Алгебра и анализ
Том 19 (2007), № 6

St. Petersburg Math. J.
Vol. 19 (2008), No. 6, Pages 911–929
S 1061-0022(08)01027-3
Article electronically published on August 21, 2008

NORMAL CYCLOTOMIC SCHEMES OVER A FINITE COMMUTATIVE RING

S. EVDOKIMOV AND I. PONOMARENKO

To the centenary of the birth of D. K. Faddeev

Abstract. Cyclotomic association schemes over a finite commutative ring R with identity are studied. The main goal is to identify the normal cyclotomic schemes $\mathcal{C}$, i.e., those for which $\mathrm{Aut}(\mathcal{C}) \le A\Gamma L_1(R)$. The problem reduces to the case where the ring R is local, and in this case a necessary condition of normality in terms of the subgroup of $R^\times$ that determines $\mathcal{C}$ is given. This condition is proved to be sufficient for a large class of local rings including the Galois rings of odd characteristic.

§1. Introduction

Let R be a finite commutative ring[1] and K a subgroup of its multiplicative group $R^\times$. We denote by $\mathrm{Rel}(K,R)$ the set of all binary relations of the form $\{(x,y) \in R \times R : y - x \in rK\}$, $r \in R$. Then the pair

$$\mathrm{Cyc}(K,R) = (R, \mathrm{Rel}(K,R)) \tag{1}$$

is an association scheme on R. We call it a *cyclotomic scheme over* R corresponding to the group K. Clearly, $\mathrm{Cyc}(K,R)$ is the scheme of 2-orbits of the group $\Gamma(K,R) = \{\gamma_{a,b} : \ a \in K, b \in R\}$, where $\gamma_{a,b}$ is the permutation of the set R that takes x to $ax+b$. In particular, $\mathrm{Cyc}(K,R)$ is a Cayley scheme over the additive group R^+ of R (see Subsection 7.2), or a translation scheme in the sense of [1]. Moreover, multiplications by elements of $R^\times$ are Cayley isomorphisms of this scheme.

Cyclotomic schemes over a field were introduced by P. Delsarte (1973) in connection with algebraic coding theory. In [4] it was proved that any such scheme is uniquely determined up to isomorphism by its 3-dimensional intersection numbers. Cyclotomic schemes over rings were introduced and studied in [5] within the framework of duality theory for association schemes. We also mention the paper [7], where cyclotomic schemes over Galois rings of characteristic 4 were used to construct amorphous association schemes. In the present paper we are mainly interested in the automorphism groups of cyclotomic schemes.

Historically, the well-known Burnside theorem on permutation groups of prime degree can be viewed as the first result on automorphism groups of cyclotomic schemes. In fact, this theorem completely determines the structure of such automorphism groups for a prime field. In the case of an arbitrary finite field we have the following statement, which is a reformulation of an old number-theoretical result from [9] (see also [1, p. 389]).

2000 *Mathematics Subject Classification.* Primary 13M99.

Key words and phrases. Association scheme, cyclotomic schemes.

Partially supported by RFBR (grants nos. 07-01-00485, 05-01-00899, and 06-01-00471), and by NSH (grant no. 4329.2006.1).

[1] Throughout the paper all rings are assumed to have identity.

©2008 American Mathematical Society

Theorem 1.1. *Let $\mathcal{C}$ be a cyclotomic scheme over a finite field $\mathbb{F}$. Then $\mathrm{Aut}(\mathcal{C}) \le \mathrm{A\Gamma L}_1(\mathbb{F})$ whenever $\mathrm{rk}(\mathcal{C}) > 2$.*

For the cyclotomic schemes over the ring $\mathbb{Z}_n$ of integers modulo a positive integer n, no result of such a kind is true. Indeed, since any such scheme is a Cayley scheme over a cyclic group $\mathbb{Z}_n^+$, it can be treated, up to the language, as an S-ring over the same group. In accordance with [8, 4] every such S-ring can be constructed from normal S-rings and S-rings of rank 2 by means of tensor products and generalized wreath products (or wedge products in terms of [8]). Here by normal S-rings we mean exactly those that come from cyclotomic schemes $\mathcal{C}$ such that $\mathrm{Aut}(\mathcal{C}) \le \mathrm{A\Gamma L}_1(\mathbb{Z}_n) = \mathrm{AGL}_1(\mathbb{Z}_n)$. However, even among the S-rings corresponding to cyclotomic schemes there exist nonnormal ones (see [4, §6]).

The above discussion leads to the following definition, which is central for this paper.

Definition 1.2. We say that a cyclotomic scheme $\mathcal{C}$ over a finite commutative ring R is *normal* if $\mathrm{Aut}(\mathcal{C}) \le \mathrm{A\Gamma L}_1(R)$.

Our goal in this paper is to identify the normal cyclotomic schemes. Since any finite commutative ring is a direct product of local rings, the theorem below reduces the general case to the local case (and moreover, gives some product formula for two-point stabilizers of the automorphism group). Below, for the ring $R = \prod_i R_i$, we use the following notation. For a cyclotomic scheme $\mathcal{C} = \mathrm{Cyc}(K, R)$ we set $\mathcal{C}_i = \mathrm{Cyc}(K_i, R_i)$, where the group $K_i \le R_i^\times$ is defined by the formula $\varphi_i(K_i) = K \cap \varphi_i(R_i^\times)$; here φ_i is the monomorphism of $R_i^\times$ to $R^\times$ such that the jth component of $\varphi_i(x)$ is equal to x for $j = i$ and to 1_{R_j} for $j \ne i$.

Theorem 1.3. *Let $R = \prod_i R_i$ be a finite commutative ring and $\mathcal{C}$ a cyclotomic scheme over R. Then*

$$\mathrm{Aut}(\mathcal{C})_{u,v} = \prod_i \mathrm{Aut}(\mathcal{C}_i)_{u_i,v_i}, \tag{2}$$

where $u = 0_R$, $v = 1_R$, $u_i = 0_{R_i}$, and $v_i = 1_{R_i}$. In particular, the scheme $\mathcal{C}$ is normal if and only if the scheme $\mathcal{C}_i$ is normal for every i.

The following theorem gives a necessary condition for a cyclotomic scheme over a local ring to be normal. We do not know any example showing that this condition is not sufficient. Below we set $I_0 = \{x \in \mathrm{rad}(R) : x\,\mathrm{rad}(R) = \{0\}\}$.

Theorem 1.4. *Suppose that a cyclotomic scheme $\mathrm{Cyc}(K, R)$ over a finite local commutative ring R is normal. Let $K = K + I$ for some ideal I of R. Then $I = 0$ unless the order q of the residue field of R equals 2. Moreover, if $q = 2$, then $I \subset I_0$.*

Let R be a local commutative ring. Given a group $K \le R^\times$, we denote by $\mathcal{I}_K$ the set of all ideals I of R such that $K + I = K$, or equivalently, $1 + I \subset K$. It is convenient for us to formulate the following definition.

Definition 1.5. A group $K \le R^\times$ is said to be *pure* if $\mathcal{I}_K = \{0\}$.

If R is a field, then obviously any subgroup of $R^\times$ is pure. Moreover, Theorem 1.4 implies that for $q > 2$ the group K is pure whenever the scheme $\mathrm{Cyc}(K, R)$ is normal. It turns out that, for the Galois rings of odd characteristic that are not fields, this necessary condition of normality is also sufficient (for the definition of a Galois ring, see §2).

Theorem 1.6. *Let R be a Galois ring* (*but not a field*) *of odd characteristic. Then the scheme $\mathrm{Cyc}(K, R)$ is normal if and only if the group K is pure.*

Let $R = \mathrm{GR}(p^d, r)$ be a Galois ring of characteristic p^d with the residue field of cardinality $q = p^r$, where p is a prime. If $d > 1$ and $p > 2$ (the case of Theorem 1.6), then it is easily seen that a group $K \le R^\times$ is pure if and only if it does not contain the group $1 + p^{d-1}R$. On the other hand, if $d = 1$ (i.e., $R = \mathbb{F}$ is a field of cardinality q), then the condition $\mathrm{rk}(\mathcal{C}) = 2$ implies $\mathrm{Aut}(\mathcal{C}) = \mathrm{Sym}(\mathbb{F})$. Also, it is easily seen that $\mathrm{Sym}(\mathbb{F}) \le \mathrm{A\Gamma L}_1(\mathbb{F})$ if and only if $q \le 4$. Thus, after combining Theorems 1.6 and 1.1, we arrive at the following statement.

Theorem 1.7. *Let $R = \mathrm{GR}(p^d, r)$ with $p > 2$. Then a cyclotomic scheme $\mathrm{Cyc}(K, R)$ is normal if and only if one of the following conditions is fulfilled*:

1) *$d = 1$ and either $(p, r) = (3, 1)$ or $K \ne R^\times$;*
2) *$d > 1$ and $K \not\geq 1 + p^{d-1}R$.*

One of the ideas for proving the sufficiency part in Theorem 1.6 is to develop a reduction technique for cyclotomic schemes over an arbitrary local ring. For an ideal I of such a ring R, the scheme $\mathrm{Cyc}(\pi_I(K), R/I)$, where $\pi_I : R \to R/I$ is the natural epimorphism, can be treated as a factor-scheme of the scheme $\mathrm{Cyc}(K, R)$ (see Subsection 2.2). This simple observation is used in the proof of Theorem 6.1, a straightforward consequence of which is the following reduction statement. Below we set $\pi_0 = \pi_{I_0}$.

Theorem 1.8. *Let R be a finite local commutative ring, $K \le R^\times$ a pure group, $\mathcal{C} = \mathrm{Cyc}(K, R)$, and $\mathcal{C}' = \mathrm{Cyc}(K', R')$, where $K' = \pi_0(K)$ and $R' = R/I_0$. Then the scheme $\mathcal{C}$ is normal whenever so is the scheme $\mathcal{C}'$.*

Unfortunately, in general the group K' may fail to be pure (even if R is a Galois ring of even characteristic), so that Theorem 1.8 cannot be used for a direct inductive proof of the normality of the scheme $\mathcal{C}$. However, if R is a Galois ring of odd characteristic, then K' is pure, and Theorem 1.6 reduces to the case where $\mathrm{rad}(R)^2 = \{0\}$. Thus, by Theorem 1.1, it suffices to prove the following statement, which is a special case of Theorem 6.4.

Theorem 1.9. *Let R be a finite local commutative ring other than a field and such that $\mathrm{rad}(R)^2 = \{0\}$. Then the scheme $\mathrm{Cyc}(K, R)$ is normal whenever the group K is pure.*

Theorems 6.1 and 6.4, which lead to Theorems 1.8 and 1.9, are proved by using the S-ring technique. Namely, for a cyclotomic scheme $\mathcal{C}$ over R, together with the usual (addition) S-ring over R^+ corresponding to $\mathcal{C}$ we consider its *multiplication* S-ring $\mathcal{A}$ over $R^\times$ (see §4). Everything reduces to the case of a pure group $K \le \mathcal{T}\mathcal{U}_0$, where $\mathcal{T}$ is the Teichmüller subgroup of $R^\times$ and $\mathcal{U}_0 = 1 + I_0$. Then the group $\mathrm{Aut}(\mathcal{C})_{u,v}$ acts faithfully on $R^\times$, and the image of this action equals $\mathrm{Aut}(\mathcal{A})$. Moreover, in this case the S-ring $\mathcal{A}$ contains the groups $\mathcal{T}$ and $\mathcal{U} = 1 + \mathrm{rad}(R)$, and becomes trivial after adding to it the cosets by any of these groups (§5). This enables us to prove that the group $\mathrm{Aut}(\mathcal{C})$ normalizes the group $\mathrm{AGL}_1(R)$ (Theorems 4.4 and 7.2). The latter means that $\mathrm{Aut}(\mathcal{C}) \le \mathrm{A\Gamma L}_1(R)$ (Lemma 2.1), i.e., the scheme $\mathcal{C}$ is normal.

Actually, the technique that we develop permits us to obtain the following sufficient condition of normality for an arbitrary finite local commutative ring R: the scheme $\mathrm{Cyc}(K, R)$ is normal whenever the group K is strongly pure (Theorem 6.2). (Here we say that a group $K \le R^\times$ is *strongly pure* if it is pure and the group $\pi_0(K)$ is strongly pure unless R is a field.) It should be noted that this condition is not necessary: it can be proved that the cyclotomic scheme corresponding to the group K in the example at the beginning of Subsection 6.2 is normal.

In some cases, somewhat more can be said about the automorphism group of a normal cyclotomic scheme $\mathcal{C} = \mathrm{Cyc}(K, R)$, where R is a finite local commutative ring. For instance, if $K \le \mathcal{T}$ and R is not a field, then

$$\mathrm{Aut}(\mathcal{C}) \le \mathrm{AGL}_1(R)$$

(statement 1 of Theorem 6.5). This inclusion remains true also in some other cases. In particular, this is so if the group K is strongly pure, and either $K \le \mathcal{U}$ or the residue field $\mathbb{F}$ of R is prime (statements 2 and 3 of Theorem 6.5). The reason for this is that in both cases the natural mapping

$$\mathrm{Aut}_{\mathcal{C}}(R) \to \mathrm{Aut}_{\mathcal{C}}(\mathbb{F})$$

is a monomorphism and the group $\mathrm{Aut}_{\mathcal{C}}(\mathbb{F})$ is trivial; here, by definition, $\mathrm{Aut}_{\mathcal{C}}(R)$ (respectively, $\mathrm{Aut}_{\mathcal{C}}(\mathbb{F})$) consists of all automorphisms of R (respectively, $\mathbb{F}$) that are automorphisms of $\mathcal{C}$ (respectively, the factor-scheme of $\mathcal{C}$ on $\mathbb{F}$); see Theorem 6.2. It should be noted that, in general, the kernel of the quotient homomorphism $\mathrm{Aut}(R) \to \mathrm{Aut}(\mathbb{F})$ is not trivial. For instance, for $R = \mathbb{F}[X]/(X^2)$ the group $\mathrm{Aut}(R)$ is isomorphic to the semidirect product of $R^\times$ by $\mathrm{Aut}(\mathbb{F})$ (indeed, the mapping $a + b\pi \mapsto a^\sigma + b^\sigma \alpha\pi$, where $a, b \in \mathbb{F}$ and $\pi = X \mod X^2$, is an automorphism of R for any $\sigma \in \mathrm{Aut}(\mathbb{F})$ and $\alpha \in R^\times$).

All terms and results concerning permutation groups can be found in the monographs [14, 15, 2]. To make the paper possibly self-contained, we cite the background on schemes and Schur rings in §7 (see [3] for details). All necessary properties of finite rings and cyclotomic schemes can be found in §2. The proofs of Theorems 1.3 and 1.4 are contained in §3; they are based on the ideas of [4], where the case of $R = \mathbb{Z}_n$ was treated. The multiplication S-ring of a cyclotomic scheme is introduced and studied in §§4 and 5. §6 contains the proofs of Theorems 6.1, 6.2, and 1.6.

Notation. As usual, $\mathbb{Z}$ denotes the ring of rational 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.

Given groups $A \le R^\times$ and $B \le R^+$ with $AB = B$, we denote by $\Gamma(A, B)$ the group $\{\gamma_{a,b} : \ a \in A, \ b \in B\}$, where $\gamma_{a,b}$ is the permutation of R taking x to $ax + b$. We omit B whenever $B = 0$, and set $\mathrm{AGL}_1(R) = \Gamma(R^\times, R^+)$ and $\mathrm{GL}_1(R) = \Gamma(R^\times)$.

By $\mathrm{A\Gamma L}_1(R)$ we denote the group of all permutations of R of the form $x \mapsto ax^\sigma + b$, where $a \in R^\times$, $b \in R$, and $\sigma \in \mathrm{Aut}(R)$. This group is a semidirect product of the groups $\mathrm{AGL}_1(R)$ and $\mathrm{Aut}(R)$ (with the natural action of the latter group on the former).

The group of all permutations of a set V is denoted by $\mathrm{Sym}(V)$.

In a natural way, each permutation $f \in \mathrm{Sym}(V)$ $(v \mapsto v^f)$ determines a permutation $R \mapsto R^f$ of the set of all relations on V. For an equivalence relation E on a set $X \subset V$ such that $E^f = E$, the permutation f induces a permutation $f^{X/E} \in \mathrm{Sym}(X/E)$. If E is Γ-invariant for some group $\Gamma \le \mathrm{Sym}(V)$, then all such permutations for $f \in \Gamma$ form a group denoted by $\Gamma^{X/E}$. If all classes of E are singletons, the set X/E is identified with X.

For a group G, the permutation group on the set G determined by the right multiplications is denoted by G_{right}.

For $\Gamma \le \mathrm{Sym}(V)$ and $X_1, \ldots, X_s \subset V$, we set $\Gamma_{X_1,\ldots,X_s} = \{\gamma \in \Gamma : X_i^\gamma = X_i \text{ for all } i\}$. If $X_i = \{v_i\}$, the brackets are omitted. If the X_i's are the classes of an equivalence relation E on V, we set $\Gamma_E = \Gamma_{X_1,\ldots,X_s}$.

§2. Finite commutative rings and cyclotomic schemes

2.1. Finite rings. It is well known (see, e.g., [10, Theorem 6.2]) that any finite commutative ring is a direct product of local rings. Let R be a finite local commutative ring. Then $R = \mathrm{rad}(R) \cup R^\times$, the ideal $\mathrm{rad}(R)$ is maximal, and the characteristic of R is a power of the characteristic of its residue field $\mathbb{F} = R/\operatorname{rad}(R)$. Moreover,

$$R^\times = \mathcal{T} \times \mathcal{U}, \tag{3}$$

where $\mathcal{T}$ is the Teichmüller group and $\mathcal{U}$ is the group of principal units. The group $\mathcal{T}$ is a cyclic group of order $q-1$, and the group $\mathcal{U} = 1 + \operatorname{rad}(R)$ is an Abelian p-group; here q and p are the order and the characteristic of the field $\mathbb{F}$.

Let $I \subset \operatorname{rad}(R)$ be an ideal of R. Then the quotient ring R/I is local and $(R/I)^\times = \pi_I(R^\times)$, where $\pi_I : R \to R/I$ is the natural epimorphism. The set $1 + I$ is a subgroup of $\mathcal{U}$. Moreover, if $I \subset I_0$, where $I_0 = \{x \in \operatorname{rad}(R) : x \operatorname{rad}(R) = 0\}$, then the mapping $r \mapsto 1 + r$ induces an isomorphism of the additive group of I onto $1 + I$. Below we set $\mathcal{U}_0 = 1 + I_0$.

We say that the local ring R is *Galois* if $\operatorname{rad}(R) = pR$.[2] For any positive integers n, r, there exists a unique (up to isomorphism) Galois ring of characteristic p^n with $q = p^r$; it is denoted by $\operatorname{GR}(p^n, r)$. We observe that $\operatorname{GR}(p, r)$ is a field of order p^r and $\operatorname{GR}(p^n, 1) \cong \mathbb{Z}_{p^n}$. Each proper ideal of the Galois ring $\operatorname{GR}(p^n, r) = R$ is of the form $p^i R$, $i = 1, \dots, n$, and the corresponding quotient ring is isomorphic to $\operatorname{GR}(p^i, r)$. We also note that the homomorphism $\operatorname{Aut}(R) \to \operatorname{Aut}(\mathbb{F})$ induced by the epimorphism $\pi_{\operatorname{rad}(R)}$ is in fact an isomorphism (see [13]).

Generally, the structure of the group $\operatorname{Aut}(R)$ is unclear even in the local case. Below we give a sufficient condition for a permutation of R to belong to this group.

Lemma 2.1. *Let R be a commutative ring, and suppose that a group $K \le R^\times$, viewed as a set, generates the group R^+. Let $\gamma \in \operatorname{Sym}(R)$ be a permutation such that*

$$0^\gamma = 0, \quad 1^\gamma = 1, \quad \gamma^{-1}\Gamma(K, R)\gamma = \Gamma(K, R).$$

Then $\gamma \in \operatorname{Aut}(R)$.

Proof. The condition $\gamma^{-1}\Gamma(K, R)\gamma = \Gamma(K, R)$ implies that, given $(a, b) \in K \times R$, there exists $(a_\gamma, b_\gamma) \in K \times R$ such that $\gamma^{-1}\gamma_{a,b}\gamma = \gamma_{a_\gamma, b_\gamma}$, or equivalently,

$$(ax^{\gamma^{-1}} + b)^\gamma = a_\gamma x + b_\gamma, \quad x \in R. \tag{4}$$

Since γ leaves both 0 and 1 fixed, for $x = 0$ this shows that $b_\gamma = b^\gamma$ for all $b \in R$, whereas for $(x, b) = (1, 0)$ this yields $a_\gamma = a^\gamma$ for all $a \in K$. Therefore, for $a = 1$ and $b = 0$ formula (4) gives

$$(x + b)^\gamma = x^\gamma + b^\gamma, \quad (x, b) \in R \times R, \quad \text{and} \quad (ax)^\gamma = a^\gamma x^\gamma, \quad (a, x) \in K \times R, \tag{5}$$

respectively. In particular, $\gamma \in \operatorname{Aut}(R^+)$, and consequently (since K generates R^+), the second relation is valid for all $a \in R$. Thus, $\gamma \in \operatorname{Aut}(R)$. □

Lemma 2.1 will be applied in §6 to a local ring R and $K = R^\times$. In this case $\langle K \rangle = R^+$, because any element of the set $\operatorname{rad}(R) = R \setminus R^\times$ is the difference of two units. The lemma is also employed to prove the following statement, in which $s = \gamma_{-1,1}$ is the involution taking x to $-x + 1$.

Corollary 2.2. *Let $\mathbb{F}$ be a field and $\gamma \in \operatorname{Sym}(\mathbb{F})$ a permutation leaving fixed both 0 and 1. Suppose that γ normalizes the two groups $\Gamma(\mathbb{F}^\times)$ and $s\Gamma(\mathbb{F}^\times)s$. Then $\gamma \in \operatorname{Aut}(\mathbb{F})$.*

Proof. A straightforward computation shows that $\gamma_{a^{-1},0} s \gamma_{a,0} s = \gamma_{1,1-a}$ for all $a \in \mathbb{F}^\times$. Assuming without loss of generality that $|\mathbb{F}| > 2$, we see that the group $\langle \Gamma(\mathbb{F}^\times), s\Gamma(\mathbb{F}^\times)s \rangle$ contains the group $\Gamma(1, \mathbb{F}^+)$ and hence is equal to $\Gamma(\mathbb{F}^\times, \mathbb{F}^+)$. Thus, we are done by Lemma 2.1 with $R = \mathbb{F}$ and $K = \mathbb{F}^\times$. □

[2] This is one of the equivalent definitions given in [10].

2.2. Cyclotomic schemes. Let $\mathcal{C} = \mathrm{Cyc}(K,R)$ be a cyclotomic scheme over a finite commutative ring R (see (1)). Since, obviously, each relation from the set $\mathrm{Rel}(K,R)$ is R^+_{right}-invariant, $\mathcal{C}$ is a Cayley scheme over the group R^+. The corresponding S-ring is called the *addition S-ring* of $\mathcal{C}$. Each basic set of it is of the form rK with $r \in R$. It follows that any ideal I of R is an $\mathcal{A}$-subgroup (indeed, $I = \bigcup_{r\in I} rK$). So, due to the bijection between the sets $\mathcal{H}(\mathcal{A})$ and $\mathcal{E}(\mathcal{C})$ (see Subsection 7.2), we have the following statement.

Lemma 2.3. *For any ideal I of the ring R, the equivalence relation*

$$E(I) = \bigcup_{X\in R/I} X \times X$$

belongs to the set $\mathcal{E}(\mathcal{C})$. In particular, this relation is $\mathrm{Aut}(\mathcal{C})$-invariant.

Since, obviously, the set $\mathrm{Rel}(K,R)$ is $\mathrm{AGL}_1(R)$-invariant, and the stabilizer of the point $u = 0$ in the group $\mathrm{AGL}_1(R)$ is equal to $\mathrm{GL}_1(R)$, we have

$$(6) \qquad \mathrm{AGL}_1(R) \le \mathrm{Iso}(\mathcal{C}), \quad \mathrm{GL}_1(R) \le \mathrm{Iso}(\mathcal{C}_u),$$

where $\mathcal{C}_u$ is the u-extension of $\mathcal{C}$ (see Subsection 7.1). The following easy statement gives a simple criterion of normality.

Lemma 2.4. *The scheme $\mathcal{C}$ is normal if and only if $\mathrm{Aut}(\mathcal{C})_{u,v} \le \mathrm{Aut}(R)$, where $u = 0$ and $v = 1$.*

Proof. The "only if" part follows from the obvious identity $\mathrm{A\Gamma L}(R)_{u,v} = \mathrm{Aut}(R)$. Conversely, by the orbit-stabilizer theorem [2, Theorem 1.4A], we have

$$[\mathrm{Aut}(\mathcal{C}) : \mathrm{Aut}(\mathcal{C})_{u,v}] = |R||K| = |\Gamma(K,R)|.$$

Since $\Gamma(K,R) \le \mathrm{Aut}(\mathcal{C})$, we conclude that $\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(\mathcal{C})_{u,v}\Gamma(K,R)$, and the "if" part follows. □

Now, let the ring R be local, and let $I \subset \mathrm{rad}(R)$ be an ideal of R. Then $R/E(I) = R/I$, the equivalence relation $E(I)$ is $\Gamma(K,R)$-invariant, and $\Gamma(K,R)^{R/E(I)} = \Gamma(\pi_I(K), R/I)$. This implies that

$$(7) \qquad \mathrm{Cyc}(K,R)_{R/E(I)} = \mathrm{Cyc}(\pi_I(K), R/I),$$

i.e., the factor-scheme of $\mathcal{C}$ modulo $E(I)$ can naturally be treated as a cyclotomic scheme over the ring R/I.

The following theorem on cyclotomic schemes with pure groups (see Definition 1.5) will be used in §6.

Theorem 2.5. *Let $\mathcal{C} = \mathrm{Cyc}(K,R)$ be a cyclotomic scheme over a local commutative ring R. If the group K is pure, then*

$$\mathcal{C}_{E_0} \ge \mathrm{Cyc}(U_0, R),$$

where $U_0 = K \cap \mathcal{U}_0$ and $E_0 = E(I_0)$.

Proof. First, we prove that if $S \in \mathrm{Rel}(K,R)$ and $S_0 \in \mathrm{Rel}(U_0,R)$ are the relations corresponding to the sets xK and xU_0 (respectively), then

$$(8) \qquad S \cap ((a + I_0) \times (b + I_0)) = S_0 \cap ((a + I_0) \times (b + I_0)), \qquad a, b \in R,$$

whenever $x \in R^\times$ and the right-hand side is nonempty. Let (y,z) belong to the left-hand side. Then $z - y \in (xK) \cap (b - a + I_0)$. On the other hand, by assumption, there exists (y_0, z_0) belonging to the right-hand side. Then $z_0 - y_0 \in (xU_0) \cap (b - a + I_0)$. Thus, $(z - y)/(z_0 - y_0) \in K \cap (1 + I_0) = U_0$, so that $z - y$ belongs to the right-hand side. The reverse inclusion is obvious.

We denote by $\mathcal{M}$ the set of all relations in $\mathrm{Rel}(U_0, R)$ corresponding to the sets xU_0 with $x \in R^\times$. Then (8) implies that $\mathcal{M} \subset \mathcal{R}^*(\mathcal{C}_{E_0})$, whence $[\mathcal{M}] \le \mathcal{C}_{E_0}$. Thus, it suffices to verify that $[\mathcal{M}] = \mathcal{C}_{E_0}$, or equivalently, that the addition S-ring $\mathcal{A}$ of the scheme $\mathrm{Cyc}(U_0, R)$ is generated (as an S-ring) by the sets xU_0, $x \in R^\times$. For this, we prove that

$$xU_0 = \bigcap_{t \in \mathcal{T}} ((x-t)U_0 + tU_0), \quad x \in \mathrm{rad}(R). \tag{9}$$

Obviously, the left-hand side of (9) is contained in the right-hand side. Conversely, let $t \in \mathcal{T}$ and $x \in \mathrm{rad}(R)$. Then, since $U_0 = 1 + H$, where H is a subgroup of the additive group of the ideal I_0 and $xH = 0$, we have

$$(x-t)U_0 + tU_0 = (x-t)(1+H) + t(1+H) = x - t + tH + t + tH = x + tH.$$

It follows that if y belongs to the right-hand side of (9), then $y \in x + tH$ for all $t \in \mathcal{T}$. On the other hand, $\bigcap_{t \in \mathcal{T}} tH = 0$ by the purity of the group U_0. Thus, $y = x$ and we are done. □

§3. Proof of Theorems 1.3 and 1.4

3.1. Proof of Theorem 1.3. Set $\Gamma = \mathrm{Aut}(\mathcal{C})$ and $\Gamma_i = \mathrm{Aut}(\mathcal{C}_i)$. To prove relation (2), first we verify that $\prod_i (\Gamma_i)_{u_i,v_i} \le \Gamma_{u,v}$. For this, we observe that the obvious inclusion $\prod_i K_i \le K$ implies that

$$\prod_i \Gamma(K_i, R_i) \le \Gamma(K, R).$$

Therefore, $\bigotimes_i \mathcal{C}_i \ge \mathcal{C}$, whence $\prod_i \Gamma_i \le \Gamma$. Since, obviously, $\prod_i (\Gamma_i)_{u_i,v_i} = (\prod_i \Gamma_i)_{u,v}$, we are done. To prove the reverse inclusion, we observe that, by Lemma 2.3 with $I = R_i$, R_i is a Γ_u-invariant set for all i. For $\gamma \in \Gamma_u$, let γ_i denote the restriction of γ to R_i. Then for any element $x = (\dots, x_i, \dots)$ of the set $R = \prod_i R_i$ we have

$$x^\gamma = (\dots, x_i^{\gamma_i}, \dots). \tag{10}$$

Indeed, by Lemma 2.3 with $I = \prod_{j \ne i} R_j$, the equivalence $E(I)$ is Γ_u-invariant. On the other hand, obviously, each class of this equivalence contains a unique element of R_i. Thus, the ith component of x^γ equals $x_i^{\gamma_i}$ by the definition of γ_i. Since $\Gamma_{u,v,R_i,v+R_i} = \Gamma_{u,v}$, from (10) it follows that

$$\Gamma_{u,v} \le \prod_i (\Gamma_{u,v})^{R_i} = \prod_i (\Gamma_{u,v,R_i,v+R_i})^{R_i} \le \prod_i ((\Gamma_{R_i,v+R_i})^{R_i})_{u_i,v_i}.$$

Thus the inclusion $\prod_i (\Gamma_i)_{u_i,v_i} \ge \Gamma_{u,v}$ and hence formula (2) are easy consequences of Lemma 3.1 below. Indeed, since the groups Γ_i and $\Gamma(K_i, R_i)$ are 2-equivalent (i.e., have one and the same set of 2-orbits) and the group Γ_i is 2-closed (i.e., is largest in the class of groups 2-equivalent to it), it follows that $(\Gamma_{R_i,v+R_i})^{R_i} \le \Gamma_i$.

Lemma 3.1. *The groups $(\Gamma_{R_i,v+R_i})^{R_i}$ and $\Gamma(K_i, R_i)$ are 2-equivalent for all i.*

Proof. Set $X = R_i$ and $Y = v + R_i$. Since $\Gamma(K_i, R) \le \Gamma$ and $\Gamma(K_i, R_i) = (\Gamma(K_i, R)_{X,Y})^X$, it follows that $\Gamma(K_i, R_i) \le \Delta^X$ where $\Delta = \Gamma_{X,Y}$. Therefore, it suffices to check that each 2-orbit of the group Δ^X is contained in some 2-orbit of the group $\Gamma(K_i, R_i)$, or equivalently, that each orbit of the group $(\Delta^X)_{u_i} = (\Delta_u)^X$ is contained in some orbit of the group $\Gamma(K_i, R_i)_{u_i} = K_i$ (we have used the fact that the group Δ^X contains a transitive subgroup $\Gamma(\{v_i\}, R_i)$). However, obviously, each orbit of the group $(\Delta_u)^X$ meets some orbit of the group K_i. So, we only need to check that the latter orbit is Δ_u-invariant. For this, we shall use the following statement.

Lemma 3.2. *For each i and for any $a, r \in R$ such that $r_j \in R_j^\times$ for all $j \ne i$, there exists $s \in K$ for which*

$$(a + rK) \cap R_i = a_i + r_i s_i K_i$$

whenever the set on the left-hand side is nonempty.

Proof. The definition of the monomorphism φ_i shows that $K = \bigcup_s sK'$, where $K' = \varphi_i(K_i)$ and s runs over a full system of representatives of K modulo K'. Moreover, for all $s, t \in K$ we have

$$sK' = tK' \ \Leftrightarrow\ s_j = t_j \text{ for all } j \ne i. \tag{11}$$

Also,

$$a + rK = \bigcup_s (a + rsK') \tag{12}$$

for all $a, r \in R$. Suppose that the set $(a + rsK') \cap R_i$ is nonempty for some a, r, and s. Then $a_j + r_j s_j = 0$ for all $j \ne i$. Therefore, if r is as in the assumptions of the lemma, then the elements s_j for $j \ne i$, and with them the coset sK' by (11), are uniquely determined by a and r. Thus, in this case, formula (12) implies that

$$(a + rK) \cap R_i = (a + rsK') \cap R_i = a_i + r_i s_i K_i.$$

Since the set $(a + rK) \cap R_i$ is nonempty if and only if so is the set $(a + rsK') \cap R_i$, we are done. □

We continue the proof of Lemma 3.1. We consider the identity of Lemma 3.2 with $a = v_i - v$ and $r = v - v_i$ and translate it by $v - v_i$; since $X + (v - v_i) = Y$, we obtain

$$rK \cap Y = \{v - v_i\}.$$

Let S denote the basis relation of the scheme $\mathcal{C}$ corresponding to r. Since the sets $rK = S_{\text{out}}(u)$ and Y are Δ_u-invariant, so is the set $\{v - v_i\}$. Applying Lemma 3.2 with $a = v - v_i$ and with r such that the set $(v - v_i + rK) \cap X$ is nonempty and $r_j \in R_j^\times$ for all $j \ne i$, we get

$$(v - v_i + rK) \cap X = r_i s_i K_i$$

for some $s \in K$. Since the sets $v - v_i + rK = S_{\text{out}}(v - v_i)$ and X are Δ_u-invariant, we conclude that so is the set $r_i s_i K_i$. Next, the sets $r_i s_i K_i$ cover X when r runs over the elements of R such that the set $(v - v_i + rK) \cap X$ is nonempty and $r_j \in R_j^\times$ for all $j \ne i$ (for instance, we can take $r_j = -1$ for $j \ne i$ and take r_i to be an arbitrary element of the ring R_i). So, any orbit of the group K_i is Δ_u-invariant. □

Thus, the first part of Theorem 1.3 is proved. The second part follows from the first and Lemma 2.4 applied to the scheme $\mathcal{C}$ and all schemes $\mathcal{C}_i$.

3.2. Proof of Theorem 1.4. Without loss of generality we assume that R is not a field. Then the required statement is a straightforward consequence of the following lemma, the idea of the proof of which is taken from [4, Subsection 5.3].

Lemma 3.3. *Under the conditions of Theorem* 1.4*, suppose that R is not a field and that $K + I = K$ for some nonzero ideal I of R. Then $|R/\operatorname{rad}(R)| = 2$ and, moreover, $I \subset I_0$.*

Proof. For each $k \in 1 + I$, we define a permutation f_k of the set R by

$$x^{f_k} = \begin{cases} kx & \text{if } x \in \mathcal{U}, \\ x & \text{otherwise.} \end{cases} \tag{13}$$

First, we show that $f_k \in \mathrm{Aut}(\mathcal{C})$, where $\mathcal{C} = \mathrm{Cyc}(K, R)$. It suffices to verify that if $x - y \in rK$, then $x^{f_k} - y^{f_k} \in rK$ for all $x, y, r \in R$. This is obvious for $x, y \notin \mathcal{U}$, and follows from the inclusion $1 + I \leq K$ for $x, y \in \mathcal{U}$. Next, if $x \in \mathcal{U}$ and $y \notin \mathcal{U}$, then

$$x^{f_k} - y^{f_k} = kx - y = k(x-y) + (k-1)y \in rK + I = rK + rI = r(K+I) = rK,$$

and we are done. The remaining case is treated similarly.

The normality of the scheme $\mathcal{C}$ implies that $x^{f_k} = ax^\sigma + b$ for some $a \in R^\times$, $b \in R$, $\sigma \in \mathrm{Aut}(R)$, and for all $x \in R$. Since $0^{f_k} = 0$ and $1^{f_k} = k$, we conclude that $b = 0$ and $a = k$. Thus, $x^{f_k} = kx^\sigma$, $x \in R$. By the choice of k, this implies that σ leaves fixed each element of $\mathcal{U}$ (and hence, each element of $\mathrm{rad}(R)$) and each set $x + \mathrm{rad}(R)$. Since $\mathcal{T}^\sigma = \mathcal{T}$ and $|\mathcal{T} \cap (x + \mathrm{rad}(R))| = 1$ for $x \in R^\times$, we see that σ leaves fixed each element of $\mathcal{T}$. Thus, $\sigma = \mathrm{id}_R$, whence $x^{f_k} = kx$ for all $x \in R$. Comparing this with (13), we obtain

$$Ix = 0, \quad x \in R \setminus \mathcal{U}. \tag{14}$$

Since $\mathrm{rad}(R) \subset R \backslash \mathcal{U}$, we have $I \subset I_0$. To complete the proof, suppose that $|R/\mathrm{rad}(R)| > 2$. Then $R^\times \setminus \mathcal{U} \neq \varnothing$ and (14) implies that $Ix = 0$ for some $x \in R^\times$. Thus, $I = 0$, which contradicts the choice of I. □

§4. Multiplication S-ring of a cyclotomic scheme

Let $\mathcal{C} = \mathrm{Cyc}(K, R)$ be a cyclotomic scheme over a finite commutative ring R. Then, by (6), we have $\Gamma(R^\times) \leq \mathrm{Iso}(\mathcal{C}_u)$, where $\mathcal{C}_u$ is the u-extension of $\mathcal{C}$ with $u = 0_R$. Since $\Delta(R^\times)$ is a relation of the scheme $\mathcal{C}_u$ and the set $R^\times$ is $\Gamma(R^\times)$-invariant, this implies that $R^\times_{\mathrm{right}} = \Gamma(R^\times)^{R^\times}$ is a subgroup of $\mathrm{Iso}((\mathcal{C}_u)_{R^\times})$. Therefore, in accordance with §7, we can consider the scheme

$$\mathcal{C}' = ((\mathcal{C}_u)_{R^\times})^{R^\times_{\mathrm{right}}}.$$

Obviously, $R^\times_{\mathrm{right}} \leq \mathrm{Aut}(\mathcal{C}')$. Thus, $\mathcal{C}'$ is a Cayley scheme over the group $R^\times$. We denote by $\mathcal{A} = \mathcal{A}(K, R)$ the S-ring over $R^\times$ corresponding to the scheme $\mathcal{C}'$.

Definition 4.1. The S-ring $\mathcal{A}$ is called the multiplication S-ring of the scheme $\mathcal{C}$.

The multiplication S-ring of a cyclotomic scheme over a field was introduced and studied in [4].

Theorem 4.2. *The set $\mathcal{S}^*(\mathcal{A})$ contains the sets rK for all $r \in R^\times$ and the sets $(1 + rK) \cap R^\times$ for all $r \in R$.*

Proof. Suppose $r \in R^\times$ and $C = rK$. Since each coset $C' \in R^\times/K$ is a neighborhood of the point u in the basis relation of $\mathcal{C}$ corresponding to C', the set $\Delta(C')$ is a relation of the scheme $\mathcal{C}_u$. Therefore, the latter scheme also contains the relation T defined by formula (4) with $G = R^\times$. Thus, $C \in \mathcal{S}^*(\mathcal{A})$ (the relation T is $R^\times_{\mathrm{right}}$-invariant and $T_{\mathrm{out}}(1) = C$).

To prove the second statement, take $r \in R$ and set $X = (1 + rK) \cap R^\times$. It is easily seen that the smallest relation S of the scheme $\mathcal{C}_u$ that contains $\{1\} \times X$ is a subset of $K \times R^\times$. Since all relations of $\mathcal{C}_u$ are $\Gamma(K)$-invariant, we see that $S_{\mathrm{out}}(1) = X$. Moreover, by the definition of the scheme $\mathcal{C}'$, the smallest relation S' of it containing S is the union of all relations $Sr' = \{(sr', tr') : (s,t) \in S\}$ with $r' \in R^\times$. However, $S'_{\mathrm{out}}(1) = S_{\mathrm{out}}(1) = X$, so that $X \in \mathcal{S}^*(\mathcal{A})$, and we are done. □

The following theorem establishes some relationship between the automorphism group of the scheme $\mathcal{C}$ and that of the S-ring $\mathcal{A}$. We put $v = 1_R$.

Theorem 4.3. *In the above notation,*

1) *the mapping $f \mapsto f^{R^\times}$ induces a homomorphism from* $\mathrm{Aut}(\mathcal{C}_{u,v})$ *to* $\mathrm{Aut}(\mathcal{A})$*, and*
2) *if R is a field, then the mapping in statement* 1) *is an isomorphism.*

Proof. Being a neighborhood of the point u in a relation of the scheme $\mathcal{C}$, the set $R^\times$ is $\mathrm{Aut}(\mathcal{C}_u)$-invariant. Therefore, the mapping $f \mapsto f^{R^\times}$ induces a homomorphism from $\mathrm{Aut}(\mathcal{C}_u)$ to $\mathrm{Aut}(\mathcal{C}_u)^{R^\times}$. Moreover,

$$\mathrm{Aut}(\mathcal{C}_u)^{R^\times} \leq \mathrm{Aut}((\mathcal{C}_u)_{R^\times}) \leq \mathrm{Aut}(\mathcal{C}').$$

Thus, statement 1) is true because $\mathrm{Aut}(\mathcal{C}')_v = \mathrm{Aut}(\mathcal{A})$ by the definition of the group $\mathrm{Aut}(\mathcal{A})$. To prove statement 2), we observe that the restriction homomorphism from $\mathrm{Aut}(\mathcal{C}_u)$ to $\mathrm{Aut}((\mathcal{C}_u)_{R^\times})$ is an isomorphism that induces an isomorphism from $\mathrm{Aut}(\mathcal{C}_{u,v})$ to $\mathrm{Aut}((\mathcal{C}_u)_{R^\times})_v$. On the other hand, by formula (23) with $\mathcal{C} = (\mathcal{C}_u)_{R^\times}$ and the fact that $\Gamma = R^\times_{\mathrm{right}}$, we have $\mathrm{Aut}(\mathcal{C}') = R^\times_{\mathrm{right}}\,\mathrm{Aut}((\mathcal{C}_u)_{R^\times})$. So, $\mathrm{Aut}(\mathcal{A}) = \mathrm{Aut}(\mathcal{C}')_v = \mathrm{Aut}((\mathcal{C}_u)_{R^\times})_v$ and we are done. □

In the general case the relationship between the groups $\mathrm{Aut}(\mathcal{C}_{u,v})$ and $\mathrm{Aut}(\mathcal{A})$ is unclear. However, we have the following statement, which will be used in §6.

Theorem 4.4. *Let R be a finite local commutative ring, let $\mathcal{C} = \mathrm{Cyc}(K,R)$, and let $\mathcal{A} = \mathcal{A}(K,R)$. Then the scheme $\mathcal{C}_{u,v}$ is trivial whenever the S-ring $\mathcal{A}$ is trivial. In particular, in this case,* $\mathrm{Aut}(\mathcal{C}) = \Gamma(K,R)$.

Proof. Suppose that the S-ring $\mathcal{A}$ is trivial. This means that $\mathcal{C}'$ is the scheme of 2-orbits of the group $R^\times_{\mathrm{right}}$, and consequently, the scheme $(\mathcal{C}')_v$ is trivial. Therefore, the scheme $((\mathcal{C}_u)_{R^\times})_v$ and its extension $(\mathcal{C}_{u,v})_{R^\times}$ are also trivial. On the other hand, the permutation $s = \gamma_{-1,1}$ is an isomorphism of the scheme $\mathcal{C}$ that interchanges u and v, so that $s \in \mathrm{Iso}(\mathcal{C}_{u,v})$. Thus, the scheme $(\mathcal{C}_{u^s,v^s})_{(R^\times)^s} = (\mathcal{C}_{v,u})_{1-R^\times}$ is trivial. It follows that the restriction of the scheme $\mathcal{C}_{u,v}$ to the set $R^\times \cup (1 - R^\times)$ is trivial. However, by the locality of the ring R we have $R = R^\times \cup (1 - R^\times)$. Thus, the scheme $\mathcal{C}_{u,v}$ is trivial. The second part of the theorem follows from the first and the proof of Lemma 2.4. □

§5. Multiplication S-ring: Pure case

In this section the multiplication S-ring of a cyclotomic scheme $\mathrm{Cyc}(K,R)$, which was introduced in §4, is studied for a pure group $K \leq \mathcal{T}\mathcal{U}_0$. First, we rewrite the second half of the sets mentioned in Theorem 4.2 in the multiplicative form.

Lemma 5.1. *Let R be a finite local commutative ring, and let $K = \mathcal{T}(1+H) \leq R^\times$ with $H \leq I_0$. Then for $r = 1 + x \in \mathcal{U}$ we have*

$$(1 + rK) \cap R^\times = \bigcup_{t\in\mathcal{T},\ t\neq 1} t(1 + z_{t,x} + \frac{t-1}{t}(H + x)),$$

where $z_{t,x} = y_t r$ with an element $y_t \in \mathrm{rad}(R)$ uniquely determined by the condition $1 - t^{-1} + y_t \in \mathcal{T}$.

Proof. By formula (3), we have

$$(1 + rK) \cap R^\times = \bigcup_{t'\in\mathcal{T},\ 1+t'\notin \mathrm{rad}(R)} (1 + (1 + x)t'(1 + H)). \tag{15}$$

Let $t' \in \mathcal{T}$, $1+t' \notin \operatorname{rad}(R)$. Then $1+t' = t(1+y_t)$ for some $t \in \mathcal{T}$. Therefore,

$$\begin{aligned} 1+(1+x)t'(1+H) &= 1+t'(1+H+x) = (1+t')(1+\frac{t}{1+t'}(H+x)) \\ &= t(1+y_t)(1+\frac{t(1+y_t)-1}{t(1+y_t)}(H+x)) = t(1+y_t+\frac{t(1+y_t)-1}{t}(H+x)) \\ &= t(1+y_t+y_tx+\frac{t-1}{t}(H+x)) = t(1+z_{t,x}+\frac{t-1}{t}(H+x)) \end{aligned}$$

(here $xH = y_tH = 0$ because $H \le I_0$). By (15), to complete the proof it suffices to note that t runs over the set $\mathcal{T} \setminus \{1\}$ when t' runs over the set $\mathcal{T} \setminus (-1+\operatorname{rad}(R))$. □

Theorem 5.2. *Let R be a finite local commutative ring, K a subgroup of $R^\times$, and $\mathcal{A}$ an S-ring over $R^\times$ such that $X(r) \in \mathcal{S}^*(\mathcal{A})$ for all $r \in R^\times$, where $X(r) = (1+rK) \cap R^\times$. Suppose that $K \le \mathcal{T}\mathcal{U}_0$ and the group K is pure. Then:*

1) *$\mathcal{T}, \mathcal{U} \in \mathcal{H}(\mathcal{A})$;*
2) *the S-ring $\mathcal{A}$ is trivial whenever so is the S-ring $\mathcal{A}_{\mathcal{T}}$ or the S-ring $\mathcal{A}_{\mathcal{U}}$.*

Before proving Theorem 5.2, we present an easy consequence of it, which will be used in the next section.

Theorem 5.3. *Let R be a finite local commutative ring, let $K \le \mathcal{T}\mathcal{U}_0$ be a pure group, and let $\mathcal{A}$ be the multiplication S-ring of the scheme* $\operatorname{Cyc}(K,R)$. *Then:*

1) *$\mathcal{T}, \mathcal{U} \in \mathcal{H}(\mathcal{A})$;*
2) *if $H \in \{\mathcal{T}, \mathcal{U}\}$, then the S-ring generated by $\mathcal{A}$ and the cosets of $R^\times$ by H is trivial.*

Proof. Statement 1) follows immediately from statement 1) of Theorem 5.2, because the S-ring $\mathcal{A}$ satisfies the assumptions of that theorem (see Theorem 4.2). To prove statement 2), we denote by $\mathcal{A}'$ the S-ring generated by $\mathcal{A}$ and the cosets of $R^\times$ by H. Since $\mathcal{A}' \ge \mathcal{A}$, the S-ring $\mathcal{A}'$ satisfies the assumptions of Theorem 5.2. So, by statement 2) of that theorem, it suffices to verify that the S-ring $\mathcal{A}'_{H'}$ is trivial, where $H' = \mathcal{U}$ if $H = \mathcal{T}$, and $H' = \mathcal{T}$ if $H = \mathcal{U}$. However, this follows from the fact that $|H' \cap C| = 1$ for any $C \in R^\times/H$. □

5.1. Proof of Theorem 5.2. Since $\mathcal{U}$ is the complement of the set $\bigcup_{r\in R^\times} X(r)$ in $R^\times$, the second part of statement 1) follows. To prove the rest of the theorem, we need the following lemma, based on Lemma 5.1. If $|R/\operatorname{rad}(R)| = 2$, then the latter lemma is useless. However, in this case, the group K and hence the S-ring $\mathcal{A}$ are trivial and the lemma below is also true. Below the basic set of $\mathcal{A}$ that contains $x \in R^\times$ is denoted by $[x]$.

Lemma 5.4. *Under the conditions of the theorem, we have:*

1) *if $[tu_1] = [tu_2]$ for some generator t of $\mathcal{T}$, where $u_1, u_2 \in \mathcal{U}$, then $u_1 = u_2$;*
2) *if $[t_1u] = [t_2u]$ for all $u \in \mathcal{U}$, where $t_1, t_2 \in \mathcal{T}$, then $t_1 = t_2$.*

Proof. Without loss of generality we assume that $\mathcal{T} \le K$. First, we prove statement 1). Any set $X \subset R^\times$ admits a unique representation in the form $X = \bigcup_{t\in\mathcal{T}} tX_t$, where $X_t \subset \mathcal{U}$ (see (3)). It follows that for any $\sigma \in \operatorname{Aut}(\mathcal{T})$ we have

$$X_t = (X^{\widehat{\sigma}})_{t^\sigma}, \quad t \in \mathcal{T}, \tag{16}$$

where $\widehat{\sigma}$ is the automorphism of the group $R^\times$ such that $\widehat{\sigma}^{\mathcal{T}} = \sigma$ and $\widehat{\sigma}^{\mathcal{U}} = \operatorname{id}_{\mathcal{U}}$. Since the group $\mathcal{T}$ is cyclic and its order is coprime to $|\mathcal{U}|$, the Chinese remainder theorem implies that the automorphism $\widehat{\sigma}$ is induced by raising to a power coprime to $|R^\times|$.

Now, without loss of generality, we assume that the residue field of R is of order at least 3, or equivalently, $|\mathcal{T}| \geq 2$. Let $X = [tu]$, where t is a generator of $\mathcal{T}$ and $u \in \mathcal{U}$. Then, obviously, $u \in X_t$, and it suffices to check that

$$X_t = \{u\}. \tag{17}$$

For this, we note that, by the Schur theorem on multipliers, we have $X^{\widehat{\sigma}} = [t^\sigma u]$ for all $\sigma \in \mathrm{Aut}(\mathcal{T})$. Therefore, $X^{\widehat{\sigma}} \subset X(r_\sigma)$ for some $r_\sigma = 1 + x_\sigma$ with $x_\sigma \in \mathrm{rad}(R)$ (we have used the fact that the latter set belongs to $\mathcal{S}^*(\mathcal{A})$ and the union of all such sets equals $R^\times \setminus \mathcal{U}$). Since $K \cap \mathcal{U} = 1 + H$, where $H \leq I_0$, Lemma 5.1 shows that

$$(X^{\widehat{\sigma}})_{t^\sigma} \subset 1 + z_{t^\sigma, x_\sigma} + \frac{t^\sigma - 1}{t^\sigma}(H + x_\sigma).$$

However, by (16), the element u belongs to the left-hand side of this inclusion, and thus, to the right-hand side; being a coset by the group $\frac{t^\sigma - 1}{t^\sigma} H$, this right-hand side is equal to $u + \frac{t^\sigma - 1}{t^\sigma} H$. We conclude that

$$X_t \subset \bigcap_{\sigma \in \mathrm{Aut}(\mathcal{T})} (u + \frac{t^\sigma - 1}{t^\sigma} H) = u + H_0,$$

where H_0 is the intersection of all groups $\frac{t^\sigma - 1}{t^\sigma} H$. To complete the proof of (17), we show that $H_0 = 0$. Suppose to the contrary that there exists a nonzero $x \in H_0$. Then $\frac{1}{1 - t^\sigma} x \in H$ for all $\sigma \in \mathrm{Aut}(\mathcal{T})$. On the other hand, the following statement, to be proved in §8, is true.[3]

Lemma 5.5. *Let $\mathbb{F}$ be a finite field of order at least 3. Then the set*

$$M = \{1/(1 - g) : \ g \text{ is a generator of the group } \mathbb{F}^\times\}$$

contains a linear base of $\mathbb{F}$ over its prime subfield.

We observe that the natural epimorphism π from R onto its residue field $\mathbb{F}$ induces a group isomorphism from $\mathcal{T}$ to $\mathbb{F}^\times$ such that

$$M = \{\pi(1/(1 - t')) : \, t' \in \mathcal{T}'\},$$

where $\mathcal{T}'$ is the set of generators of the group $\mathcal{T}$. Then Lemma 5.5 shows that for any $r \in R$ the element $\pi(r)$ is an integral combination of the elements $\pi(1/(1 - t'))$, $t' \in \mathcal{T}'$. Let s denote the integral combination (with the same coefficients) of the elements $1/(1 - t')$, $t' \in \mathcal{T}'$. Then $r - s \in \mathrm{rad}(R)$, and hence rx is a linear combination of the elements $x/(1 - t')$, $t' \in \mathcal{T}'$. Since all of them belong to H (see above), this implies that $rx \in H$. Thus, $Rx \subset H$. It follows that $1 + I \subset 1 + H \subset K$, where $I = Rx$, which contradicts the purity of K. This completes the proof of statement 1).

To prove statement 2), suppose that $[t_1 u] = [t_2 u]$ for all $u \in \mathcal{U}$ where $t_1, t_2 \in \mathcal{T}$. By the second part of statement 1) of Theorem 5.2, proved above, without loss of generality we may assume that $t_1 \neq 1$ and $t_2 \neq 1$. It suffices to verify that if $t_1 \neq t_2$, then there exists $r \in \mathcal{U}$ such that

$$t_1^{-1}(1 + rK) \cap \mathcal{U} \neq t_2^{-1}(1 + rK) \cap \mathcal{U}. \tag{18}$$

(Indeed, then there exists an element u belonging to the left-hand side but not to the right-hand side (or *vice versa*). Then $t_1 u \in X(r)$ and $t_2 u \notin X(r)$. Since $X(r) \in \mathcal{S}^*(\mathcal{A})$, this implies that $[t_1 u] \neq [t_2 u]$, which contradicts our assumption.) Let $r = 1 + x \in \mathcal{U}$ be such that equality occurs in (18). Then Lemma 5.1 implies

$$1 + z_{t_1, x} + \frac{t_1 - 1}{t_1}(H + x) = 1 + z_{t_2, x} + \frac{t_2 - 1}{t_2}(H + x), \tag{19}$$

[3] The idea of the proof was communicated to the authors by Igor Shparlinski.

where H is as above. Since the left-hand side and the right-hand side are cosets by the groups $\frac{t_1-1}{t_1}H$ and $\frac{t_2-1}{t_2}H$, respectively, these groups are equal. Moreover, formula (19) shows that

$$sx \in y + H',$$

where $s = y_{t_1} - y_{t_2} + \frac{t_1-1}{t_1} - \frac{t_2-1}{t_2}$, $y = y_{t_2} - y_{t_1}$ (see Lemma 5.1), and $H' = \frac{t_1-1}{t_1}H = \frac{t_2-1}{t_2}H$. We observe that $y \in \mathrm{rad}(R)$, and $s \in R^\times$ because $t_1 \neq t_2$. It follows that x belongs to the coset

$$C = s^{-1}y + s^{-1}H' \subset s^{-1}y + I_0.$$

On the other hand, by the purity of K we have $H \neq I_0$, whence $s^{-1}H' \neq I_0$. Thus, $C \subsetneqq s^{-1}y + I_0$, and inequality (18) is fulfilled for any $r = 1 + x$ with $x \in (s^{-1}y + I_0) \setminus C$. $\square$

To prove the first part of statement 1) of Theorem 5.2, we take a generator t of the group $\mathcal{T}$. It suffices to verify that the set $X = [t]$ is contained in $\mathcal{T}$. For this, we observe that statement 1) of Lemma 5.4 implies that $t^p \in X^{[p]}$, where p is the characteristic of the residue field of the ring R and $X^{[p]}$ is as in the Schur theorem on multipliers. So, $t \in X' = (X^{[p]})^{\widehat{\sigma}}$, where σ is the automorphism of $\mathcal{T}$ inverse to raising to the pth power and $\widehat{\sigma}$ is the automorphism of $R^\times$ defined above. Then, by the Schur theorem on multipliers, we have $X' \in \mathcal{S}^*(\mathcal{A})$, whence $X \subset X'$. Since obviously $|X'| \leq |X|$, we conclude that $X' = X$. However, the only set $Y \subset \mathcal{U}$ for which $Y^{[p]} = Y$ is $Y = \{1\}$. Thus, $X \subset \mathcal{T}$, and statement 1) is proved.

To prove statement 2), suppose that the S-ring $\mathcal{A}_{\mathcal{T}}$ is trivial. Let $u_1, u_2 \in \mathcal{U}$, $u_1 \neq u_2$. Then statement 1) of Lemma 5.4 implies that $[tu_1] \neq [tu_2]$ for some $t \in \mathcal{T}$. Since $[t] = \{t\}$, we have $[tu_i] = [t][u_i]$ for $i = 1, 2$, whence it follows that $[u_1] \neq [u_2]$. Thus, the S-ring $\mathcal{A}_{\mathcal{U}}$ is trivial, and consequently, so is the S-ring $\mathcal{A}$. The second part of the statement is proved in a similar way, by using statement 2) of Lemma 5.4. $\square$

§6. Proof of Theorem 1.6

6.1. Reduction. For a cyclotomic scheme $\mathcal{C}$ over a ring R, we set

$$\mathrm{Aut}_{\mathcal{C}}(R) = \mathrm{Aut}(\mathcal{C}) \cap \mathrm{Aut}(R), \quad \mathrm{Aut}_{\mathcal{C}}(R/I) = \mathrm{Aut}_{\mathcal{C}_{R/E(I)}}(R/I),$$

where I is an ideal of R.

Theorem 6.1. *Let R be a finite local commutative ring, and let $\mathcal{C} = \mathrm{Cyc}(K, R)$, where K is a pure subgroup of the group $R^\times$. Then the restriction mapping from $\mathrm{Aut}_{\mathcal{C}}(R)$ to $\mathrm{Aut}_{\mathcal{C}}(R/I_0)$ is a monomorphism. Moreover, $\mathrm{Aut}(\mathcal{C}) \leq \mathrm{A\Gamma L}_1(R)$ whenever $\mathrm{Aut}(\mathcal{C})^{R/E_0} \leq \mathrm{A\Gamma L}_1(R/I_0)$, where $E_0 = E_{I_0}$.*

Proof. First, we observe that the kernel of the homomorphism $f \mapsto f^{R/E_0}$ from $\mathrm{Aut}(\mathcal{C})$ to $\mathrm{Aut}(\mathcal{C})^{R/E_0}$ coincides with the group $\mathrm{Aut}(\mathcal{C})_{E_0}$. Moreover,

$$\mathrm{Aut}(\mathcal{C})_{E_0} \leq \mathrm{AGL}_1(R). \tag{20}$$

Indeed, $\mathcal{C}_{E_0} \geq \mathrm{Cyc}(U_0, R)$ in view of Theorem 2.5. Therefore, $\mathrm{Aut}(\mathcal{C})_{E_0} = \mathrm{Aut}(\mathcal{C}_{E_0}) \leq \mathrm{Aut}(\mathrm{Cyc}(U_0, R))$. Thus, by Theorem 4.4, it suffices to verify that the S-ring $\mathcal{A}(U_0, R)$ is trivial. However, this immediately follows from statement 2) of Theorem 5.3.

Let a permutation $f \in \mathrm{Aut}_{\mathcal{C}}(R)$ be such that the permutation f^{R/E_0} is identical. Then $f \in \mathrm{Aut}(\mathcal{C}_{E_0})$, whence $f \in \mathrm{AGL}_1(R)$ by (20). Since, obviously, f leaves the points 0 and 1 fixed, this implies that $f = \mathrm{id}_R$. This proves the first statement of the theorem.

To prove the second statement, suppose that $\mathrm{Aut}(\mathcal{C})^{R/E_0} \leq \mathrm{A\Gamma L}_1(R/I_0)$. Then, by the locality of the ring R and Lemma 2.1 with $K = R^\times$, it suffices to check that the group $\Gamma = \Gamma(R^\times, R)$ is normalized by the group $\mathrm{Aut}(\mathcal{C})$. By (20) all we need to prove is

$$f^{-1}\Gamma f \subset \Gamma\,\mathrm{Aut}(\mathcal{C}_{E_0}), \quad f \in \mathrm{Aut}(\mathcal{C}),$$

Take $\gamma \in \Gamma$ and $f \in \mathrm{Aut}(\mathcal{C})$. Then

$$\overline{f^{-1}\gamma f} = \overline{f}^{-1}\overline{\gamma}\overline{f} \in \overline{f}^{-1}\overline{\Gamma}\overline{f} = \overline{\Gamma}, \tag{21}$$

where the bar means factorization modulo E_0 (we have used the fact that, by assumption, $\overline{f} \in \overline{\mathrm{Aut}(\mathcal{C})} \leq \mathrm{A\Gamma L}_1(R/I_0)$). On the other hand, $f^{-1}\gamma f = \gamma(\gamma^{-1}f^{-1}\gamma)f = \gamma f_1$, where $f_1 = (\gamma^{-1}f^{-1}\gamma)f$. Since $\Gamma \leq \mathrm{Iso}(\mathcal{C})$, we have $f_1 \in \mathrm{Aut}(\mathcal{C})$. Therefore, from (21) it follows that

$$\overline{f_1} \in \overline{\Gamma} \cap \overline{\mathrm{Aut}(\mathcal{C})} = \Gamma(\overline{K}, \overline{R}),$$

where $\overline{K} = \pi_0(K)$ and $\overline{R} = R/I_0$. Since the natural homomorphism $\Gamma(K,R) \to \Gamma(\overline{K}, \overline{R})$ is surjective, this implies the existence of $\gamma_1 \in \Gamma(K,R)$ such that $\overline{\gamma_1} = \overline{f_1}$. Thus, $\gamma_1^{-1}f_1 \in \mathrm{Aut}(\mathcal{C}_{E_0})$, and consequently,

$$f^{-1}\gamma f = (\gamma\gamma_1)(\gamma_1^{-1}f_1) \in \Gamma\,\mathrm{Aut}(\mathcal{C}_{E_0}). \qquad \square$$

6.2. Strongly pure groups and normality. We deduce Theorem 1.6 from a more general result, by using the notion of strong purity defined recursively as follows. A group $K \leq R^\times$ is said to be *strongly pure* if it is pure and the group $\pi_0(K) \leq (R/I_0)^\times$ is strongly pure unless R is a field. Obviously, any strongly pure group is pure. The converse statement fails in general: a counterexample is given by $R = \mathbb{F}[X]/(X^n)$, where $\mathbb{F}$ is a finite field and $n \geq 4$, and $K = 1 + \mathbb{F}x^{n-2}$ with $x = X \mod X^n$. However, the definition implies immediately that any pure group is strongly pure whenever $\mathrm{rad}(R)^2 = 0$.

Theorem 6.2. *Let R be a finite local commutative ring other than a field. Then the scheme $\mathcal{C} = \mathrm{Cyc}(K,R)$ is normal whenever the group K is strongly pure. Moreover, in this case the restriction mapping from $\mathrm{Aut}_{\mathcal{C}}(R)$ to $\mathrm{Aut}_{\mathcal{C}}(\mathbb{F})$ is a monomorphism, where $\mathbb{F}$ is the residue field of R.*

Proof. With the help of Theorem 6.1, applied inductively to the scheme $\mathcal{C}$ and its factors, we immediately obtain the monomorphism statement. Moreover, the proof of normality reduces to the case where $\mathrm{rad}(R)^2 = 0$ and the group K is pure, and in this case it suffices to verify that

$$\mathrm{Aut}(\mathcal{C})^{\mathbb{F}} \leq \mathrm{A\Gamma L}_1(\mathbb{F}). \tag{22}$$

For this, we need the following lemma. $\square$

Lemma 6.3. *The groups $\mathrm{Aut}(\mathcal{C}_u)^{R^\times}$ and $\mathrm{Aut}(\mathcal{C}_v)^{1-R^\times}$ normalize the groups $\Gamma(\mathcal{T})^{R^\times}$ and $(s\Gamma(\mathcal{T})s)^{1-R^\times}$, respectively, where $u = 0$, $v = 1$, and $s = \gamma_{-1,1}$.*

Proof. Statement 1) of Theorem 5.3 shows that $\mathcal{T} \in \mathcal{H}(\mathcal{A})$, where $\mathcal{A}$ is the multiplication S-ring of the scheme $\mathcal{C}$. Therefore, by Theorem 7.2 (with $H = \mathcal{T}$), $\mathrm{Aut}(\mathcal{A})$ normalizes the group $\langle \mathrm{Aut}(\mathcal{A}'), \Gamma(\mathcal{T})^{R^\times} \rangle$. However, in our case the group $\mathrm{Aut}(\mathcal{A}')$ is trivial by statement 2) of Theorem 5.3. Thus, $\mathrm{Aut}(\mathcal{A})$ normalizes $\Gamma(\mathcal{T})^{R^\times}$. On the other hand, the definition of the S-ring $\mathcal{A}$ shows that $\mathrm{Aut}(\mathcal{C}_u)^{R^\times} \leq \Gamma(R^\times)^{R^\times}\,\mathrm{Aut}(\mathcal{A})$. Thus, $\mathrm{Aut}(\mathcal{C}_u)^{R^\times}$ normalizes the group $\Gamma(\mathcal{T})^{R^\times}$. To complete the proof we observe that, obviously, s is an isomorphism of $\mathcal{C}$ that interchanges u and v. So, the group $\mathrm{Aut}(\mathcal{C}_v)^{1-R^\times}$ normalizes the group $(s\Gamma(\mathcal{T})s)^{1-R^\times}$. $\square$

To check (22), it suffices to show that if $\gamma \in \mathrm{Aut}(\mathcal{C}_{u,v})$, then $\gamma^{\mathbb{F}} \in \mathrm{Aut}(\mathbb{F})$. However, from Lemma 6.3 it follows that the permutation $\gamma^{X_0} = (\gamma^{R^\times})^{X_0}$ normalizes the group $\Gamma(\mathbb{F}^\times)^{X_0}$ whereas the permutation $\gamma^{X_1} = (\gamma^{1-R^\times})^{X_1}$ normalizes the group $(s^{\mathbb{F}}\Gamma(\mathbb{F}^\times)s^{\mathbb{F}})^{X_1}$, where $X_i = \mathbb{F} \setminus \{i\}$, $i \in \{0_{\mathbb{F}}, 1_{\mathbb{F}}\}$. Thus, $\gamma^{\mathbb{F}}$ normalizes each of the groups $\Gamma(\mathbb{F}^\times)$ and $s^{\mathbb{F}}\Gamma(\mathbb{F}^\times)s^{\mathbb{F}}$, and we are done by Corollary 2.2. $\square$

Since, obviously, a pure group $K \leq \mathcal{T}\mathcal{U}_0$ is strongly pure, Theorem 6.2 implies the following statement.

Theorem 6.4. *Let R be a finite local commutative ring other than a field, and let K be a pure subgroup of $R^\times$. Then the scheme $\mathrm{Cyc}(K,R)$ is normal whenever $K \leq \mathcal{T}\mathcal{U}_0$.*

We complete this subsection with a sufficient condition for the automorphism group of a cyclotomic scheme to be a subgroup of $\mathrm{AGL}_1(R)$.

Theorem 6.5. *Let $\mathcal{C} = \mathrm{Cyc}(K,R)$ be a cyclotomic scheme over a finite local commutative ring R other than a field. Then $\mathrm{Aut}(\mathcal{C}) \leq \mathrm{AGL}_1(R)$ whenever one of the following conditions is satisfied*:

1) *$K \leq \mathcal{T}$;*
2) *K is a strongly pure subgroup of $\mathcal{U}$;*
3) *the group K is strongly pure and the residue field of R is prime.*

Proof. To prove statement 1), we observe that by Theorem 4.2, the S-ring $\mathcal{A}(K,R)$ contains all elements of the set $R^\times/K$. Therefore, by statement 2) of Theorem 5.3, this S-ring is trivial, and it remains to use Theorem 4.4. To prove statements 2) and 3), we observe that, by the first part of Theorem 6.2, we have $\mathrm{Aut}(\mathcal{C}) \leq \mathrm{A\Gamma L}_1(R)$. Therefore, by the second part of that theorem, it suffices to prove that the group $\mathrm{Aut}_{\mathcal{C}}(\mathbb{F})$ is trivial, where $\mathbb{F}$ is the residue field of R. However, this is clear for statement 2) because $\mathcal{C}_{\mathbb{F}} = \mathrm{Cyc}(1,\mathbb{F})$ (see (7)), and for statement 3) because $\mathrm{Aut}(\mathbb{F}) = 1$. □

6.3. Proof of Theorem 1.6. By Theorem 6.2, the required statement is a consequence of the following theorem.

Theorem 6.6. *For a Galois ring of odd characteristic, any pure group is strongly pure.*

Proof. Let $R = \mathrm{GR}(p^n, r)$, where p is odd. We may assume that $n > 1$. Then the group $\mathcal{U}$ is isomorphic to a direct product of r copies of a cyclic group of order p^{n-1} (see [10]). In particular, $\mathrm{rk}(\mathcal{U}) = r$, and the maximal elementary Abelian subgroup of $\mathcal{U}$ is equal to $\mathcal{U}_0$. Since the rank of an Abelian group does not increase under factorization, it suffices to prove the lemma below. □

Lemma 6.7. *Under the above assumptions, a group $K \leq R^\times$ is pure if and only if $\mathrm{rk}(U) < r$, where $U = K \cap \mathcal{U}$.*

Proof. Suppose that the group K is not pure. Then $\mathcal{U}_0 \leq U$. On the other hand, since $I_0 = p^{n-1}R$, the group $\mathcal{U}_0$ is elementary Abelian of order p^r. Thus, $\mathrm{rk}(U) \geq \mathrm{rk}(\mathcal{U}_0) = r$. Conversely, let $\mathrm{rk}(U) = r$. Then the maximal elementary Abelian subgroup of U is of order p^r. Therefore, it coincides with the maximal elementary Abelian subgroup of $\mathcal{U}$. Since the latter subgroup equals $\mathcal{U}_0$, we are done. □

§7. Association schemes and Schur rings

7.1. Schemes. Let V be a finite set, and let $\mathcal{R}$ be a partition of V^2 into nonempty subsets. We denote by $\mathcal{R}^*$ the set consisting of all unions of elements of $\mathcal{R}$. A pair

$$\mathcal{C} = (V, \mathcal{R})$$

is called a *coherent configuration*, *association scheme*, or *scheme* on V if 1) the set $\mathcal{R}$ is closed with respect to transposition, 2) the diagonal $\Delta(V)$ of V^2 belongs to $\mathcal{R}^*$, and 3) given $R, S, T \in \mathcal{R}$, 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 the sets V, $\mathcal{R} = \mathcal{R}(\mathcal{C})$, and $\mathcal{R}^* = \mathcal{R}^*(\mathcal{C})$ are called the *points*, the *basis relations* and the *relations* of $\mathcal{C}$, respectively.

The number $\mathrm{rk}(\mathcal{C}) = |\mathcal{R}|$ is called the *rank* of $\mathcal{C}$. We observe that, given nonempty sets $X, Y \subset V$, we have $X \times Y \in \mathcal{R}^*$ if and only if $\Delta(X), \Delta(Y) \in \mathcal{R}^*$. If $\Delta(V) \in \mathcal{R}$, the scheme $\mathcal{C}$ is said to be *homogeneous.*

Two schemes are *isomorphic* if there exists a bijection between their point sets preserving the basis relations. Any such bijection is called an *isomorphism* of these schemes. The set of all isomorphisms of a scheme $\mathcal{C}$ is denoted by $\mathrm{Iso}(\mathcal{C})$. This group contains a normal subgroup

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

called the *automorphism group* of $\mathcal{C}$. For a permutation group $\Gamma \leq \mathrm{Iso}(\mathcal{C})$, we denote by $\mathcal{C}^\Gamma$ the scheme on the same point set, the relations of which are exactly the elements of $\mathcal{R}^*$ invariant with respect to Γ. In particular, if the scheme $\mathcal{C}$ is *trivial*, i.e., $\mathcal{R}^* = 2^{V^2}$, then $\mathrm{Iso}(\mathcal{C}) = \mathrm{Sym}(V)$, and $\mathcal{C}^\Gamma$ equals the *scheme of* 2*-orbits* of the group Γ. In the general case, it can be proved that if Γ acts regularly on the set $\{X \subset V :\ \Delta(X) \in \mathcal{R}\}$, then

$$\mathrm{Aut}(\mathcal{C}^\Gamma) = \Gamma\,\mathrm{Aut}(\mathcal{C}) \tag{23}$$

(see [4, Theorem 2.2]).

Given a set $U \subset V$, denote by $\mathcal{R}_U$ the set of all nonempty relations $R_U = R \cap U^2$, $R \in \mathcal{R}$ (viewed as relations on U). If $\Delta(U) \in \mathcal{R}^*$, then the pair $\mathcal{C}_U = (U, \mathcal{R}_U)$ is a scheme on U. Clearly,

$$\mathrm{Aut}(\mathcal{C})^U \leq \mathrm{Aut}(\mathcal{C}_U).$$

Given an equivalence relation E on V, denote by $\mathcal{R}_{V/E}$ the set of all relations

$$R_{V/E} = \{(X,Y) \in (V/E)^2 :\ R \cap (X \times Y) \neq \varnothing\}, \quad R \in \mathcal{R}.$$

If $E \in \mathcal{R}^*$, then $\mathcal{C}_{V/E} = (V/E, \mathcal{R}_{V/E})$ is a scheme on V/E. The set of all such E is denoted by $\mathcal{E} = \mathcal{E}(\mathcal{C})$. Clearly,

$$\mathrm{Aut}(\mathcal{C})^{V/E} \leq \mathrm{Aut}(\mathcal{C}_{V/E}).$$

The set of all schemes on V is partially ordered by inclusion: $\mathcal{C} \leq \mathcal{C}'$ if and only if $\mathcal{R}^* \subset (\mathcal{R}')^*$. The largest scheme is the trivial scheme on V, whereas the smallest one is the scheme of 2-orbits of the group $\mathrm{Sym}(V)$. For the sets $\mathcal{R}_1, \ldots, \mathcal{R}_s \subset 2^{V^2}$, we denote by $[\mathcal{R}_1, \ldots, \mathcal{R}_s]$ the smallest scheme $\mathcal{C}$ on V such that $\mathcal{R}_i \subset \mathcal{R}^*$ for all i; we omit the braces if $\mathcal{R}_i = \{R_i\}$ and write $\mathcal{C}_i$ instead of $\mathcal{R}_i$ if $\mathcal{R}_i$ is the set of all basis relations of the scheme $\mathcal{C}_i$. In particular, for a scheme $\mathcal{C}$ on V and $v_1, \ldots, v_s \in V$ we set $\mathcal{C}_{v_1,\ldots,v_s} = [\mathcal{C}, \Delta(\{v_1\}), \ldots, \Delta(\{v_s\})]$. It is easily seen that

$$\mathrm{Aut}(\mathcal{C}_{v_1,\ldots,v_s}) = \mathrm{Aut}(\mathcal{C})_{v_1,\ldots,v_s},$$

where $\mathrm{Aut}(\mathcal{C})_{v_1,\ldots,v_s}$ is the pointwise stabilizer of the set $\{v_1, \ldots, v_s\}$ in the group $\mathrm{Aut}(\mathcal{C})$. We shall also use the following property of the v*-extension* $\mathcal{C}_v$ of the scheme $\mathcal{C}$, where $v \in V$: if $X = R_{\mathrm{out}}(v)$ is the neighborhood of v in a relation $R \in \mathcal{R}^*$, then $\Delta(X)$ is a relation of the scheme $\mathcal{C}_v$. Finally, if E is an equivalence relation on V, we set $\mathcal{C}_E = [\mathcal{C}, \{\Delta(X) :\ X \in V/E\}]$. It immediately follows that

$$\mathrm{Aut}(\mathcal{C}_E) \trianglelefteq \mathrm{Aut}(\mathcal{C}), \quad E \in \mathcal{E}(\mathcal{C}). \tag{24}$$

7.2. Schur rings and Cayley schemes. Let G be a finite group. A subring $\mathcal{A}$ of the group ring $\mathbb{Z}[G]$ is called a *Schur ring* (S*-ring*, for brevity) over G if it has a (uniquely determined) $\mathbb{Z}$-base consisting of elements $\sum_{x \in X} x$, 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 $\mathcal{S}$ the *basic sets* of $\mathcal{A}$ and denote by $\mathcal{S}^* = \mathcal{S}^*(\mathcal{A})$ the set of all unions of them and by $\mathcal{H} = \mathcal{H}(\mathcal{A})$ the set of all $\mathcal{A}$-*subgroups* of G (i.e., the subgroups belonging to $\mathcal{S}^*$). The number $\mathrm{rk}(\mathcal{A}) = \dim_{\mathbb{Z}}(\mathcal{A})$ is called the *rank* of $\mathcal{A}$. If $\mathrm{rk}(\mathcal{A}) = |G|$ (equivalently, $\mathcal{A} = \mathbb{Z}[G]$), then we say that the S-ring $\mathcal{A}$ is *trivial.* Given $H \in \mathcal{H}$, we denote by $\mathcal{A}_H$ the S-ring over H such that $\mathcal{S}(\mathcal{A}_H) = \{X \in \mathcal{S} :\ X \subset H\}$.

The proof of the following theorem, called the *Schur theorem on multipliers*, can be found in [14]. Below, for $X \subset G$, $m \in \mathbb{Z}$, and a prime p, we set

$$X^{(m)} = \{x^m :\ x \in X\}, \quad X^{[p]} = \{x^p :\ x \in X,\ |xH \cap X| \not\equiv 0 \pmod p\},$$

where $H = \{g \in G :\ g^p = 1\}$.

Theorem 7.1. *Let G be a finite Abelian group and $\mathcal{A}$ an* S*-ring over G. Then, for any $X \in \mathcal{S}(\mathcal{A})$,*

1) *$X^{(m)} \in \mathcal{S}(\mathcal{A})$ for any integer m coprime to $|G|$, and*
2) *$X^{[p]} \in \mathcal{S}^*(\mathcal{A})$ for any prime p dividing $|G|$.*

For a finite group G, we denote by $\mathcal{R}(G)$ the set of all binary relations on G that are invariant with respect to the group G_{right}. Then the mapping

$$2^G \to \mathcal{R}(G), \quad X \mapsto R_G(X),$$

where $R_G(X) = \{(g, xg) :\ g \in G, x \in X\}$, is a bijection. A straightforward computation shows that if $H \trianglelefteq G$ and $C \in G/H$, then

$$R_G(C) = \bigcup_{C' \in G/H} C' \times CC'.[4] \tag{25}$$

In particular, $R_G(H)$ is an equivalence relation on G.

Let $\mathcal{A}$ be an S-ring over the group G. Then the pair $\mathcal{C} = (G, \mathcal{R})$ with $\mathcal{R} = R_G(\mathcal{S}) = \{R_G(X) :\ X \in \mathcal{S}\}$ is a scheme on G, and $G_{\mathrm{right}} \leq \mathrm{Aut}(\mathcal{C})$. Any scheme satisfying the latter condition is called a *Cayley scheme* on G. In fact, the above correspondence induces a bijection between the S-rings over G and the Cayley schemes on G, and this bijection preserves the natural partial orders on these sets. Obviously, $\mathcal{R}^* = R_G(\mathcal{S}^*)$ and $\mathcal{E} = R_G(\mathcal{H})$. Moreover,

$$\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(\mathcal{A})\, G_{\mathrm{right}}, \tag{26}$$

where $\mathrm{Aut}(\mathcal{A}) = \mathrm{Aut}(\mathcal{C})_v$ with $v = 1_G$.

Theorem 7.2. *Let $\mathcal{A}$ be an* S*-ring over a group G and H a normal $\mathcal{A}$-subgroup of G. Then* $\mathrm{Aut}(\mathcal{A})$ *normalizes the group $\langle \mathrm{Aut}(\mathcal{A}'), H' \rangle$, where $\mathcal{A}'$ is the* S*-ring over G generated by $\mathcal{A}$ and by the cosets of G by H, and H' is the subgroup of the group G_{right} corresponding to multiplications by the elements of H.*

Proof. Let $\mathcal{C}$ and $\mathcal{C}'$ be the Cayley schemes over the group G that correspond to the S-rings $\mathcal{A}$ and $\mathcal{A}'$, respectively. Then $\mathcal{C}' = [\mathcal{C}, \mathcal{R}_G(G/H)]$ (see (4)). We show that

$$\mathcal{C}_E = (\mathcal{C}')_E, \tag{27}$$

where $E = R_G(H)$. Indeed, obviously, $\Delta(C)$ is a relation of the scheme $\mathcal{C}_E$ for all $C \in G/H$. The observation at the end of the first paragraph of Subsection 7.2 shows that $R_G(C)$ is also a relation of the scheme $\mathcal{C}_E$ for all C. Therefore, $R_G(G/H) \subset \mathcal{R}^*(\mathcal{C}_E)$, whence $(\mathcal{C}')_E \leq \mathcal{C}_E$. Since the reverse inclusion is clear, (27) is proved. Next, we have

$$\mathrm{Aut}((\mathcal{C}')_E) = \mathrm{Aut}(\mathcal{A}')H'. \tag{28}$$

[4] If $C = H$, then the normality condition for H is not necessary.

Indeed, by definition we have $\mathrm{Aut}(\mathcal{C}') = \mathrm{Aut}(\mathcal{A}')G_{\mathrm{right}}$. Also, by the normality of H we have $(G_{\mathrm{right}})_E = H'$. Since, obviously, $\mathrm{Aut}(\mathcal{A}')_E = \mathrm{Aut}(\mathcal{A}')$, it follows that

$$\mathrm{Aut}((\mathcal{C}')_E) = \mathrm{Aut}(\mathcal{C}')_E = (\mathrm{Aut}(\mathcal{A}')G_{\mathrm{right}})_E = \mathrm{Aut}(\mathcal{A}')(G_{\mathrm{right}})_E = \mathrm{Aut}(\mathcal{A}')H',$$

whence (28) follows.

Since $H \in \mathcal{H}(\mathcal{A})$, we have $E \in \mathcal{E}(\mathcal{C})$. Therefore, from (24) it follows that $\mathrm{Aut}(\mathcal{C}_E)$ is a normal subgroup of the group $\mathrm{Aut}(\mathcal{C})$. This implies that the group $\mathrm{Aut}(\mathcal{A})$ normalizes $\mathrm{Aut}(\mathcal{C}_E)$. However, $\mathrm{Aut}(\mathcal{C}_E) = \mathrm{Aut}((\mathcal{C}')_E) = \mathrm{Aut}(\mathcal{A}')H'$ (see (27) and (28)). The theorem is proved. □

§8. Proof of Lemma 5.5

We denote by P the set of generators of the group $\mathbb{F}^\times$ and put $f(g) = 1/(1-g)$, $g \in \mathbb{F} \setminus \{1\}$. Then it suffices to verify that for any $a \in \mathbb{F}$, the set S_a of solutions in P to the equation

$$f(g_1) + f(g_2) + f(g_3) = a \tag{29}$$

is nonempty. For this, we observe that

$$\begin{aligned} |S_a| &= \sum_{g_1,g_2,g_3 \in P} q^{-1} \sum_{\psi \in \Psi} \psi(f(g_1) + f(g_2) + f(g_3) - a) \\ &= q^{-1} \sum_{g_1,g_2,g_3 \in P} 1 + q^{-1} \sum_{\psi \in \Psi \setminus \{\psi_0\}} \sum_{g_1,g_2,g_3 \in P} \psi(f(g_1))\psi(f(g_2))\psi(f(g_3))\overline{\psi(a)} \\ &= |P|^3/q + q^{-1}\overline{\psi(a)} \sum_{\psi \in \Psi \setminus \{\psi_0\}} (\sum_{g \in P} \psi(f(g)))^3, \end{aligned} \tag{30}$$

where $q = |\mathbb{F}|$, Ψ is the set of all additive characters of $\mathbb{F}$, and ψ_0 is the principal character. On the other hand, by the inclusion-exclusion principle we have

$$\sum_{g \in P} \psi(f(g)) = \sum_{d|q-1} \mu(d) d^{-1} \sum_{g \in \mathbb{F}^\times \setminus G_d} \psi(f(g^d)),$$

where μ is the Möbius function and $G_d = \{g \in \mathbb{F}^\times : \ g^d = 1\}$. However, applying [11, Theorem 2], we obtain

$$|\sum_{g \in F^\times \setminus G_d} \psi(f(g^d))| \leq 2dq^{1/2}.$$

This implies that

$$|\sum_{g \in P} \psi(f(g))| \leq \sum_{d|q-1} 2q^{1/2} = 2\tau(q-1)q^{1/2},$$

where $\tau(q-1)$ is the number of divisors of the integer $q-1$. Thus, by (30),

$$|S_a| \geq |P|^3/q - q^{-1} \sum_{\psi \in \Psi \setminus \{\psi_0\}} |\sum_{g \in P} \psi(f(g))|^3 \geq \varphi(q-1)^3/q - 8\tau(q-1)^3 q^{3/2}, \tag{31}$$

where φ is the Euler function. Using the well-known estimates $\varphi(n) \geq (n \log 2)/(2 \log n)$ and $\log \tau(n) < 1.6 \log 2 \log n / \log\log n$ for $n \geq 3$ (see [6] and [12]), it is not difficult to check that the right-hand side of (31) is positive for all $q > 575$. Therefore, the set S_a is nonempty for such q, so that equation (29) is solvable for all a. For $q \leq 575$ the statement of the lemma can be checked by an exhaustive search.

References

[1] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-regular graphs*, Ergeb. Math. Grenzgeb. (3), Bd. 18, Springer-Verlag, Berlin, 1989. MR1002568 (90e:05001)

[2] J. D. Dixon and B. Mortimer , *Permutation groups*, Grad. Texts in Math., No. 163, Springer-Verlag, New York, 1996. MR1409812 (98m:20003)

[3] S. A. Evdokimov, *Schurity and separability of association schemes*, Thesis for a Doctor's Degree, S.-Peterburg. Gos. Univ., St. Petersburg, 2004. (Russian)

[4] S. A. Evdokimov and I. N. Ponomarenko, *Characterization of cyclotomic schemes and normal Schur rings over a cyclic group*, Algebra i Analiz **14** (2002), no. 2, 11–55; English transl., St. Petersburg Math. J. **14** (2003), no. 2, 189–221. MR1925880 (2003h:20005)

[5] R. W. Goldbach and H. L. Claasen, *Cyclotomic schemes over finite rings*, Indag. Math. (N.S.) **3** (1992), 301–312. MR1186739 (94b:05219)

[6] H. Hatalová and T. Salát, *Remarks on two results in the elementary theory of numbers*, Acta Fac. Rerum Natur. Univ. Comenian. Math. **20** (1970), 113–117. MR0268115 (42:3014)

[7] T. Ito, A. Munemasa, and M. Yamada, *Amorphous association schemes over the Galois rings of characteristic* 4, European J. Combin. **12** (1991), 513–526. MR1136393 (93a:05133)

[8] K. H. Leung and S. H. Man, *On Schur rings over cyclic groups.* II, J. Algebra **183** (1996), 273–285. MR1399027 (98h:20009)

[9] R. McConnel, *Pseudo-ordered polynomials over a finite field*, Acta Arith. **8** (1962/1963), 127–151. MR0164953 (29:2244)

[10] B. R. McDonald, *Finite rings with identity*, Pure Appl. Math., vol. 28, Marcel Dekker, Inc., New York, 1974. MR0354768 (50:7245)

[11] C. J. Moreno and O. Moreno, *Exponential sums and Goppa codes.* I, Proc. Amer. Math. Soc. **111** (1991), no. 2, 523–531. MR1028291 (91f:11087)

[12] J.-L. Nicolas and G. Robin, *Majorations explicites pour le nombre de diviseurs de N*, Canad. Math. Bull **26** (1983), no. 4, 485–492. MR0716590 (85e:11006)

[13] Z. -X. Wan, *Lectures on finite fields and Galois rings*, World Sci. Publ. Co., Inc., River Edge, NJ, 2003. MR2008834 (2004h:11101)

[14] H. Wielandt, *Finite permutation groups*, Academic Press, New York–London, 1964. MR0183775 (32:1252)

[15] ______, *Permutation groups through invariant relations and invariant functions*, Lecture Notes, Ohio State Univ. Columbus, Dept. Math., Ohio, 1969.

St. Petersburg Branch, Steklov Mathematical Institute, Russian Academy of Sciences, Fontanka 27, St. Petersburg 191023, Russia
E-mail address: evdokim@pdmi.ras.ru

St. Petersburg Branch, Steklov Mathematical Institute, Russian Academy of Sciences, Fontanka 27, St. Petersburg 191023, Russia
E-mail address: inp@pdmi.ras.ru

Received 20/JUN/2007

Translated by THE AUTHORS