PDMI PREPRINT 19/2003

A new look at the Burnside-Schur theorem

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 †

23.10.2003

Abstract

The famous Burnside-Schur theorem states that every primitive finite permutation group containing a regular cyclic subgroup is either 2-transitive or isomorphic to a subgroup of a 1-dimensional affine group of prime degree. It is known that this theorem can be expressed as a statement on Schur rings over a finite cyclic group. Generalizing the latters we introduce Schur rings over a finite commutative ring and prove an analog of this statement for them. Besides, the finite local commutative rings are characterized in the permutation group terms.

*Partially supported by RFFI, grants 01-01-00219, 03-01-00349
†Partially supported by RFFI, grants, 01-01-00219, 03-01-00349, NSH-2251.2003.1

1 Introduction

1.1. The starting point of the paper is the following statement.

Theorem (Burnside-Schur). Every primitive finite permutation group containing a regular cyclic subgroup is either 2-transitive or permutationally isomorphic to a subgroup of the affine group $\mathrm{AGL}_1(p)$ where p is a prime.[1] ■

In fact, Burnside [3, pp.339-343] proved the theorem for the permutation groups of prime power degree and conjectured that the statement would still true when the regular subgroup in question was abelian, not only cyclic. Schur [11] disproved this conjecture and showed that every primitive permutation group of composite degree containing a regular cyclic subgroup is 2-transitive. This result was generalized by Wielandt in [12, Theorem 25.4] (see also Corollary 1.3 below).

In contrast to the method of Burnside who employed the character theory the idea of Schur was as follows. Let Γ be a permutation group containing a regular subgroup G. Then the submodule $\mathcal{A}(\Gamma)$ of the group ring of G spanned by the orbits of a one-point stabilizer of Γ is a subring of the latter ring (after the choice of the point these orbits are treated in a natural way as subsets of G). The ring $\mathcal{A}(\Gamma)$ is a special case of a Schur ring (or S-ring) over the group G (for the definition of S-rings and basic facts about them see Section 2).[2] Schur observed that the group Γ is 2-transitive (resp. primitive) iff the S-ring $\mathcal{A}(\Gamma)$ is of rank 2 (resp. primitive). Thus the Burnside-Schur theorem when the degree of Γ is a composite number is an immediate consequence of the following theorem proved in fact by Schur: every primitive S-ring over a cyclic group of composite order is of rank 2.

An essential ingredient of Schur's proof is the following theorem on multipliers: every S-ring over a finite abelian group G is invariant with respect to the group K_G consisting of the automorphisms of G induced by raising to powers coprime to $|G|$. If the group G is cyclic, then it can be treated as the additive group of the ring $\mathbb{Z}_n$ of integers modulo n where $n = |G|$. In this case K_G is identified with the multiplications by the units of $\mathbb{Z}_n$. Thus in the cyclic case the multiplier theorem states that every S-ring over G is an S-ring *over the ring* $\mathbb{Z}_n$ in the sense of the following definition.

Definition. *Let $\mathcal{A}$ be an S-ring over a group G and R a finite commutative ring. We say that $\mathcal{A}$ is an S-ring over the ring R if $G = R^+$ and $\mathcal{A}$ is invariant with respect to the group $K_R \leq \mathrm{Aut}(G)$ induced by the action of $R^\times$ on R^+ by multiplications.*

Example. Let R be a finite commutative ring and $K \leq K_R$. Then, obviously, the set of all K-invariant elements of $\mathbb{Z}[R^+]$ forms an S-ring over the ring R. It is called a *cyclotomic* one. The basic sets of this ring are exactly the orbits of K on R. Since the group K_R is regular on $R^\times$, the cyclotomic rings are in 1-1 correspondence to the subgroups of $R^\times$. The translation association schemes corresponding to cyclotomic S-rings were studied in [8]. Let now R is a field of order q and $\Gamma \leq \mathrm{Sym}(R)$ a permutation group containing the translations of R. Suppose that $\mathcal{A}(\Gamma)$ is a cyclotomic ring of rank greater than 2. Then Γ is a subgroup of the automorphism group of the translation association scheme (Cayley ring) corresponding to $\mathcal{A}(\Gamma)$ (see e.g. [7]). So $\Gamma \leq \mathrm{A\Gamma L}_1(q)$

[1] In the prime degree case the assumption on the existence of a regular cyclic subgroup is unnecessary.

[2] The term was proposed by Wielandt in [12] where the theory of S-rings was developed.

by [2, p.389].

It should be remarked that the group K_G as in the Schur theorem on multipliers coincides with the center of $\mathrm{Aut}(G)$. If G is cyclic, then obviously $K_G = \mathrm{Aut}(G)$ and so any S-ring over G admits the maximal possible multiplier group. This probably explains the fact that there is a nice theory of S-rings over finite cyclic groups [9, 7]. On the contrary, $K_G < \mathrm{Aut}(G)$ for any noncyclic G (in this case K_G is not even a maximal abelian subgroup of $\mathrm{Aut}(G)$) and the theory of S-rings over arbitrary abelian groups is far from being completed. The present paper is the first step to reconstruct the main features of the cyclic case theory for the S-rings admitting an appropriate sufficiently large multiplier group containing K_G (e.g. K_R where R is a finite commutative ring with $R^+ = G$). In subsequent papers we plan to study S-rings over finite commutative rings and describe them completely at least for the products of Galois rings of pairwise coprime characteristics.

1.2. To formulate the main results of the paper we recall some basic facts on finite rings (see e.g. [10]). Let R be a finite ring with identity. Then

$$R = \prod_p R_p$$

where p runs over all prime divisors of $|R|$ and R_p is a *primary component* of R, i.e. a subring of R such that $(R_p)^+$ is the Sylow p-subgroup of R^+. Moreover, each commutative primary component of R is a direct product of local rings (i.e. ones the non-units of which form an ideal). Below an S-ring over a finite commutative ring R is called *quasiprimitive* if it is K_R-primitive (see the definition before Theorem 1.2). If R is not isomorphic to the product of two rings one of which is $\mathbb{Z}_2 \times \mathbb{Z}_2$, then it is generated by the units (see [10, p.406]) and so in this case an S-ring $\mathcal{A}$ over R is quasiprimitive iff $\{0\}$ and R are the only ideals of R that are also $\mathcal{A}$-subgroups of R^+. Now the following statement can be considered as a generalization of the Burnside-Schur theorem.

Theorem 1.1 *Let R be a finite commutative ring with identity. If every primary component of R is a local ring, then each quasiprimitive S-ring over R is either of rank 2 or cyclotomic. In the latter case R is a field.*

To see that Theorem 1.1 really generalizes the Burnside-Schur theorem let Γ be a primitive permutation group containing a regular cyclic subgroup G. Then by the Schur theorem on multipliers one can assume (without loss of gnerality) that $\mathcal{A}(\Gamma)$ is an S-ring over the ring $\mathbb{Z}_n$ where $n = |G|$. Since Γ is a primitive group, $\mathcal{A}(\Gamma)$ is a primitive S-ring over the group $\mathbb{Z}_n^+$, which means that it is quasiprimitive S-ring over the ring $\mathbb{Z}_n$. Besides, every primary component of $\mathbb{Z}_n$ is obviously a local ring. Thus the statement of Theorem 1.1 (with $R = \mathbb{Z}_n$) holds for the S-ring $\mathcal{A}(\Gamma)$. If $\mathrm{rk}(\mathcal{A}(\Gamma)) = 2$, then Γ is 2-transitive. Otherwise, $\mathcal{A}(\Gamma)$ is cyclotomic and $n = p$ is a prime. So $\Gamma \leq \mathrm{AGL}_1(p)$ by [2, Proposition 12.7.5] (see the example in Subsection 1.1).

Theorem 1.1 is an immediate consequence of Theorem 1.4 below which will be deduced from the following theorem on groups to be proved in Section 4. Below an S-ring $\mathcal{A}$ over a group G is called *K-primitive* where $K \leq \mathrm{Aut}(G)$, if $\{1\}$ and G are the only K-invariant $\mathcal{A}$-subgroups of G (for $K = \{1\}$ this means that $\mathcal{A}$ is primitive).

Theorem 1.2 *Let G be a finite abelian group and $K \leq \mathrm{Aut}(G)$. Suppose that there exists a Sylow p-subgroup P of G such that*

(1) *$K \cap \mathrm{Aut}(P)$ is an abelian group,*

(2) *P is the disjoint union of an orbit of $K \cap \mathrm{Aut}(P)$ and a K-invariant subgroup of P.*

Then each K-primitive K-invariant S-ring over G is either of rank 2 or Cayley isomorphic to a cyclotomic ring over a field with K going to the multiplications by nonzero elements of the field.

Corollary 1.3 (Wielandt). *Each primitive permutation group containing an abelian regular subgroup of composite order which has a cyclic Sylow subgroup, is 2-transitive.*

Proof. Let G be an abelian group of composite order such that one of its Sylow subgroups, say P, is cyclic. It suffices to prove that every primitive S-ring over G is of rank 2. Set $K = K_G$. Then by the Schur theorem on multipliers any S-ring over G is K-invariant. Moreover, it is easily seen that P is the disjoint union of the K-orbit containing a generator of P, and the subgroup of P of prime index. So by Theorem 1.2 every K-primitive S-ring over G is either of rank 2 or cyclotomic over a field. Since $|G|$ is a composite number, the latter case is impossible. To complete the proof it suffices to note that obviously an S-ring over G is K-primitive iff it is primitive.■

Let R be a finite commutative ring with identity at least one primary component of which, say R_p, is a local ring. Then the hypothesis of Theorem 1.2 is satisfied for $G = R^+$, $K = K_R$ and $P = (R_p)^+$ (indeed, $K \cap \mathrm{Aut}(P) = K_{R_p}$, $(1_{R_p})^{K_{R_p}} = (R_p)^\times$ and $P = (R_p)^\times \cup \mathrm{rad}(R_p)$). Besides, in accordance with our definitions the quasiprimitive S-rings over R are exactly the K-primitive K-invariant S-rings over G. Thus the following statement is a specialization of Theorem 1.2

Theorem 1.4 *Let R be a finite commutative ring with identity. If at least one primary component of R is a local ring, then each quasiprimitive S-ring over R is either of rank 2 or cyclotomic. In the latter case R is a field.*■

As the following example shows the locality of some primary component of the ring R in Theorem 1.4 is essential. Indeed, let $R = \mathbb{Z}_p \times \mathbb{Z}_p$ where $p > 2$ is a prime. Set

$$X_0 = \{(0,0)\}, \quad X_1 = (\mathbb{Z}_p^\times \times \{0\}) \cup (\{0\} \times \mathbb{Z}_p^\times), \quad X_2 = \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times.$$

Then, obviously, X_0, X_1, X_2 are the basic sets of an S-ring $\mathcal{A}$ over the group R^+. Since $R^\times = \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$ and $\mathbb{Z}_p \times \{0\}$ and $\{0\} \times \mathbb{Z}_p$ are the only proper ideals of R, one can see that $\mathcal{A}$ is a quasiprimitive S-ring over the ring R. It remains to note that $\mathrm{rk}(\mathcal{A}) = 3$ and the ring R is not local.

Let $G = P$ be a finite abelian p-group. As we saw above the hypothesis of Theorem 1.2 is satisfied when $K = K_R$ where R is a local commutative ring on P, i.e. one with $R^+ = P$. In fact this is the only possible case because as R runs over all such rings, $R^\times$ runs over all groups K as in this theorem (see Theorem 1.5). To be more precise, let $K \leq \mathrm{Aut}(P)$ be an abelian group and $e \in P$. We say that (K, e) is a *local pair* on P if the set $P \setminus O$ is a subgroup of P where $O = e^K$. It is easily seen that this subgroup is uniquely determined by K and the group K acts regular and faithfully on O.

Theorem 1.5 *Let P be a finite abelian p-group. Then the mapping*

$$R \mapsto (K_R, 1_R) \tag{1}$$

establishes a 1-1 correspondence between the set of all local commutative rings on P and the set of all local pairs on P. Moreover, two such rings are isomorphic iff the corresponding subgroups are conjugate in $\mathrm{Aut}(P)$.

The proof of Theorem 1.5 as well as Theorem 1.2 is contained in Section 4. In fact, the latter theorem is deduced from the first one and the theorem on a separating subgroup proved in Section 3. Section 2 contains necessary definitions and facts on S-rings. All undefined terms and results concerning permutation groups can be found in [5].

1.3. We complete the introduction by making some remarks on a topic closely related to the contents of the paper. Following [12] a finite group G is called a *B-group* if every primitive group containing a regular subgroup isomorphic to G is 2-transitive. In fact, the Burnside-Schur theorem states in particular that a cyclic group of composite order is a B-group (see also Corollary 1.3). As P. Cameron observed in [4] the classification of finite simple groups implies that for almost all positive integers n, every group of order n is a B-group. At the same time the problem of the classification of B-groups (even abelian ones) is still open. In this connection it should be remarked that most of B-groups G listed in [12] including those as in Corollary 1.3 satisfy *a priori* a more strong condition: every primitive S-ring over G is of rank 2 (in fact there exist S-rings even over a cyclic group that do not come from permutation groups, see [6]). Obviously, no group of odd prime order satisfies this condition. However, the following is true.

Proposition 1.6 *For any abelian group G there exists an abelian group $K \leq \mathrm{Aut}(G)$ such that each K-primitive K-invariant S-ring over G is of rank 2.*

Proof. By Theorem 1.1 it suffices to verify that each abelian p-group P of composite order is isomorphic to the additive group of a local commutative ring which is not a field. By Theorem 1.5 all we need is to present a local pair (K, e) on P such that $P \setminus e^K \neq \{0\}$. Let p^m be the exponent of P and $P = \mathbb{Z}_{p^m}^+ \times P'$ for some P'. Then treating P as a $\mathbb{Z}_{p^m}$-module one can take $e = (1, 0)$ and $K = \{x \mapsto ax + x_1 b,\ x \in P:\ a \in \mathbb{Z}_{p^m}^\times,\ b \in P'\}$ where x_1 is the first coordinate of x. It is easy to see that the group K is abelian.■

Proposition 1.6 shows that the study of pairs (G, K) as in it is seemingly more fruitful than that of B-groups. For instance, it would be interesting to identify B-rings, i.e. finite commutative rings R for which (R^+, K_R) is such a pair (a special class of B-rings can be derived from Theorem 1.4).

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

For a ring R with identity we denote by R^+, $R^\times$ and $\mathrm{rad}(R)$ the additive and multiplicative groups of R and the radical of R respectively.

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

2 S-rings

2.1. Let G be a finite group. A subring $\mathcal{A}$ of the group ring $\mathbb{Z}[G]$ is called a *Schur ring* (briefly *S-ring*) over G if it has a (uniquely determined) $\mathbb{Z}$-base consisting of the elements $\xi(X) = \sum_{x\in X} x$ where X runs over a family $\mathcal{S} = \mathcal{S}(\mathcal{A})$ 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 $\mathcal{S}$ *basic* sets of $\mathcal{A}$ and denote by $\mathcal{S}^*(\mathcal{A})$ the set of all unions of them and by $\mathcal{H}(\mathcal{A})$ the set of all $\mathcal{A}$-*subgroups* of G, i.e. those belonging to $\mathcal{S}^*(\mathcal{A})$. For $K \le \mathrm{Aut}(G)$ we set $\mathcal{H}_K(\mathcal{A}) = \{H \in \mathcal{H}(\mathcal{A}) :\ H^K = H\}$. The basic set of $\mathcal{A}$ that contains $x \in G$ is denoted by $[x]$. The number $\mathrm{rk}(\mathcal{A}) = \dim_{\mathbb{Z}}(\mathcal{A})$ is called the *rank* of $\mathcal{A}$. Two S-rings $\mathcal{A}$ over G and $\mathcal{A}'$ over G' are called *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 isomorphism from $\mathbb{Z}[G]$ to $\mathbb{Z}[G']$ induced by f.

The first statement of the following lemma was in fact proved in a different form in [12, Theorem 23.9] which also contains the proof of the second statement for $K = \{1\}$.

Lemma 2.1 *Let G be a finite abelian group, $\mathcal{A}$ an S-ring over G and p a prime dividing $|G|$. Then for any $X \in \mathcal{S}(\mathcal{A})$ the following statements hold:*

(1) *$X^{[p]} \in \mathcal{S}^*(\mathcal{A})$ where $X^{[p]} = \{x^p :\ x \in X,\ |xE \cap X| \not\equiv 0 \pmod p\}$ with $E = \{g \in G :\ g^p = 1\}$.*

(2) *if the ring $\mathcal{A}$ is K-invariant and K-primitive for some group $K \le \mathrm{Aut}(G)$, then $X^{[p]} = \{1\}$; in particular, $|xE \cap X| \equiv 0 \pmod p$ for all $x \in G \setminus E$.*

Proof. Let $X \in \mathcal{S}(\mathcal{A})$. Then using a well-known property of binomial coefficients we have

$$\xi(X)^p = (\sum_{x\in X} x)^p \equiv \sum_{x\in X} x^p \pmod p. \tag{2}$$

On the other hand, given a coset $C \in G/E$, the element g^p does not depend on the choice of $g \in C$. Denote it by h_C. We observe that the mapping $C \mapsto h_C$ is a bijection from G/E onto G^p. So

$$\sum_{x\in X} x^p = \sum_{C\in G/E} |C \cap X| \cdot h_C \equiv \sum_{\substack{C\in G/E,\\ |C\cap X|\not\equiv 0 \pmod p}} |C \cap X| \cdot h_C \pmod p. \tag{3}$$

By [12, Proposition 22.3] formulas (2) and (3) imply that the set $\{h_C :\ C \in G/E,\ |C \cap X| \not\equiv 0 \pmod p\}$ belongs to $\mathcal{S}^*(\mathcal{A})$. Since this set equals $X^{[p]}$, statement (1) is proved. To prove statement (2) suppose that the ring $\mathcal{A}$ is K-invariant and K-primitive for some $K \le \mathrm{Aut}(G)$. It suffices to verify that $X^{[p]} = \{1\}$. To do this denote by H the subgroup of G generated by the sets $(X^{[p]})^k$, $k \in K$. Then $H \in \mathcal{H}_K(\mathcal{A})$ by statement (1) and the K-invariance of $\mathcal{A}$. On the other hand, $H \le G^p < G$. So $H = \{1\}$ due to the K-primitivity of $\mathcal{A}$. Since $X^{[p]} \subset H$, we are done.■

2.2. Let G be a finite abelian group and $\widehat{G}$ the group dual to G. For $\sigma \in \mathrm{Aut}(G)$ and $\chi \in \widehat{G}$ we define a function $\chi^{\widehat{\sigma}}$ on $\widehat{G}$ by $\chi^{\widehat{\sigma}}(g) = \chi(g^{\sigma^{-1}})$, $g \in G$. It is easily seen that $\chi^{\widehat{\sigma}} \in \widehat{G}$. Moreover, the mapping $\chi \mapsto \chi^{\widehat{\sigma}}$, $\chi \in \widehat{G}$, belongs to $\mathrm{Aut}(\widehat{G})$ and the mapping

$$\mathrm{Aut}(G) \to \mathrm{Aut}(\widehat{G}), \quad \sigma \mapsto \widehat{\sigma},$$

is a group isomorphism. This enables us to identify $\mathrm{Aut}(G)$ with $\mathrm{Aut}(\widehat{G})$ and treat any subgroup K of $\mathrm{Aut}(G)$ as a subgroup of $\mathrm{Aut}(\widehat{G})$. Clearly, H is a K-invariant subgroup of G iff $H^{\perp}$ is a K-invariant subgroup of $\widehat{G}$ where $H^{\perp} = \{\chi \in \widehat{G} :\ H \le \ker(\chi)\}$.

Let $\mathcal{A}$ be an S-ring over the group G. Denote by $\widehat{S}$ the set of all classes of the equivalence relation on $\widehat{G}$ defined as follows: $\chi_1 \sim \chi_2$ iff the extensions of χ_1 and χ_2 to $\mathbb{Z}[G]$ coincide on $\mathcal{A}$. Then the $\mathbb{Z}$-submodule of $\mathbb{Z}[\widehat{G}]$ spanned by the elements $\xi(X)$, $X \in \widehat{S}$, is an S-ring over $\widehat{G}$ (see [1, Theorem 6.3]). This ring is called *dual* to $\mathcal{A}$ and denoted by $\widehat{\mathcal{A}}$. Obviously, $\mathcal{S}(\widehat{\mathcal{A}}) = \widehat{S}$. Moreover, $\mathrm{rk}(\mathcal{A}) = \mathrm{rk}(\widehat{\mathcal{A}})$.

Theorem 2.2 *Let $\mathcal{A}$ be an S-ring over a finite abelian group G and $K \le \mathrm{Aut}(G)$. Then*

(1) *the ring $\mathcal{A}$ is K-invariant iff the dual ring $\widehat{\mathcal{A}}$ is K-invariant.*

(2) *$H \in \mathcal{H}_K(\mathcal{A})$ iff $H^{\perp} \in \mathcal{H}_K(\widehat{\mathcal{A}})$; in particular, the ring $\mathcal{A}$ is K-primitive iff the dual ring $\widehat{\mathcal{A}}$ is K-primitive.*

Proof. If the ring $\mathcal{A}$ is K-invariant, then given $\sigma \in K$ we have: $\chi_1 \sim \chi_2$ iff $\chi_1^{\sigma} \sim \chi_2^{\sigma}$. So the ring $\widehat{\mathcal{A}}$ is K-invariant. The converse statement follows from the equality $\widehat{\widehat{\mathcal{A}}} = \mathcal{A}$. To prove the first part of statement (2) we observe that given $H \le G$ and $\chi \in \widehat{G}$ we have: $H \le \ker(\chi)$ iff $\sum_{h\in H} \chi(h) = |H|$ (we used that $|\chi(h)| = 1$ for all h and $\chi(1) = 1$). Let now $H \in \mathcal{H}_K(\mathcal{A})$. Then the above observation implies that $\chi \in H^{\perp}$ iff $\chi' \in H^{\perp}$ whenever $\chi \sim \chi'$. So $[\chi] \subset H^{\perp}$ for all $\chi \in H^{\perp}$, and hence $H^{\perp} \in \mathcal{H}_K(\widehat{\mathcal{A}})$. The second part of statement (2) is the consequence of the first one and the obvious equalities $\{1\}^{\perp} = \widehat{G}$ and $G^{\perp} = \{1\}$.■

3 Theorem on a separating subgroup

In this section we prove a statement on S-rings over a finite group which is a key one for the proof of Theorem 1.2. In this connection it is worth remarking that the proofs of Wielandt's theorem (Corollary 1.3) from [2] and [5] go back to its original proof (see [12, Theorem 25.4]). A detailed analysis shows that in fact most part of Wielandt's proof deals with a special case of Theorem 3.1 below. In its turn this theorem is a consequence of a more general result on association schemes the proof of which is outside the scope of the present paper.

The following definition is taken from [7]. Given a nonempty subset X of a finite group G the group

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

is called the *radical* of X.[3] It is the largest subgroup of G such that X is a union of the left as well as right cosets by this subgroup. Besides, obviously $\mathrm{rad}(X) \subset \langle X \rangle$ where $\langle X \rangle$ is a subgroup of G generated by X. If $X \in \mathcal{S}^*(\mathcal{A})$ where $\mathcal{A}$ is an S-ring over G, then $\mathrm{rad}(X)$ and $\langle X \rangle$ are $\mathcal{A}$-subgroups of G.

Theorem 3.1 *Let X be a basic set of an S-ring $\mathcal{A}$ over a finite group G. Suppose that*

$$\langle X \cap H \rangle \le \mathrm{rad}(X \setminus H)$$

for some subgroup H of G such that $X \cap H \ne \emptyset$ and $X \setminus H \ne \emptyset$. Then $X = \langle X \rangle \setminus \mathrm{rad}(X)$ with $\mathrm{rad}(X) \le H \le \langle X \rangle$.

Proof. For $A, B, C \subset G$ set $\xi_A = \xi(A)$ and $\xi_{A,B,C} = (\xi_A \xi_B) \circ \xi_C$. Since $X \in \mathcal{S}(\mathcal{A})$, we have

$$\xi_{X,X^{-1},X} = a_X \xi_X = a_X \xi_Y + a_X \xi_Z \tag{4}$$

for some integer $a_X \ge 0$, where $Y = X \cap H$ and $Z = X \setminus H$. Obviously, $\xi_{Y,Y^{-1},Z} = \xi_{Y,Z^{-1},Y} = \xi_{Z,Y^{-1},Y} = 0$ and hence

$$\begin{aligned} &\xi_{X,X^{-1},X} = ((\xi_Y + \xi_Z)(\xi_{Y^{-1}} + \xi_{Z^{-1}})) \circ (\xi_Y + \xi_Z) = \\ &(\xi_{Y,Y^{-1},Y} + \xi_{Z,Z^{-1},Y}) + (\xi_{Y,Z^{-1},Z} + \xi_{Z,Y^{-1},Z} + \xi_{Z,Z^{-1},Z}). \end{aligned} \tag{5}$$

From the hypothesis of the theorem it follows that

$$\xi_{Z,Z^{-1},Y} = |Z|\xi_Y, \quad \xi_{Y,Z^{-1},Z} = \delta|Y|\xi_Z, \quad \xi_{Z,Y^{-1},Z} = |Y|\xi_Z \tag{6}$$

$\delta = \delta_{X,X^{-1}}$ is the Kronecker delta. Due to (4) and (5) this implies that $\xi_{Y,Y^{-1},Y} = a_Y \xi_Y$ and $\xi_{Z,Z^{-1},Z} = a_Z \xi_Z$ for some integers $a_Y \ge 0$ and $a_Z \ge 0$. Thus,

$$a_X = |Z| + a_Y = (\delta + 1)|Y| + a_Z. \tag{7}$$

We observe that $a_Y = |Y \cap gY|$ for $g \in Y$ and $a_Z = |Z \cap gZ|$ for $g \in Z$. Now let us prove that $\delta = 1$ and

$$a_Y \ge 2|Y| - |H|, \quad a_Z \le |Z| - |H|. \tag{8}$$

Since $H \cap Z = \emptyset$, we have $gH \cap gZ = \emptyset$ for $g \in Z$. So $a_Z \le |Z| - |H|$ because $gH \subset Z$. This implies that $\delta = 1$, for otherwise

$$a_X = |Y| + a_Z \le |Y| + |Z| - |H| < |Z| \le |Z| + a_Y = a_X$$

(we used (7) and the inclusion $Y \subset H \setminus \{1\}$). In particular, $Y = Y^{-1}$ and $Z = Z^{-1}$. Moreover, the latter equality implies that $a_Z = |Z| - |H|$ iff $Z \cup gZ = Z \cup H$ for all $g \in Z$, i.e. iff $Z \cup H$ is a subgroup of G. Next, by the inclusion-exclusion principle we have

$$a_Y = |Y \cap gY| = 2|Y| - |Y \cup gY| \ge 2|Y| - |H|, \quad g \in Y,$$

[3] Not to mix it up with the radical of a ring.

with the equality attained iff $Y \cap gY = H$ for all $g \in Y$, i.e. iff $H \setminus Y$ is a subgroup of H (indeed, otherwise $H = Y \cup (h_1 h_2^{-1})Y$ for some $h_1, h_2 \in H \setminus Y$ with $h_1 h_2 \in Y$, whence $h_1 \in (h_1 h_2^{-1})Y$ which is impossible).

From (7) and the equality $\delta = 1$ it follows that

$$0 = (a_Y - 2|Y| + |H|) + (|Z| - |H| - a_Z).$$

By (8) both expressions in the brackets are nonnegative. So they equal to 0. Due to the above paragraph this means that $H \setminus Y$ and $Z \cup H$ are subgroups of G. Since obviously $X = (H \setminus Y) \cup (Z \cup H)$, we conclude that $\langle X \rangle = Z \cup H$ and $\mathrm{rad}(X) = H \setminus Y$, which completes the proof.∎

If the hypothesis of Theorem 3.1 is satisfied, we say that H *separates* X. In this case, obviously, H is a proper subgroup of G and $X \neq \{1\}$. Moreover, from Theorem 3.1 it follows that X is uniquely determined by H (in fact, X is the set difference of the smallest $\mathcal{A}$-subgroup of G containing H and the largest $\mathcal{A}$-subgroup of G contained in H). Denote by $\mathcal{H}_{sep}(\mathcal{A})$ the set of all subgroups of G each of which separates some basic set of the S-ring $\mathcal{A}$. Obviously, $\mathcal{H}_{sep}(\mathcal{A}) \cap \mathcal{H}(\mathcal{A}) = \emptyset$.

Corollary 3.2 *Let G be a finite group, $K \leq \mathrm{Aut}(G)$ and $\mathcal{A}$ a K-primitive K-invariant S-ring over G. Then* $\mathrm{rk}(\mathcal{A}) = 2$ *whenever $\mathcal{H}_{sep}(\mathcal{A})$ contains a K-invariant group.*

Proof. Immediately follows from Theorem 3.1 and the lemma below to be also used in Section 4.

Lemma 3.3 *In the conditions of Corollary 3.2 given a proper K-invariant subgroup H of G we have:*

$$H' \leq H \implies H' = \{1\}, \quad H' \geq H \implies H' = G \tag{9}$$

for any group $H' \in \mathcal{H}(\mathcal{A})$.

Proof. Let $H' \in \mathcal{H}(\mathcal{A})$. Set H'' to be the group generated by the groups $(H')^k$ for $k \in K$ if $H' \leq H$, and to be the intersection of the same groups if $H' \geq H$. Then $H'' \in \mathcal{H}_K(\mathcal{A})$ with $H'' \neq G$ in the first case and $H'' \neq \{1\}$ in the second. Thus we are done by the K-primitivity of $\mathcal{A}$.∎

4 Proofs of theorems

4.1. Proof of Theorem 1.5. Let us prove the injectivity of the mapping (1). It suffices to verify that the multiplication in a local commutative ring R on P is uniquely determined by the corresponding local pair $(K, e) = (K_R, 1_R)$. Let $r \in R$. If $r \in R^\times$, then $x \cdot r = x^{k(r)}$ for all x where $k(r)$ is the element of K induced by r. We observe that $k(r)$ depends only on r but not on the multiplication law in the ring R. (Indeed, $e^{k(r)} = r$ because $e = 1_R$, and due to the regularity there is the only element of K taking e to r.) If $r \notin R^\times$, then due to the locality of R, the element $e + r$ belongs to $R^\times$ and $x \cdot r = x \cdot (e + r) - x$. Thus the injectivity is proved.

To prove the surjectivity let (K, e) be a local pair on P. Denote by E the subring of the ring $\mathrm{End}(P)$ generated by K. Since the group K is abelian, the ring E is commutative. Let us show that the group homomorphism

$$E^+ \to P, \quad T \mapsto T(e) \tag{10}$$

is in fact an isomorphism. Suppose that $T(e) = 0$ (here and below we treat P as an additive group). Then

$$T(e^k) = (Tk)(e) = (kT)(e) = T(e)^k = 0$$

for all $k \in K$. On the other hand, from the definition of a local pair it follows that each element of $P \setminus O$ where $O = e^K$, is the difference (in P) of some elements of O. Thus $T(x) = 0$ for all $x \in P$, i.e. $T = 0$. So (10) is a monomorphism. Next, obviously the image of K with respect to (10) equals O. So (10) is an epimorphism because O generates P (see above).

Isomorphism (10) takes K to O and $E \setminus K$ to $P \setminus O$. Since $P \setminus O$ is a subgroup of P, $E \setminus K$ is a subgroup of the group E^+. This implies that $E \setminus K$ is an ideal of E ($E \setminus K$ is stable with respect to multiplication by K and hence by E). Since $K \subset E^\times$, we conclude that $E \setminus K$ is the only maximal ideal of E. Thus E is a local ring with $\mathrm{rad}(E) = E \setminus K$ and $E^\times = K$. Now using isomorphism (10) we come to a local ring R on P such that $\mathrm{rad}(R) = P \setminus O$, $R^\times = O$ and $1_R = e$. By the definition of R we have $T(x) = xT(e)$ for all $T \in E$ and $x \in P$. It follows that $K = K_R$, whence $(K, e) = (K_R, 1_R)$. Thus the surjectivity of (1) and the first part of the theorem are proved.

To complete the proof we observe first that any isomorphism of two local commutative rings on P induces an inner automorphism of the group $\mathrm{Aut}(P)$ taking the multiplications by the units of the first ring to those of the second one. Conversely, let R_1 and R_2 be local commutative rings on P such that $\sigma^{-1} K_{R_1} \sigma = K_{R_2}$ for some $\sigma \in \mathrm{Aut}(P)$. Since the multiplicative group of any ring transitively acts by multiplications on itself we assume without loss of generality that $(1_{R_1})^\sigma = 1_{R_2}$. Obviously, the automorphism σ induces a bijection $r \mapsto r_\sigma$ from $R_1^\times$ onto $R_2^\times$ such that

$$x^{k_1(r)\sigma} = x^{\sigma k_2(r_\sigma)}, \quad x \in P, \tag{11}$$

for all $r \in R_1^\times$ where $k_i(r')$ denotes the automorphism of P induced by the multiplication by $r' \in R_i^\times$ in the ring R_i $(i = 1, 2)$. Taking $x = 1_{R_1}$ we obtain that $r_\sigma = r^\sigma$ for all $r \in R_1^\times$. So (11) implies that

$$(x \cdot r)^\sigma = x^\sigma \cdot r^\sigma, \quad x \in R_1,\ r \in R_1^\times,$$

where the multiplication on the right-hand (resp. left-hand) side is meant in R_1 (resp. in R_2). Since $R_1 \setminus R_1^\times \subset R_1^\times - R_1^\times$, the last identity is true for all $r \in R_1$. Thus σ is a ring isomorphism from R_1 onto R_2 and we are done.■

Corollary 4.1 *Let P be a finite abelian p-group and $K \le \mathrm{Aut}(P)$ the first component of some local pair on P (i.e. K transitively acts on the set $P \setminus P_0$ for some group $P_0 < P$). Then*

(1) $\mathrm{Orb}(K_0, P \setminus P_0) = \{xP_0 :\ x \in P \setminus P_0\}$ *where K_0 is the Sylow p-subgroup of K.*

(2) *each orbit of K on $\widehat{P} \setminus \{1\}$ is the set difference of some K-invariant subgroup of $\widehat{P}$ and its maximal K-invariant subgroup; moreover $P_0^\perp$ is the smallest nontrivial K-invariant subgroup of $\widehat{P}$.*

Proof. By Theorem 1.5 one can assume that $P = R^+$, $K = K_R$ and $P_0 = \mathrm{rad}(R)$ for some commutative local ring R. Then K_0 is induced by the action of $1+\mathrm{rad}(R)$ on R^+ (see [10, p.355]), whence statement (1) follows. Next, for $r \in R$ and $\chi \in \widehat{R^+}$ set $\chi^r(x) = \chi(rx)$, $x \in R^+$. Obviously, $\chi^r \in \widehat{R^+}$ and $(\chi^r)^s = \chi^{rs}$ for all $r, s \in R$. Since $R \setminus \mathrm{rad}(R) = R^\times$ we have $\chi^R = \chi^{R^\times} \cup \chi^{\mathrm{rad}(R)}$ for all $\chi \in \widehat{R^+}$. If the character χ is not principal, then $\chi^{R^\times} \cap \chi^{\mathrm{rad}(R)} = \emptyset$. (Otherwise, $\chi((u-r)x) = 0$ for some $u \in R^\times$, $r \in \mathrm{rad}(R)$ and all $x \in R$. Since $u - v \in R^\times$, this implies that χ is principal.) Thus any orbit of $R^\times$ on $\widehat{R^+} \setminus \{0\}$ is of the form $\chi^{R^\times} = \chi^R \setminus \chi^{\mathrm{rad}(R)}$. Since, obviously, χ^R and $\chi^{\mathrm{rad}(R)}$ are $R^\times$-invariant subgroups of $\widehat{R^+}$ and $\chi^{R^\times} = \chi^{K_R}$, statement (2) follows.■

4.2. Proof of Theorem 1.2. In the conditions of Theorem 1.2 let $\mathcal{A}$ be a K-primitive K-invariant S-ring over the group G and P_0 a K-invariant subgroup of P for which $P \setminus P_0$ is an orbit of $K \cap \mathrm{Aut}(P)$. Obviously, $P_0 < P$. We consider three cases.

Case 1: $G = P$ and $P_0 \neq \{1\}$. The Sylow p-subgroup K_0 of K acts on the nontrivial p-group P_0 as an automorphism group. So there exists $x \in P_0 \setminus \{1\}$ fixed by K_0. We claim that the group $H = P_0$ separates the basic set $X = [x]$ of $\mathcal{A}$ (we observe that H is a proper K-invariant subgroup of G). Indeed, $X \cap H \neq \emptyset$ by obvious reason, $X \setminus H \neq \emptyset$ by the first implication of Lemma 3.3 for $H' = \langle X \rangle$, and $H \leq \mathrm{rad}(X \setminus H)$ by statement (1) of Corollary 4.1 because $X^{K_0} = X$ due to the K_0-invariance of $\mathcal{A}$ and the choice of X. Thus $H \in \mathcal{H}_{sep}(\mathcal{A})$. Since H is K-invariant, we are done by Corollary 3.2.

Case 2: $G = P$ and $P_0 = \{1\}$. Let $e \in P \setminus \{1\}$. From the hypothesis of the theorem it follows that (K, e) is a local pair on P such that $P \setminus e^K = \{1\}$. So by Theorem 1.5 without loss of generality we can assume that $G = \mathbb{F}^+$ and $K = K_\mathbb{F}$ where $\mathbb{F}$ is a field. Set L to be the setwise stabilizer of the basic set $[1_\mathbb{F}]$ of the S-ring $\mathcal{A}$ in the group K. Since $\mathcal{A}$ is K-invariant, we have $[r] = r[1_\mathbb{F}]$ for all $r \in \mathbb{F}^\times$. So every basic set of $\mathcal{A}$ is L-invariant. Moreover, if $x, y \in [r]$ where $r \in \mathbb{F}^\times$, then

$$[1_\mathbb{F}]x^{-1}y = [r]r^{-1}x^{-1}y = [x]x^{-1}yr^{-1} = [y]r^{-1} = [r]r^{-1} = [1_\mathbb{F}],$$

whence $x^{-1}y \in L$. Thus, $\mathcal{S}(\mathcal{A}) = \mathrm{Orb}(L, \mathbb{F})$ and we are done.

Case 3: $G \neq P$. Let $\widehat{\mathcal{A}}$ be the S-ring (over $\widehat{G}$) dual to $\mathcal{A}$. Since $\mathrm{rk}(\widehat{\mathcal{A}}) = \mathrm{rk}(\mathcal{A})$, it suffices to prove that $\mathrm{rk}(\widehat{\mathcal{A}}) = 2$. To do this we observe that by Theorem 2.2 the ring $\widehat{\mathcal{A}}$ is both K-invariant and K-primitive. Set $H = (P_0Q)^\perp$ with Q the product of all Sylow q-subgroups of G for $q \neq p$. Then H is a proper K-invariant subgroup of $\widehat{G}$. By Corollary 3.2 it suffices to verify that $H \in \mathcal{H}_{sep}(\widehat{\mathcal{A}})$. To do this we will show that the group H separates the basic set $X = [x]$ of $\widehat{\mathcal{A}}$ where $x \in \widehat{Q} \setminus \{1\}$ (such an x does exist because $Q \neq \{1\}$). Indeed, obviously $X \setminus H \neq \emptyset$. So it remains to prove that

$$X \cap H \neq \emptyset, \quad H \leq \mathrm{rad}(X \setminus H). \tag{12}$$

First we observe that the first formula of (12) is the consequence of the second one. Indeed, otherwise $X = X \setminus H$ and $\mathrm{rad}(X) \geq H$. However, H is a proper K-invariant subgroup of $\widehat{G}$. So by the second implication of Lemma 3.3 with G replaced by $\widehat{G}$ and $H' = \langle X \rangle$ we obtain that $\mathrm{rad}(X) = \widehat{G}$ which is impossible. Let us prove the second formula of (12). To do this set

$L = K \cap \mathrm{Aut}(P)$. Then from statement (2) of Corollary 4.1 with K replaced by L, it follows that

$$H \setminus \{1\} \in \mathrm{Orb}(L, \widehat{P}) \quad \text{and} \quad \mathrm{rad}(O) \geq H \quad \text{for all} \quad O \in \mathrm{Orb}(L, \widehat{P} \setminus H). \tag{13}$$

Moreover, since the ring $\widehat{\mathcal{A}}$ is L-invariant, the set X is L-invariant by the choice of x, and so the set $y\widehat{P} \cap X$ is also L-invariant for all $y \in \widehat{G}$. This implies that for each $y \in \widehat{Q}$ we have

$$(y\widehat{P} \cap X) \setminus H = y \cdot \bigcup_{O \in \mathcal{O}_y} O \tag{14}$$

for some $\mathcal{O}_y \subset \mathrm{Orb}(L, \widehat{P})$. From (13) it follows that the cardinality of any element of $\mathrm{Orb}(L, \widehat{P})$ other than $\{1\}$ and $H \setminus \{1\}$ is divided by p. By statement (2) of Lemma 2.1 this implies that $\{1\} \in \mathcal{O}_y$ iff $H \setminus \{1\} \in \mathcal{O}_y$. So using (13) once more we conclude that the radical of the left-hand side of (14) contains H. Thus $\mathrm{rad}(X \setminus H) \geq H$ and we are done.■

References

[1] E. Bannai, T. Ito, *Algebraic combinatorics. I*, Benjamin/Cummings, Menlo Park, CA, 1984.

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

[3] W. Burnside, *Theory of groups of finite order*, 2nd edition, 1911.

[4] P. J. Cameron, *Homogeneous Cayley objects*, Europ. J. Combinatorics, **21** (2000), 745–760.

[5] J. D. Dixon, B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, No. 163, Springer-Verlag New York, 1996.

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

[7] S. Evdokimov, I. Ponomarenko, *Characterization of cyclotomic schemes and normal Schur rings over a cyclic group*, Algebra and Analysis, **14** (2002), 2, 11–55.

[8] R. W. Goldbach, H. L. Claasen, *Cyclotomic schemes over finite rings*, Indag. Math. (N.S.), **3** (1992), 301–312.

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

[10] B. R. McDonald, *Finite rings with identity*, Pure and Applied Mathematics, Vol. 28, Marcel Dekker Inc., New York, 1974.

[11] I. Schur, *Zür Theorie der einfach transitiven Permutationgruppen*, S.-B. Preus Akad. Wiss. Phys.-Math. Kl., (1933), 598–623.

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