\mathcal{R}^*(W)$, and hence is a cellular set of W_v. Since $(G_pX)^{\pi_p(K)} = G_pX$, we conclude that $G_pX \in \mathrm{Cel}^*(W')$. So by the definition of the ring $\mathrm{pr}_p(W')$ we have

$$\mathrm{pr}_p(W') = \mathrm{pr}_p(W'_{G_pX}). \tag{39}$$

On the other hand, the group $\mathrm{Aut}(W')$ obviously contains K, $\pi_p(K)$ and hence $\pi_{p'}(K)$. So the set $\mathrm{pr}_p(W'_{G_px})$ does not depend on the choice of $x \in X$. Thus (38) follows from (39). Now equalities (37), (38) and the fact that the actions of K and $\pi_p(K)$ on G_p are equal imply that

$$\mathrm{pr}_p(W_v) = (W_v)_{G_p} = W'_{G_p} = \mathrm{pr}_p(W') = \mathrm{pr}_p(W'_{G_pg}) = \mathrm{pr}_p(\mathcal{Z}(\pi_p(K), G_pg)) = \mathcal{Z}(\pi_p(K), G_p),$$

which completes the proof of the theorem.∎

To complete the proof of the implication (3) $\Rightarrow$ (2) suppose that statement (3) of Theorem 6.1 holds. Let $p \in \mathcal{P}(G)$. Then the hypothesis of Theorem 7.3 is satisfied for the group K_p: condition (1) is the consequence of the obvious inclusion $\mathrm{rad}(K_p) \le \mathrm{rad}(K)$ whereas condition (2) follows from the definition of $\mathcal{P}^*(K)$. So this theorem and Lemma 7.2 imply that $(W_p)_v = \mathcal{Z}(K_p, G_p)$ and hence $\mathrm{pr}_p(W_v) = \mathcal{Z}(\pi_p(K), G_p)$ by Theorem 7.4. Thus

$$W_v \ge \bigotimes_{p\in\mathcal{P}(G)} \mathrm{pr}_p(W_v) = \bigotimes_{p\in\mathcal{P}(G)} \mathcal{Z}(\pi_p(K), G_p). \tag{40}$$

Each factor of the right-hand side of (40) is obviously a 1-regular ring. So the entire tensor product and the ring W_v are also 1-regular (see Lemma 9.2). By Lemma 7.2 this implies that $W_v = \mathcal{Z}(K, G)$. Theorem 6.1 is proved.∎

8 Schurity of the Cayley rings W^* and $\widehat{W}^*$

The main result of this section relates to the cellular rings W^* and $\widehat{W}^*$ defined in (22).

Theorem 8.1 *The Cayley rings W^* over G and $\widehat{W}^*$ over Γ are Schurian.*

Proof. By statement (1) of Theorem 4.8 the Cayley ring W^* is normal. Since the group G is cyclic, Theorem 6.1 ((1) $\Rightarrow$ (3)) implies that the S-ring over G corresponding to W^* is an orbit one and hence Schurian. Thus W^* is a Schurian ring.

Now, let $\widehat{\mathcal{A}}^*$ be the S-ring over Γ corresponding to the Cayley ring $\widehat{W}^*$. Since $E_G = G^{\rho_\Gamma}$ and $R_s = \{s\}^{\rho_\Gamma}$ (see Subsection 4.4), formula (23) and Theorem 4.2 imply that $G \in \mathcal{H}(\widehat{\mathcal{A}}^*)$ and $\{s\} \in \mathcal{S}(\widehat{\mathcal{A}}^*)$ (consequently, $sGs \in \mathcal{H}(\widehat{\mathcal{A}}^*)$). Moreover, from Theorem 4.8, statement (1) of Lemma 4.4 and Theorem 4.2, it follows that $\widehat{\mathcal{A}}^*_G$ is a normal S-ring over G. By Theorem 6.1 ((1) $\Rightarrow$ (3)) we have $\widehat{\mathcal{A}}^*_G = \mathcal{O}(K, G)$ for some $K \le \mathrm{Aut}(\mathbb{F})$. This implies that

$$\widehat{\mathcal{A}}^*_{sGs} = \xi(s)\widehat{\mathcal{A}}^*_G\xi(s) = \xi(s)\mathcal{O}(K, G)\xi(s) = \mathcal{O}(K, sGs).$$

Thus the Schurity of $\widehat{W}^*$ is the consequence of the following statement.

Theorem 8.2 *Let $\mathbb{F}$ be a finite field with $q = p^d$ elements, $\Gamma = A \cdot G$ a semidirect product of the additive group A of $\mathbb{F}$ by its multiplicative group G and s the element of Γ with A-component $1_{\mathbb{F}}$ and G-component $-1_{\mathbb{F}}$*[6] *Suppose that $\mathcal{A}$ is an S-ring over Γ such that*

(1) *$G, sGs \in \mathcal{H}(\mathcal{A})$,*

(2) *$\mathcal{A}_G = \mathcal{O}(K, G)$, $\mathcal{A}_{sGs} = \mathcal{O}(K, sGs)$ where $K \le \mathrm{Aut}(\mathbb{F})$.*

Then $\mathcal{A} = \mathcal{O}(K, \Gamma)$

Remark 8.3 *We observe that G and sGs are the stabilizers of the points $0_{\mathbb{F}}$ and $1_{\mathbb{F}}$ in the group Γ acting on $\mathbb{F}$ in accordance with (20).*

Proof. We deduce the theorem from the following three lemmas. Below we shall frequently use the fact that $\mathcal{A}_{\Gamma_0} = \mathbb{Z}[\Gamma_0]$ where Γ_0 is the subgroup of Γ consisting of all elements with both components belonging to the prime subfield $\mathbb{F}_0$ of $\mathbb{F}$. This follows from the equalities $\mathcal{A}_{G \cap \Gamma_0} = \mathbb{Z}[G \cap \Gamma_0]$ and $\mathcal{A}_{sGs \cap \Gamma_0} = \mathbb{Z}[sGs \cap \Gamma_0]$ (see condition (2)) after taking into account that Γ_0 is generated by $G \cap \Gamma_0$ and $sGs \cap \Gamma_0$.

Lemma 8.4 *The following statements are true:*

(1) *$A \in \mathcal{H}(\mathcal{A})$ and $\mathcal{A}_A = \mathcal{O}(K, A)$,*

(2) *if $X \in \mathcal{S}(\mathcal{A})$, then $\mathrm{pr}_G(X), \mathrm{pr}_A(X) \in \mathcal{S}(\mathcal{A})$.*

Proof. For $x \in \mathbb{F}$ let $\eta(x) = x \cdot 1 \in \Gamma$. First we prove that given a primitive element g of $\mathbb{F}$ we have

$$Y^{-1}X \cap tX^{-1}Yt = (\eta(g-1))^K \tag{41}$$

where $X = (0 \cdot g)^K$, $Y = ((1-g) \cdot g)^K$ and $t = 0 \cdot (-1)$. Let $\gamma = a \cdot h$ belong to the left-hand side of (41). Then a straightforward check shows that

$$a = (1 - g^{-1})^{\sigma} g^{\tau} = g^{\sigma'} - 1, \quad h = (g^{-1})^{\sigma} g^{\tau} = (g^{-1})^{\tau'} g^{\sigma'}$$

for some $\sigma, \tau, \sigma', \tau' \in K$. Since $K \le \mathrm{Aut}(\mathbb{F})$, the automorphisms $\sigma, \tau, \sigma', \tau'$ are determined by raising to the degrees $p^i, p^j, p^{i'}, p^{j'}$, respectively where $0 \le i, j, i', j' \le d-1$. So $h = g^{-p^i + p^j} = g^{-p^{j'} + p^{i'}}$. Once g is primitive, we obtain from here that $p^i + p^{i'} = p^j + p^{j'} \pmod{q-1}$. This implies that either $i = j, i' = j'$ or $i = j', j = i'$. In the first case, obviously, $h = 1$. In the second one we have $(1 - g^{-p^i})g^{p^j} = g^{p^j} - 1$ or, equivalently, $g^{p^i} = g^{p^j}$. So $i = j$ and hence $h = 1$ again. Thus, $\gamma \in (\eta(g-1))^K$. Since obviously the left-hand side of (41) is invariant with respect to K, (41) follows.

Let us prove that $A \in \mathcal{H}(\mathcal{A})$. To do this let g be a primitive element of $\mathbb{F}$. Then from (41) and the hypothesis of Theorem 8.2 it follows that $(\eta(g-1))^K \in \mathcal{S}^*(\mathcal{A})$. Since $(\eta(g))^K = (\eta(g-1))^K \cdot \eta(1)$

[6]Below we identify A and G with subgroups of Γ. Thus $A = \{x \cdot 1 : x \in \mathbb{F}\}$, $G = \{0 \cdot x : x \in \mathbb{F}^{\times}\}$ and $sGs = \{(1-x) \cdot x : x \in \mathbb{F}^{\times}\}$ where $0 = 0_{\mathbb{F}}$ and $1 = 1_{\mathbb{F}}$.

and $\{\eta(1)\} \in \mathcal{S}(\mathcal{A})$, we have $(\eta(g))^K \in \mathcal{S}^*(\mathcal{A})$. Suppose that g is a normal element of the field $\mathbb{F}$, i.e. that the additive group of $\mathbb{F}$ is generated by the elements g^σ, $\sigma \in \mathrm{Aut}(\mathbb{F})$ (as for the existence of a primitive normal element in a finite field see [12, Theorem 2.40]). Then the set $(\eta(g))^{\mathrm{Aut}(\mathbb{F})}$ generates the subgroup A of Γ. On the other hand, if $\mathrm{Aut}(\mathbb{F}) = \bigcup_\tau \tau K$, then $(\eta(g))^{\mathrm{Aut}(\mathbb{F})} = \bigcup_\tau (\eta(g^\tau))^K$. Since g^τ is a primitive element of $\mathbb{F}$ for all τ, from the above it follows that $(\eta(g))^{\mathrm{Aut}(\mathbb{F})} \in \mathcal{S}^*(\mathcal{A})$. Thus $A \in \mathcal{H}(\mathcal{A})$ which proves the first part of statement (1).

To prove statement (2) we observe first that $\mathrm{pr}_G(X) \in \mathcal{S}(\mathcal{A})$ for all $X \in \mathcal{S}(\mathcal{A})$ because $A, G \in \mathcal{H}(\mathcal{A})$ and $\mathcal{A}_{\Gamma/A} = \mathcal{A}_G$ (see (13)). Next, given $X \subset \Gamma$ we obviously have

$$\mathrm{pr}_A(X) = X\,\mathrm{pr}_G(X)^{-1} \cap A.$$

This implies that $\mathrm{pr}_A(X) \in \mathcal{S}^*(\mathcal{A})$ whenever $X \in \mathcal{S}^*(\mathcal{A})$. Moreover, if $\mathrm{pr}_A(X) = Y_1 \cup Y_2$ where Y_i is a proper subset of $\mathrm{pr}_A(X)$ belonging to $\mathcal{S}^*(\mathcal{A})$ $(i = 1,2)$, then $X = X_1 \cup X_2$ where $X_i = Y_i\,\mathrm{pr}_G(X) \cap X$ is a proper subset of X belonging to $\mathcal{S}^*(\mathcal{A})$ $(i = 1,2)$. Thus, if $X \in \mathcal{S}(\mathcal{A})$, then $\mathrm{pr}_A(X) \in \mathcal{S}(\mathcal{A})$, which completes the proof of statement (2). Since $\mathrm{pr}_A(sGs) = A \setminus \{1_\Gamma\}$, this statement implies that

$$\mathcal{S}(\mathcal{A}_A) = \{1_\Gamma\} \cup \{\mathrm{pr}_A(X) :\ X \in \mathcal{S}(\mathcal{A}_{sGs})\}.$$

Taking into account that $\mathcal{S}(\mathcal{A}_{sGs}) = \mathrm{Orb}(K, sGs)$, we conclude that $\mathcal{A}_A = \mathcal{O}(K, A)$, which proves the second part of statement (1). The lemma is proved.■

Lemma 8.5 *Let g be a primitive element of the field $\mathbb{F}$. Then*

(1) *given $a \in \mathbb{F}$, we have $[a \cdot g^\sigma] \in \mathrm{Orb}(K,\Gamma)$ for all $\sigma \in \mathrm{Aut}(\mathbb{F})$ whenever $[a \cdot g] \in \mathrm{Orb}(K,\Gamma)$,*

(2) *if g is a normal element of $\mathbb{F}$, then $[a \cdot g] \in \mathrm{Orb}(K,\Gamma)$ for all $a \in \mathbb{F}$.*

Proof. Let $a \in \mathbb{F}$ such that $[a \cdot g] \in \mathrm{Orb}(K,\Gamma)$. It suffices to prove that $[a \cdot g^p] \in \mathrm{Orb}(K,\Gamma)$. However, since $[0 \cdot g^i] \in \mathrm{Orb}(K,G)$ for all i, we have

$$[0 \cdot g^{p-1}][a \cdot g] \cap A[0 \cdot g^p] = \{a^\tau \cdot (g^{p-1})^\sigma g^\tau :\ (g^{p-1})^\sigma g^\tau \in (g^p)^K,\ \sigma,\tau \in K\}. \tag{42}$$

On the other hand, if $(g^{p-1})^\sigma g^\tau = g^p$ with $\sigma,\tau \in \mathrm{Aut}(\mathbb{F})$, then $g^{(p-1)p^i+p^j} = g^p$ for some $i,j \in \{0,1,\ldots,d-1\}$ and hence $(p-1)p^i+p^j = p \pmod{q-1}$. This implies that $i=j=0$. So $\sigma=\tau=\mathrm{id}_\mathbb{F}$. Thus the set on the right hand side of (42) coincides with $X = (a \cdot g^p)^K$. Since $A \in \mathcal{H}(\mathcal{A})$ (see statement (1) of Lemma 8.4), we conclude that the left hand side of (42) and hence the set X belong to $\mathcal{S}^*(\mathcal{A})$. Taking into account that $|X| = |\,\mathrm{pr}_G(X)| = |K|$ and $\mathrm{pr}_G(X) \in \mathrm{Orb}(K,G)$ we deduce from statement (2) of Lemma 8.4 that $X \in \mathcal{S}(\mathcal{A})$, which proves statement (1).

To prove statement (2) let g be a normal element of $\mathbb{F}$ and $a \in \mathbb{F}$. Then $a = \sum_{i=0}^{d-1} x_i g_i$ where $x_i \in \mathbb{F}_0$ and $g_i = g^{p^i}$ for all i. We shall prove by induction on $k = 0,1,\ldots,d$ that $[a_k \cdot g_k] \in \mathrm{Orb}(K,\Gamma)$ where $a_k = \sum_{i=0}^{k-1} x_i g_i$. Then the required statement is obtained for $k=d$. If $k=0$, then $a_k = 0$ and the induction base follows from the hypothesis of Theorem 8.2. Let $k > 0$ and $[a_{k-1} \cdot g_{k-1}] \in \mathrm{Orb}(K,\Gamma)$. Then by statement (1) we have $[a_{k-1} \cdot g_k] \in \mathrm{Orb}(K,\Gamma)$. Since obviously

$$[a_k \cdot g_k] = [x_k \cdot 1][a_{k-1} \cdot g_k]$$

we conclude that $[a_k \cdot g_k] \in \mathrm{Orb}(K,\Gamma)$.■

Below an element $x \in \mathbb{F}$ is called maximal if $|x^{\mathrm{Aut}(\mathbb{F})}| = |\,\mathrm{Aut}(\mathbb{F})|$.

Lemma 8.6 *If the equality $[\gamma] = \gamma^K$ is true for all $\gamma \in \Gamma$ such that the A-component of γ is a maximal element of $\mathbb{F}$, then it is true for all $\gamma \in \Gamma$.*

Proof. Let g be a primitive element of $\mathbb{F}$. We prove first that given a nonmaximal $a \in \mathbb{F}$ we have

$$a^\sigma g^\tau = a^{\sigma'} g^{\tau'} \quad \Leftrightarrow \quad a^\sigma = a^{\sigma'},\ g^\tau = g^{\tau'} \tag{43}$$

for all $\sigma, \tau, \sigma', \tau' \in \mathrm{Aut}(\mathbb{F})$. To do this we observe that $a \in \mathbb{F}_{p^{d_1}}$ for some divisor d_1 of d different from d and assume without loss of generality that $\tau' = \mathrm{id}_\mathbb{F}$. Then from the left hand side of the equivalence (43) it follows that $g^\tau/g \in \mathbb{F}_{p^{d_1}}$. This implies that $(g^\tau/g)^{p^{d_1}-1} = 1$. Since $g^\tau = g^{p^i}$ for some $i \in \{0, 1, \ldots, d-1\}$, we have $g^{(p^i-1)(p^{d_1}-1)} = 1$, whence it follows that $(p^i - 1)(p^{d_1} - 1)$ is divided by $p^d - 1$. On the other hand, since $p^d - 1 = p^{d-i}(p^i - 1) + p^{d-i} - 1$, we find that $\mathrm{GCD}(p^d - 1, p^i - 1) = \mathrm{GCD}(p^d - 1, p^{d-i} - 1)$. So $(p^{d-i} - 1)(p^{d_1} - 1)$ is divided by $p^d - 1$. Thus $(p^{i_0} - 1)(p^{d_1} - 1)$ is divided by $p^d - 1$ where $i_0 = \min(i, d - i)$. Besides, the former number is less than the latter one, because $i_0 \le d/2$ and $d_1 \le d/2$. This means that $i_0 = 0$, whence $i = 0$. So $g^\tau = g$ and hence $a^\sigma = a^{\sigma'}$. This proves (43).

Let $\gamma = a \cdot h$ be an element of Γ with nonmaximal a. Then from (43) it follows that ag is a maximal element of $\mathbb{F}$ and

$$(a \cdot h)^M (0 \cdot g)^K \cap (ag)^K \cdot G = (ag \cdot hg)^M, \quad (ag \cdot hg)^K (0 \cdot g^{-1})^K \cap a^K \cdot G = (a \cdot h)^K \tag{44}$$

where M is a union of cosets of K_0 in K with K_0 being the stabilizer of γ in K. Moreover, $(ag{\cdot}hg)^K \in \mathcal{S}(\mathcal{A})$ by the lemma hypothesis, $(0{\cdot}g)^K, (0{\cdot}g^{-1})^K \in \mathcal{S}(\mathcal{A})$ by the theorem hypothesis and $a^K{\cdot}G, (ag)^K{\cdot}G \in \mathcal{S}^*(\mathcal{A})$ by Lemma 8.4. So the second equality of (44) implies that $(a{\cdot}h)^K \in \mathcal{S}^*(\mathcal{A})$ whereas the first one shows that, moreover, $(a \cdot h)^K \in \mathcal{S}(\mathcal{A})$ because $(ag \cdot hg)^M$ is a proper subset of the basic set $(ag \cdot hg)^K$ for any proper subset M of K.■

To complete the proof of the theorem, by Lemma 8.6 it suffices to verify that $[a \cdot h] = (a \cdot h)^K$ where a is a maximal element of $\mathbb{F}$ and $h \in \mathbb{F}^\times$. To do this we will show that

$$\Big(\bigcap_{\sigma \in \mathrm{Aut}(\mathbb{F})} (0 \cdot h/g^\sigma)^K (a \cdot g^\sigma)^K\Big) \cap A \cdot h^K = (a \cdot h)^K \tag{45}$$

where g is a normal primitive element of $\mathbb{F}$. Then $(a \cdot h)^K \in \mathcal{S}^*(\mathcal{A})$ because $(0 \cdot h/g^\sigma)^K \in \mathcal{S}(\mathcal{A})$, $(a \cdot g^\sigma)^K \in \mathcal{S}(\mathcal{A})$ (see statement (2) of Lemma 8.5), $A \in \mathcal{S}^*(\mathcal{A})$ (see statement (1) of Lemma 8.4) and so $(a \cdot h)^K \in \mathcal{S}(\mathcal{A})$ by statement (2) of Lemma 8.4 due to the maximality of a.

Obviously, the right-hand side of (45) is contained in the left-hand side. Conversely, let γ belong to the latter. Then $\gamma = a^\tau \cdot h^\rho$ where $\tau, \rho \in K$, and assuming without loss of generality that $\rho = \mathrm{id}_\mathbb{F}$ we have

$$s = (s - p^i)p^{j_i} + p^{i+k} \pmod{q-1}, \quad i = 0, 1, \ldots, d-1, \tag{46}$$

for some integers j_i, where s and k are integers such that $h = g^s$ and $a^\tau = a^{p^k}$. (The fact that in the equalities (46) the integer k can be chosen not depending on i follows from the maximality of a.) It suffices to verify that

$$sp^k = s \pmod{q-1}. \tag{47}$$

Then $\gamma = a^\tau \cdot h = a^{p^k} \cdot g^s = a^{p^k} \cdot g^{sp^k} = (a \cdot h)^\tau$, and we are done.

Let us prove (47). Given an integer t, $0 \le t < q-1$, there exist uniquely determined integers $t_0, t_1, \ldots, t_{d-1}$ belonging to $\{0, 1, \ldots, p-1\}$ such that $t = \sum_{i=0}^{d-1} t_i p^i$. For an arbitrary integers t, i we set $t_i = t'_{i'}$ where t' (resp. i') is the smallest nonnegative integer such that $t' = t \,(\mathrm{mod}\, q-1)$ (resp. $i' = i \,(\mathrm{mod}\, q-1)$). From the definition, it follows that $t = \widetilde{t} \,(\mathrm{mod}\, q-1)$ iff $t_i = \widetilde{t}_i$ for all i belonging to a full system of representatives modulo d. It is easy to see that

$$(tp^j)_{i+j} = t_i \tag{48}$$

for all integers t, i, j. Thus to prove (47) it suffices to verify that $s_i = s_{i+k}$ for all $i \in \{0, 1, \ldots, d-1\}$. Let $i \in \{0, 1, \ldots, d-1\}$. Then from (46) it follows that $(s - p^i)p^{j_i} = s - p^{i+k} \,(\mathrm{mod}\, q-1)$. By (48) this implies that

$$c(l, s - p^i) = c(l, s - p^{i+k}), \quad l \in \{0, 1, \ldots, p-1\} \tag{49}$$

where $c(l, t) = |\{j \in \{0, 1, \ldots, d-1\} : \ t_j = l\}|$. Suppose that $s_i \ne s_{i+k}$. Then at least one of the integers s_i, s_{i+k}, say s_i, is different from 0. If $s_{i+k} \ne 0$, then $c(s_i - 1, s - p^i) = c(s_i - 1, s) - 1$, whereas $c(s_i - 1, s - p^{i+k}) = c(s_i - 1, s)$, which contradicts (49) for $l = s_i - 1$. If $s_{i+k} = 0$, then it is easy to see that

$$c(p-1, s - p^i) \le c(p-1, s) \le c(p-1, s - p^{i+k}).$$

From (49) for $l = p-1$, it follows that $c(p-1, s-p^i) = c(p-1, s)$ and $c(p-1, s-p^{i+k}) = c(p-1, s)$. The first equality implies that $s_i \ne p-1$, whereas the second one implies that $s_{i+k-1} = p-1$. So

$$c(s_i - 1, s - p^i) = c(s_i - 1, s) - 1, \quad c(s_i - 1, s - p^{i+k}) = c(s_i - 1, s),$$

which contradicts (49) for $l = s_i - 1$.∎

9 Appendix. 1-regular cellular rings

A cellular ring $W \le \mathrm{Mat}_V$ is called *1-regular* if there exists $v \in V$ such that $|R(v)| \le 1$ for all $R \in \mathcal{R}(W)$. Any such v is called a *regular* point of W. In this case $W_v = \mathrm{Mat}_V$. The set X of all regular points of W is obviously a cellular set of W such that W_X is a semiregular ring. It is easy to see that the centralizer ring of a permutation group is 1-regular iff the base number of the group is at most 1. More generally, the following statement is true.

Lemma 9.1 *Let $\Gamma \le \mathrm{Sym}(V)$ be a permutation group and m a positive integer. Then the following statements are equivalent:*

(1) $b(\Gamma) \le m$,

(2) $\mathcal{Z}(\Gamma_{v_1,\ldots,v_{m-1}})$ *is a 1-regular ring for some* $v_1, \ldots, v_{m-1} \in V$,

(3) $\mathcal{Z}_m(\Gamma)$ *is a 1-regular ring.*

Proof. The lemma is reduced to the case $m = 1$ by observing that $b(\Gamma) \le m$ iff $b(\Gamma_{v_1,\ldots,v_{m-1}}) \le 1$ for some $v_1, \ldots, v_{m-1} \in V$ as well as iff $b(\Gamma^{(m)}) \le 1$ where $\Gamma^{(m)}$ is the permutation group on V^m induced by the action of Γ on the m-tuples of points.∎

The lemma below immediately follows from the definition.

Lemma 9.2 *The class of all 1-regular rings is closed with respect to taking overrings and tensor products.*∎

Theorem 9.3 *Any 1-regular ring is separable and Schurian.*

Proof. Let W be a 1-regular ring. Denote by X the set of all regular points of W. Then $X \in \mathrm{Cel}^*(W)$ and W_X is a semiregular ring. According to [6, Theorem 4.4] every semiregular ring is separable and Schurian. So the theorem follows from the lemma below.

Lemma 9.4 *Let $W \le \mathrm{Mat}_V$ be a cellular ring, $\mathcal{R} = \mathcal{R}(W)$ and $X \in \mathrm{Cel}^*(W)$. Suppose that for every $Y \in \mathrm{Cel}(W_{V\setminus X})$ there exists $R_Y \in \mathcal{R}_{X,Y}$, such that $d_{out}(R_Y) = 1$. Then*

(1) *given $\varphi \in \mathrm{Isow}(W, W')$ the restriction map*

$$\mathrm{Iso}(W, W', \varphi) \to \mathrm{Iso}(W_X, W'_{X^\varphi}, \varphi_X), \quad f \mapsto f_X$$

is a bijection. In particular, the restriction map $\mathrm{Aut}(W) \to \mathrm{Aut}(W_X)$ is a group isomorphism.

(2) *W is separable (resp. Schurian) whenever W_X is separable (resp. Schurian).*

Proof. For each cell Y of $W_{V\setminus X}$ let us fix a basic relation $R_Y \in \mathcal{R}_{X,Y}$ such that $d_{out}(R_Y) = 1$. If $Y \in \mathrm{Cel}(W_X)$, then set $R_Y = \Delta^{(2)}(Y)$. Let $Y \in \mathrm{Cel}(W)$. Then $A_Y A_Y^T = A(E_Y)$ for some $E_Y \in \mathcal{E}(W)$ where $A_Y = A(R_Y)$. So the mapping $h : Y \to X/E_Y$ such that $v^h = R_Y(v)$, is a bijection and

$$R_Y = \bigcup_{v\in Y} v^h \times \{v\}. \tag{50}$$

Let $R \in \mathcal{R}_{Y,Z}$ for some $Y, Z \in \mathrm{Cel}(W)$. Let us choose $S \in \mathcal{R}_{X,X}$ such that the matrix $A(S)$ enters the decomposition of $A_Y A(R)(A_Z)^T$ by the basis matrices of W. Then obviously $S \cap (U_Y \times U_Z) \ne \emptyset$ for some $U_Y \in X/E_Y$, $U_Z \in X/E_Z$ only if $(u, v) \in R$ where $u = h_Y^{-1}(U_Y)$ and $v = h_Z^{-1}(U_Z)$. So

$$A_Y^T A(S) A_Z = c(S)A(R) \tag{51}$$

for a positive rational $c(S)$.

To prove statement (1) let $\varphi \in \mathrm{Isow}(W, W')$ where $W' \le \mathrm{Mat}_{V'}$. Set $X' = X^\varphi$. Further given $Y \in \mathrm{Cel}(W)$ set $Y' = Y^\varphi$, $R_{Y'} = (R_Y)^\varphi$ and $E_{Y'} = (E_Y)^\varphi$ (see Lemma 2.1). Then $d_{out}(R_{Y'}) = 1$ and so $R_{Y'} = \bigcup_{v'\in Y'} (v')^{h'} \times \{v'\}$ where $h' : Y' \to X'/E_{Y'}$ is a bijection such that $(v')^{h'} = R_{Y'}(v')$. Let now $f_0 \in \mathrm{Iso}(W_X, W'_{X'}, \varphi_X)$. Given $Y \in \mathrm{Cel}(W)$ set $f_Y : X/E_Y \to X'/E_{Y'}$ to be the bijection induced by f_0. Then obviously the mapping

$$f : V \to V', \quad v \mapsto v^h f_Y (h')^{-1},$$

where Y is the cell of W containing v is a bijection. It follows from (50) that $(R_Y)^f = R_{Y'}$ for all $Y \in \mathrm{Cel}(W)$. So by the equality (51) we have $R^f = R^\varphi$ for all $R \in \mathcal{R}(W)$. Thus $f \in \mathrm{Iso}(W, W', \varphi)$. Since $R_Y = \Delta^{(2)}(Y)$ for $Y \in \mathrm{Cel}(W_X)$, we have $f_X = f_0$ for all $f_0 \in \mathrm{Iso}(W_X, W'_{X'}, \varphi_X)$. On the other hand, given an arbitrary $f \in \mathrm{Iso}(W, W', \varphi)$ the bijection $V \to V'$ constructed as above for $f_0 = f_X$ coincides with f. Thus statement (1) follows.

To prove statement (2) suppose first that W_X is separable. Let $\varphi \in \mathrm{Isow}(W, W')$ for some W'. Then it follows from the separability of W_X that there exists $f_0 \in \mathrm{Iso}(W_X, W'_{X'}, \varphi_X)$ where $X' = X^\varphi$. By statement (1) $f_0 = f_X$ for some $f \in \mathrm{Iso}(W, W', \varphi)$. Thus W is separable. Suppose now that W_X is Schurian. Let $R \in \mathcal{R}_{Y,Z}$ where $Y, Z \in \mathrm{Cel}(W)$. Set

$$\overline{S} = \{(U_Y, U_Z) :\in X/E_Y \times X/E_Z :\ S \cap (U_Y \times U_Z) \neq \emptyset\}$$

where S is as in (51). Then by this formula the mapping $(U_Y, U_Z) \mapsto (u, v)$ where $u = (h_Y)^{-1}(U_Y)$, $v = (h_Z)^{-1}(U_Z)$ is a bijection from $\overline{S}$ onto R. Using (50) and the invariancy of the relations R_Y and R_Z with respect to the group $\mathrm{Aut}(W)$ we see that this bijection defines an equivalence between the actions of $\mathrm{Aut}(W)$ on $\overline{S}$ and R. On the other hand, $\mathrm{Aut}(W_X)$ acts transitively on $\overline{S}$ due to the Schurity of W_X. This implies by statement (1) that $\mathrm{Aut}(W)$ transitively acts on $\overline{S}$ and hence by the above on R. Thus R is a 2-orbit of $\mathrm{Aut}(W)$ and W is Schurian.∎

Corollary 9.5 *The mappings $W \mapsto \mathrm{Aut}(W)$, $\Gamma \mapsto \mathcal{Z}(\Gamma)$ determine a one-to-one correspondence between the 1-regular cellular rings and the permutation groups with base number at most 1.*∎

Theorem 9.6 *Let W be a cellular ring and $m \geq 1$ a positive integer. If the ring $W_{v_1,\ldots,v_{m-1}}$ is 1-regular for some points $v_1, \ldots, v_{m-1}$ of W, then the ring $\widehat{W}^{(m)}$ is also 1-regular.*

Proof. Since $W_{v_1,\ldots,v_{m-1}}$ is a 1-regular ring, by Lemma 9.2 and Lemma 3.1 the ring $\widehat{W}_U$ where U is defined in the latter lemma, is also 1-regular. Denote by $\overline{v} = (v_1, \ldots, v_{m-1}, v_m)$ a regular point of $\widehat{W}_U$. Let us prove that $\overline{v}$ is a regular point of $\widehat{W}$. Given $i \in \{1, \ldots, m\}$ set $E_i = \{(\overline{u}, \overline{u}') \in V^m \times V^m :\ u_i = u'_i\}$. Then it suffices to prove that

$$\forall i \in \{1, \ldots, m\}\ \forall U_i \in V^m/E_i\ \exists R_i \in \mathcal{R}^*(\widehat{W}) :\quad R_i(\overline{v}) = U_i. \tag{52}$$

Indeed, given a point $\overline{u} \in V^m$ we obviously have $\{\overline{u}\} = \bigcap_{i=1}^m U_i$ where U_i is the class of E_i containing $\overline{u}$. According to (52) $U_i = R_i(\overline{v})$ where $R_i \in \mathcal{R}^*(\widehat{W})$ for all i. So $\{\overline{u}\} = R(\overline{v})$ where $R = \bigcap_{i=1}^m R_i$. Thus $R \in \mathcal{R}^*(\widehat{W})$ and $d_{out}(R) = 1$. This implies that $R \in \mathcal{R}(\widehat{W})$ and hence $\overline{v}$ is a regular point of $\widehat{W}$.

Let us prove (52). Suppose first that $i = m$. Given $U' \in V^m/E_m$ there exists $v \in V$ such that $U' = \{\overline{u} \in V^m :\ u_m = v\}$. Denote by R the basis relation of $\widehat{W}$ containing the pair $(\overline{v}, v^\varsigma)$. Then $d_{out}(R) = 1$ because $R \subset E$ and $\overline{v}$ is a regular point of $\widehat{W}_U$. So $U' = R'(v)$ where R' is the binary relation on V^m with adjacency matrix $A(R') = A(R)A(E_m)$. Since obviously $E_m \in \mathcal{E}(\widehat{W})$, we have $R' \in \mathcal{R}(\widehat{W})$. In the case of arbitrary i set G to be the image of the natural representation of the symmetric group of degree m by permutation matrices of Mat_{V^m}. Then it follows from [4] that $G \subset \widehat{W}$. Since the action of the group G by right multiplications on the set $\{A(E_i) :\ i = 1, \ldots, m\}$ is transitive, this reduces the general case to the case $i = m$.∎

Theorem 9.3 and Theorem 9.6 imply the following statement.

Corollary 9.7 *Let W be a cellular ring and b is the base number of W. Then the ring $\widehat{W}^{(m)}$ is separable and Schurian whenever $m \geq b+1$.*■

References

[1] A. E. Brouwer, A. M. Cohen, A. Neumaier, *Distance-Regular graphs*, Springer, Berlin, 1989.

[2] S. Evdokimov, I. Ponomarenko, *Isomorphism of coloured graphs with slowly increasing multiplicity of Jordan blocks*, Combinatorica, **19** (1999), 321–333.

[3] S. Evdokimov, I. Ponomarenko, *On primitive cellular algebras*, Zapiski Nauchnykh Seminarov POMI, **256** (1999), 38–68.

[4] S. Evdokimov, M. Karpinski, I. Ponomarenko, *On a New High Dimensional Weisfeiler-Lehman Algorithm*, Journal of Algebraic Combinatorics, **10** (1999), 29–45.

[5] S. A. Evdokimov, I. N. Ponomarenko, *On highly closed cellular algebras and highly closed isomorphisms*, Electronic J. of Combinatorics, **6** (1999), #R18.

[6] S. Evdokimov, I. Ponomarenko, *Separability Number and Schurity Number of Coherent Configurations*, Electronic Journal of Combinatorics, **7** (2000), #R31.

[7] S. Evdokimov, I. Ponomarenko, G. Tinhofer, *Forestal algebras and algebraic forests (on a new class of weakly compact graphs)*, Discrete Mathematics, **225** (2000), 149–172.

[8] S. Evdokimov, I. Ponomarenko, *On a family of Schur rings over a finite cyclic group*, Algebra and Analysis, **13** (2001), 3, 139–154.

[9] D. G. Higman, *Coherent configurations. I*, Rend. Sem. Mat. Univ. Padova, **44** (1970), 1–25.

[10] K. H. Leung, S. H. Man, *On Schur Rings over Cyclic Groups, II*, J. Algebra, **183** (1996), 273–285.

[11] K. H. Leung, S. H. Man, *On Schur Rings over Cyclic Groups*, Israel J. Math., **106** (1998), 251–267.

[12] R. Lidl, H. Niedereiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1986 (Russian).

[13] R. McConnel, *Pseudo-ordered polynomials over a finite field*, Acta Arith., **8** (1963), 127–151.

[14] M. E. Muzychuk, *The structure of basis sets of Schur rings over cyclic groups*, J. of Algebra, **169** (1994), 655–678.

[15] R. Pöschel, *Untersuchungen von S-Ringen insbesondere im Gruppenring von p-Gruppen*, Math. Nachr., **60** (1974), 1–27.

[16] I. M. Vinogradov, *Basic number theory*, Moscow, 1972.

[17] B. Ju. Weisfeiler, A. A. Leman, *Reduction of a graph to a canonical form and an algebra which appears in the process*, NTI, Ser.2, (1968), 9, 12–16.

[18] B. Ju. Weisfeiler (editor), *On construction and identification of graphs*, Springer Lecture Notes, 558, 1976.

[19] H. Wielandt, *Finite permutation groups*, Academic press, New York - London, 1964.

[20] H. Wielandt, *Permutation groups through invariant relations and invariant functions*, Lect. Notes Dept. Math. Ohio St. Univ., Columbus, 1969.