J Algebr Comb (2008) 27: 173–185
DOI 10.1007/s10801-007-0081-4

On cyclotomic schemes over finite near-fields

J. Bagherian · Ilia Ponomarenko · A. Rahnamai Barghi

Received: 24 March 2006 / Accepted: 22 May 2007 /
Published online: 16 June 2007

Abstract We introduce a concept of cyclotomic association scheme over a finite near-field $\mathbb{K}$. It is proved that any isomorphism of two such nontrivial schemes is induced by a suitable element of the group $\mathrm{AGL}(V)$, where V is the linear space associated with $\mathbb{K}$. A sufficient condition on a cyclotomic scheme $\mathcal{C}$ that guarantee the inclusion $\mathrm{Aut}(\mathcal{C}) \le \mathrm{A\Gamma L}(1, \mathbb{F})$, where $\mathbb{F}$ is a finite field with $|\mathbb{K}|$ elements, is given.

Keywords Association scheme · Finite near-field · Permutation group

1 Introduction

An algebraic structure $\mathbb{K} = (\mathbb{K}, +, \circ)$ is called a (right) *near-field* if $\mathbb{K}^+ = (\mathbb{K}, +)$ is a group with the neutral element $0_{\mathbb{K}}$, $\mathbb{K}^\times = (\mathbb{K} \setminus \{0_{\mathbb{K}}\}, \circ)$ is a group, $x \circ 0_{\mathbb{K}} = 0_{\mathbb{K}}$ for all $x \in \mathbb{K}$, and

$$(x + y) \circ z = x \circ z + y \circ z, \quad x, y, z \in \mathbb{K}. \tag{1}$$

In the finite case, the group $\mathbb{K}^+$ is elementary Abelian, and the group $\mathbb{K}^\times$ is Abelian iff $\mathbb{K}$ is a field (as to near-fields theory, we refer to [13]). By the Zassenhaus theorem

I. Ponomarenko partially supported by RFFI, grants 03-01-00349, NSH-2251.2003.1.

J. Bagherian · A. Rahnamai Barghi (✉)
Institute for Advanced Studies in Basic Sciences (IASBS), P.O. Box 45195-1159, Zanjan, Iran
e-mail: rahnama@iasbs.ac.ir

J. Bagherian
e-mail: bagherian@iasbs.ac.ir

I. Ponomarenko
Petersburg Department of V.A. Steklov Institute of Mathematics, Fontanka 27, St. Petersburg 191023, Russia
e-mail: inp@pdmi.ras.ru

apart from seven exceptional cases, each finite near-field $\mathbb{K}$ is the *Dickson near-field*, i.e., there exist a finite field $\mathbb{F}_0$ and its extension $\mathbb{F}$ such that $\mathbb{F}^+ = \mathbb{K}^+$ and

$$y \circ x = y^{\sigma_x} \cdot x, \quad x, y \in \mathbb{K}, \tag{2}$$

where $\sigma_x \in \mathrm{Aut}(\mathbb{F}/\mathbb{F}_0)$ and $\cdot$ denotes the multiplication in $\mathbb{F}$. In this case, $|\mathbb{F}_0| = q$ and $|\mathbb{K}| = |\mathbb{F}| = q^n$, where q is a power of a certain prime p, and $n = [\mathbb{F} : \mathbb{F}_0]$. It can be proved that (q, n) forms a *Dickson pair*, i.e., every prime factor of n is a divisor of $q - 1$ and $4 \mid n$ implies $4 \mid (q - 1)$. There exist exactly $\varphi(n)/k$ nonisomorphic Dickson near-fields corresponding to the same Dickson pair (q, n), where k is the order of $p \pmod n$. The multiplicative group of any Dickson near-field is solvable (and even meta-cyclic).

Let $\mathbb{K}$ be a finite near-field and K be a subgroup of the group $\mathbb{K}^\times$. Set $\mathcal{R} = \{R_a\}_{a \in \mathbb{K}}$, where

$$R_a = \big\{(x, y) \in \mathbb{K}^2 : \ y - x \in a \circ K\big\}. \tag{3}$$

Then it is easily seen that any element of $\mathcal{R}$ is a 2-orbit of the permutation group

$$\Gamma(K, \mathbb{K}) = \{x \mapsto x \circ b + c, \ x \in \mathbb{K} : \ b \in K, c \in \mathbb{K}\}, \tag{4}$$

and so the pair $(\mathbb{K}, \mathcal{R})$ forms an *association scheme* on $\mathbb{K}$ (see Sect. 2 for the background on permutation groups and association schemes). We call it the *cyclotomic scheme* over the near-field $\mathbb{K}$ and denote it by $\mathrm{Cyc}(K, \mathbb{K})$. The number $|K|$ is called the *valency* of the scheme. If $K = \mathbb{K}^\times$, then the scheme is of rank 2, and we call it the *trivial* scheme. The set of all cyclotomic schemes of valency $m < q^n - 1$ over a Dickson near-field corresponding to a Dickson pair (q, n) is denoted by $\mathrm{Cyc}(q, n, m)$.

When $\mathbb{K} = \mathbb{F}$ is a field, we come to cyclotomic schemes introduced by P. Delsarte (1973), see [1, p. 66]. One can see that any two such schemes of the same valency are isomorphic. Moreover, the automorphism group of such a nontrivial scheme is a subgroup of the group $\mathrm{A\Gamma L}(1, \mathbb{F})$ (see [1, p. 389]). However, there exist a number of cyclotomic schemes over near-fields which are not isomorphic to cyclotomic schemes over fields. The main purpose of this paper is to study isomorphisms of cyclotomic schemes over near-fields.

The additive group of a finite near-field $\mathbb{K}$ being an elementary Abelian one can be identified with the additive group of a linear space $V_{\mathbb{K}}$ over the prime field contained in the center of $\mathbb{K}$. The existence of an isomorphism between a cyclotomic scheme over a near-field $\mathbb{K}$ and a cyclotomic scheme over a near-field $\mathbb{K}'$, implies that $|\mathbb{K}| = |\mathbb{K}'|$ and hence that the linear spaces $V_{\mathbb{K}}$ and $V_{\mathbb{K}'}$ are isomorphic. Thus to study isomorphisms of cyclotomic schemes, we can restrict ourselves to near-fields $\mathbb{K}$ with a fixed linear space $V = V_{\mathbb{K}}$.

Theorem 1.1 *Let $\mathcal{C}$ and $\mathcal{C}'$ be nontrivial cyclotomic schemes over near-fields $\mathbb{K}$ and $\mathbb{K}'$, respectively. Suppose that $V = V_{\mathbb{K}} = V_{\mathbb{K}'}$. Then $\mathrm{Iso}(\mathcal{C}, \mathcal{C}') \subset \mathrm{AGL}(V)$. In particular, $\mathrm{Aut}(\mathcal{C}) \le \mathrm{AGL}(V)$.*

For a trivial scheme $\mathcal{C}$, we obviously have $\mathrm{Aut}(\mathcal{C}) = \mathrm{Sym}(\mathbb{K})$. Thus the inclusion $\mathrm{Aut}(\mathcal{C}) \le \mathrm{AGL}(V)$ holds only if $|\mathbb{K}| \le 4$. In general, the right-hand side of the first inclusion of Theorem 1.1 cannot be refined, because $\mathrm{Iso}(\mathcal{C}, \mathcal{C}) = \mathrm{AGL}(V)$ for a

scheme $\mathcal{C} = \mathrm{Cyc}(K, \mathbb{F})$, where $\mathbb{F}$ is a finite field of composite order, and K is the multiplicative group of the prime subfield of $\mathbb{F}$.

We prove Theorem 1.1 in Sect. 3. The key ingredient for the proof is Theorem 3.2 showing that the operation of taking the 2-closure preserves the socle of any uniprimitive 3/2-transitive permutation groups of affine type. (Here we essentially use the result of [9].) From Theorem 1.1 we deduce a criterion for the isomorphism of cyclotomic schemes (Theorem 3.4).

The second part of Theorem 1.1 can be made much more precise in some cases. For instance, if the cyclotomic scheme $\mathcal{C} = \mathrm{Cyc}(K, \mathbb{K})$ is imprimitive, then $\mathrm{Aut}(\mathcal{C}) = \Gamma(K, \mathbb{K})$ (Corollary 3.5). In general, this equality does not hold even for a cyclotomic scheme over a finite field, because the group $\mathrm{Aut}(\mathcal{C})$ can contain some automorphisms of this field. However, we are able to specify the automorphisms of a cyclotomic scheme by using Zsigmondy prime divisors of its valency.

Definition 1.2 *Given integers $q, n \in \mathbb{N}$, a prime divisor r of $q^n - 1$ is called a Zsigmondy prime for (q, n) if r does not divide $q^i - 1$ for all $1 \le i < n$. The set of all such primes greater than a fixed number $k \in \mathbb{N}$ is denoted by $Z_k(q, n)$.*

It is known that at least one Zsigmondy prime for (q, n) exists unless $(q, n) = (2, 6)$, or $q + 1$ is a power of 2 and $n = 2$ (see, e.g., [11]). Moreover, any such prime is of the form $r = an + 1$ for some $a \ge 1$.

Theorem 1.3 *Let $\mathcal{C} \in \mathrm{Cyc}(p^d, n, m)$ be a cyclotomic scheme over a Dickson near-field and $k = dn$. Then $\mathrm{Aut}(\mathcal{C}) \le \mathrm{A\Gamma L}(1, p^k)$ whenever m has a prime divisor $r \in Z_{2k+1}(p, k)$.*

From Lemma 4.2 it follows that for a fixed p^d the set $Z_{2k+1}(p, k)$ is not empty for all sufficiently large k. This fact enables us to prove that the hypothesis of Theorem 1.3 is satisfied in many cases. More precisely, the following statement holds.

Theorem 1.4 *Let $\mathcal{C} \in \mathrm{Cyc}(p^d, n, m)$ be a cyclotomic scheme over a Dickson near-field and $q = p^d$. Then $\mathrm{Aut}(\mathcal{C}) \le \mathrm{A\Gamma L}(1, q^n)$ for all $n \gg q$ such that $|Z_{2dn+1}(p, dn)| \ne 1$.*

Theorem 1.4 is proved in Sect. 4 by means of the classification of linear groups with orders having certain large prime divisors given in [4]. We believe that a more delicate analysis of this classification could improve our result to show that given a prime power q for all but finitely many Dickson pairs (q, n), the inclusion $\mathrm{Aut}(\mathcal{C}) \le \mathrm{A\Gamma L}(1, q^n)$ holds for all nontrivial cyclotomic schemes $\mathcal{C}$ over a Dickson near-field corresponding to (q, n).

2 Permutation groups and association schemes

2.1

Concerning basic facts of finite permutation group theory, we refer to [3]. Let V be a finite set, $\Gamma \le \mathrm{Sym}(V)$, and $m \in \mathbb{N}$. Denote by $\mathrm{Orb}_m(\Gamma)$ the set of all orbits of the

induced action of Γ on the set V^m; these orbits are called the *m-orbits* of Γ. The largest subgroup of $\mathrm{Sym}(V)$ the m-orbits of which coincide with those of Γ is called the *m-closure* of Γ; we denote it by $\Gamma^{(m)}$.

Let U be a set with at least two elements, and let $m \geq 2$ be an integer. Following [9], we say that a permutation group $G \leq \mathrm{Sym}(V)$ *preserves a product decomposition* U^m of V if the latter can be identified with the Cartesian product U^m in such a way that G is a subgroup of the wreath product $\mathrm{Sym}(U) \wr \mathrm{Sym}(m)$ in product action. Any element g of the latter group induces uniquely determined permutations $g_1, \ldots, g_m \in \mathrm{Sym}(U)$ and $\sigma \in \mathrm{Sym}(m)$ such that

$$(u_1, \ldots, u_m)^g = \bigl(u_{i_1}^{g_{i_1}}, \ldots, u_{i_m}^{g_{i_m}}\bigr), \quad \text{where } i_j = j^{\sigma^{-1}}. \tag{5}$$

If G projects onto a transitive subgroup of $\mathrm{Sym}(m)$, then the subgroup of index m in G stabilizing the first entry of points of U^m induces a subgroup of $\mathrm{Sym}(U)$ by permuting the first entries of points of $V = U^m$; this subgroup is called the group *induced by G on U*. The following statement being a special case of result [9, Lemma 4.1] will be used in Sect. 3. Below a primitive group is called *uniprimitive* if it is not 2-transitive, and it is called of *affine type* if its socle is Abelian.

Theorem 2.1 *Let $G \leq \mathrm{Sym}(V)$ be a uniprimitive group of affine type. Suppose that $\mathrm{soc}(G) \neq \mathrm{soc}(G^{(2)})$. Then G and $G^{(2)}$ preserve a product decomposition $V = U^m$ such that $|U| \geq 5$, $m \geq 2$, and the group induced by $G^{(2)}$ on U contains $\mathrm{Alt}(U)$.*

2.2

Let V be a finite set and $\mathcal{R}$ a partition of the set V^2 containing its diagonal $\Delta(V)$ and closed with respect to the permutation of coordinates. The pair $\mathcal{C} = (V, \mathcal{R})$ is called an *association scheme* or a *scheme* on V if, given binary relations $R, S, T \in \mathcal{R}$, the number

$$\bigl|\bigl\{v \in V : (u, v) \in R, (v, w) \in S\bigr\}\bigr|$$

does not depend on the choice of $(u, w) \in T$. The elements of $\mathcal{R}$ and the number $|\mathcal{R}|$ are called the *basis relations* and the *rank* of $\mathcal{C}$ respectively. The scheme is called *imprimitive* if a union of some of its basis relations is an equivalence relation on V other than $\Delta(V)$ and V^2; otherwise the scheme is called *primitive* whenever $|V| > 1$.

Two schemes $\mathcal{C} = (V, \mathcal{R})$ and $\mathcal{C}' = (V', \mathcal{R}')$ are called *isomorphic* if there exists a bijection $f : V \to V'$, called the *isomorphism* from $\mathcal{C}$ to $\mathcal{C}'$, such that $\mathcal{R}^f = \mathcal{R}'$, where $\mathcal{R}^f = \{R^f : R \in \mathcal{R}\}$ with $R^f = \{(u^f, v^f) : (u, v) \in R\}$. The set of all such isomorphisms is denoted by $\mathrm{Iso}(\mathcal{C}, \mathcal{C}')$. The group $\mathrm{Iso}(\mathcal{C}) = \mathrm{Iso}(\mathcal{C}, \mathcal{C})$ contains the normal subgroup

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

called the *automorphism group* of the scheme $\mathcal{C}$.

A wide class of schemes comes from permutation groups as follows. Let $\Gamma \leq \mathrm{Sym}(V)$ be a permutation group and $\mathcal{R} = \mathrm{Orb}_2(\Gamma)$. Then the pair $\mathrm{Inv}(\Gamma) = (V, \mathcal{R})$ is a scheme and

$$\mathrm{Aut}\bigl(\mathrm{Inv}(\Gamma)\bigr) = \Gamma^{(2)}.$$

In particular, any cyclotomic scheme $\mathrm{Cyc}(K,\mathbb{K})$ over a near-field $\mathbb{K}$ equals the scheme $\mathrm{Inv}(\Gamma)$ with $\Gamma=\Gamma(K,\mathbb{K})$ (see (4)). One can prove that this scheme is primitive iff so is the group Γ.

2.3

Let $\mathbb{K}$ be a near-field and $K\le\mathbb{K}^\times$. Then the group $\Gamma(K,\mathbb{K})$ defined by (4) can be naturally identified with a subgroup of the group $\mathrm{AGL}(V)$, where $V=V_{\mathbb{K}}$ (see Sect. 1). Under this identification, the group K (considered as a subgroup of the group $\Gamma(K,\mathbb{K})$) goes to a subgroup of the group $\mathrm{GL}(V)$. This subgroup is called the *base group* of the cyclotomic scheme $\mathrm{Cyc}(K,\mathbb{K})$.

Theorem 2.2 *Let $\mathcal{C}$ be a cyclotomic scheme over a near-field $\mathbb{K}$. Then $\mathcal{C}$ is primitive iff the base group of $\mathcal{C}$ is irreducible.*

Proof Let $\mathcal{C}=\mathrm{Cyc}(K,\mathbb{K})$ for some group $K\le\mathbb{K}^\times$. Then the scheme $\mathcal{C}$ is primitive iff the group $\Gamma=\Gamma(K,\mathbb{K})$ is primitive (see Subsect. 2.2). However, from [3, Theorem 4.7.A] it follows that the latter statement holds iff the stabilizer of the point $0_{\mathbb{K}}$ in the group Γ is an irreducible subgroup of the group $\mathrm{GL}(V_{\mathbb{K}})$. Since this stabilizer coincides with the base group of the scheme $\mathcal{C}$, we are done. □

It should be noted that the base group of a primitive cyclotomic scheme $\mathrm{Cyc}(K,\mathbb{K})$ can be primitive (as a linear group) or not. For example, it is always primitive for $K=\mathbb{K}^\times$, and it is imprimitive for $K=\{1\}$ if the number $|\mathbb{K}|$ is a composite one.

Corollary 2.3 *The cyclotomic scheme $\mathcal{C}$ in Theorem 1.3 is primitive.*

Proof Let G be the base group of the scheme $\mathcal{C}$. Then G is a solvable subgroup of the group $\mathrm{GL}(k,p)$, and r divides the order m of G. By [6, Proposition 6.3] this implies that the group G is irreducible. Thus the scheme $\mathcal{C}$ is primitive by Theorem 2.2. □

Let V be a finite dimensional linear space over a finite prime field, and let $G\le\mathrm{GL}(V)$ be an irreducible Abelian group. Then G is a cyclic group and its linear span $L(G)$ in the algebra $\mathrm{End}(V)$ is a finite field with $|V|$ elements (see [6, Lemma 0.5]). The multiplicative group of this field acts regularly on nonzero vectors of V, i.e., this group is a Singer subgroup of the group $\mathrm{GL}(V)$. So, given a fixed nonzero $u_0\in V$, the mapping

$$\tau: L(G)\to V,\quad A\mapsto Au_0,$$

is a bijection. This defines a field $\mathbb{F}=\mathbb{F}(G)$ with elements from V such that $\mathbb{F}^+$ coincides with the additive group of the linear space V. Clearly, $\tau(G)\le\mathbb{F}^\times$.

Theorem 2.4 *Any primitive cyclotomic scheme with Abelian base group is a cyclotomic scheme over a field.*

Proof Let $\mathcal{C}=\mathrm{Cyc}(K,\mathbb{K})$ be a primitive cyclotomic scheme and $V=V_{\mathbb{K}}$. Suppose that its base group $G\le\mathrm{GL}(V)$ is Abelian. Then G is irreducible by Theorem 2.2.

This enables us to construct the field $\mathbb{F} = \mathbb{F}(G)$. From the definition of this field it follows that $\mathbb{F}^+ = \mathbb{K}^+$ and

$$x \circ y = x \cdot y, \quad x \in V,\ y \in M,$$

where $M = \tau(G)$, and $\circ$ and $\cdot$ denote the multiplications in $\mathbb{K}$ and $\mathbb{F}$, respectively. This implies that $\Gamma(K, \mathbb{K}) = \Gamma(M, \mathbb{F})$, and hence $\mathcal{C} = \mathrm{Cyc}(M, \mathbb{F})$ is a cyclotomic scheme over the field $\mathbb{F}$. □

3 An isomorphism criterion for cyclotomic schemes

3.1

In this section, we prove Theorem 1.1. For cyclotomic schemes with primitive base group we will use Theorem 2.1. In the imprimitive case, we need an auxiliary result on 3/2-transitive groups, where by such a group we mean a transitive permutation group Γ for which the orbits of its one point stabilizer Γ_v other than $\{v\}$ all have the same size.

Lemma 3.1 *Let $G \le \mathrm{Sym}(V)$ be a 3/2-transitive group preserving a product decomposition $V = U^m$ for $m \ge 2$. Then the stabilizer $G_{u,v}$ of some points $u, v \in V$ is an Abelian 2-group.*

Proof Let $u \in V$ and $I = \{1, \dots, m\}$. Without loss of generality we may assume that $u = (u_0, \dots, u_0) \in U^m$ for some $u_0 \in U$. Then from (5) it follows that $u_0^{g_i} = u_0$ for all $g \in G_u$ and all $i \in I$. So the cardinality of the set $I_v = \{i \in I :\ v_i \ne u_0\}$, where v_i is the ith component of $v \in V$, does not depend on the choice of v inside of an orbit of the group G_u. Thus, the sets

$$V_k = \big\{v \in V :\ |I_v| = k\big\}, \quad k = 1, 2, \tag{6}$$
$$R = \big\{(v, w) \in V_1 \times V_2 :\ v_i = w_i \text{ for the unique } i \in I_v\big\}$$

are G_u-invariant. Obviously, $|R_{\mathrm{in}}(w)| = 2$ for all $w \in V_2$ where $R_{\mathrm{in}}(w) = \{v \in V : (v, w) \in R\}$. We divide the remaining argument into a sequence of claims.

Claim 1 Let $X \in \mathrm{Orb}(G_u, V_1)$, $Y \in \mathrm{Orb}(G_u, V_2)$, and $S = R \cap (X \times Y)$. Then

$$\big|S_{\mathrm{out}}(x)\big| \le 2, \quad x \in X,$$

where $S_{\mathrm{out}}(x) = \{v \in V :\ (x, v) \in S\}$. Indeed, since S is a G_u-invariant relation, the numbers $|S_{\mathrm{out}}(x)|$ and $|S_{\mathrm{in}}(y)|$ do not depend on $x \in X$ and $y \in Y$, respectively. If we denote them by a and b, then obviously $|X|a = |Y|b$. Taking into account that $|X| = |Y|$ due to 3/2-transitivity of G, we conclude that $a = b \le 2$ (see the above remark).

Claim 2 Let x and y be elements of V_1 such that $I_x \neq I_y$. Then

$$\left|y^{G_{u,x}}\right| \leq 2.$$

Indeed, let $I_x = \{i\}$ and $I_y = \{j\}$ for some distinct $i, j \in I$. Then there exists a uniquely determined element $w \in V_2$ such that $x_i = w_i$ and $y_j = w_j$. Denote by X and Y the orbits of the group G_u containing x and w, respectively. From Claim 1, it follows that $S_{\mathrm{out}}(x) = \{w, w'\}$ for some $w' \in Y$. Since the set $S_{\mathrm{out}}(x)$ is obviously $G_{u,x}$-invariant, we conclude that so is the set $R_{\mathrm{in}}(w) \cup R_{\mathrm{in}}(w')$. However, this set contains at most three elements two of which are x and y. Thus

$$\left|y^{G_{u,x}}\right| \leq \left|\left(R_{\mathrm{in}}(w) \cup R_{\mathrm{in}}(w')\right) \setminus \{x\}\right| \leq 2,$$

which proves the claim.

Claim 3 Let $(x, w) \in V_1 \times V_2$. Then the transitive constituent H of the group $G_{u,x}$ induced by its action on the set $Y = w^{G_{u,x}}$ is a 2-group. Indeed, without loss of generality we may assume that $|Y| > 2$ and $I_w = \{i, j\}$ for some distinct $i, j \in I$. Then $i, j \notin I_x$, since otherwise $Y \subset R_{\mathrm{out}}(x)$ and hence $|Y| \leq 2$ by Claim 1. Set y to be the unique element of $V_1 \setminus \{x\}$ such that $y_i = w_i$. By Claim 2 the set $X = y^{G_{u,x}}$ consists of (not necessary distinct) elements $y, z \in V_1$, whence by Claim 1 it follows that

$$Y = S_{\mathrm{out}}(y) \cup S_{\mathrm{out}}(z), \quad 1 \leq \left|S_{\mathrm{out}}(y)\right| = \left|S_{\mathrm{out}}(z)\right| \leq 2.$$

Since $|Y| > 2$ and $|S_{\mathrm{in}}(w)| = |S_{\mathrm{in}}(w')|$ for all $w' \in Y$, we conclude that $S_{\mathrm{out}}(y)$ and $S_{\mathrm{out}}(z)$ are disjoint blocks of the group H, and each of them is of size 2. This implies that H is a 2-group isomorphic to a subgroup of the group $\mathrm{Sym}(2) \wr \mathrm{Sym}(2)$.

Claim 4 The action of G_u on V_2 is faithful. Indeed, any $g \in G_u$ is of the form (5). Suppose that $w^g = w$ for all $w \in V_2$. Then, given $i \in I$ and all $w \in V_2$ such that $\{i, j\} \subset I_w$ and $w_i = w_j$ where $j = i^\sigma$, we have

$$w_j = (w_{i_j})^{g_{i_j}} = (w_i)^{g_i} = (w_j)^{g_i}.$$

This implies that $g_i = \mathrm{id}_U$ for all $i \in I$. Next, if $\sigma \neq \mathrm{id}_I$, then obviously $w^g \neq w$ for all $w \in V_2$ such that $I_w = \{i, j\}$ and $w_i \neq w_j$, where $j = i^\sigma$. Thus $g = \mathrm{id}_V$, and we are done.

To complete the proof of Lemma 3.1 take $v \in V_1$. Denote by K the direct product of transitive constituents of the group $G_{u,v}$ corresponding to its orbits contained in the set V_2. Then K is a 2-group by Claim 3. On the other hand, by Claim 4 the group $G_{u,v}$ is isomorphic to a subgroup of the group K. Thus $G_{u,v}$ is a 2-group. □

Theorem 3.2 *Let $G \leq \mathrm{Sym}(V)$ be a uniprimitive 3/2-transitive group of affine type. Then $\mathrm{soc}(G) = \mathrm{soc}(\Gamma)$, where $\Gamma = G^{(2)}$.*

Proof Suppose that $\mathrm{soc}(G) \neq \mathrm{soc}(\Gamma)$. Then from Theorem 2.1 it follows that the groups G and Γ preserve a product decomposition $V = U^m$ such that $|U| \geq 5$,

$m \geq 2$, and the group induced by Γ on U contains $\mathrm{Alt}(U)$. This implies that

$$|\Gamma| = am\big|\mathrm{Alt}(U)\big| \tag{7}$$

for some $a \in \mathbb{N}$. On the other hand, the group Γ obviously is 3/2-transitive. Denote by d the size of an orbit of its one point stabilizer Γ_v other than $\{v\}$. Then it is easy to see that $d = me$ for some divisor e of $|U| - 1$ (it suffices to check the orbit of a point from the set V_1 defined in (6)). By Lemma 3.1 for $G = \Gamma$ this implies that

$$|\Gamma| = |V|me2^k \tag{8}$$

for some $k \in \mathbb{N}$. Thus equalities (7) and (8) show that $|\mathrm{Alt}(U)|$ divides $|V|e2^k$. Since e divides $|U| - 1$, it follows that $(|U| - 2)!$ divides $|V|2^{k+1}$. However, this is impossible for $|U| \geq 5$, since $|V|$ is a prime power (we used the fact that G is of affine type). □

From Theorem 3.2 it follows that $G^{(2)}$ is a uniprimitive 3/2-transitive group of affine type. If in addition, the group G preserves a product decomposition, then the same decomposition is preserved by $G^{(2)}$. Thus, in this case, the form of this group can be found by means of the classification of 3/2-transitive imprimitive linear groups given in [8].

3.2

In this subsection we fix a near-field $\mathbb{K}$ and a cyclotomic scheme $\mathcal{C}$ over $\mathbb{K}$ and denote by $T = T_V$ the translation group of the linear space $V = V_{\mathbb{K}}$. Clearly, $T \leq \mathrm{Sym}(V)$.

Lemma 3.3 *If the scheme $\mathcal{C}$ is nontrivial, then T is a characteristic subgroup of the group* $\mathrm{Aut}(\mathcal{C})$. *More exactly, the following statements hold*:

(1) *If $\mathcal{C}$ is imprimitive, then* $\mathrm{Aut}(\mathcal{C})$ *is a Frobenius group with kernel T.*
(2) *If $\mathcal{C}$ is primitive, then* $T = \mathrm{soc}(\mathrm{Aut}(\mathcal{C}))$.

Proof Let $\mathcal{C} = \mathrm{Cyc}(K, \mathbb{K})$ and $\Gamma = \Gamma(K, \mathbb{K})$, where $K < \mathbb{K}^\times$ (see (4)). Then $\mathcal{C} = \mathrm{Inv}(\Gamma)$ and so $\mathrm{Aut}(\mathcal{C}) = \Gamma^{(2)}$. On the other hand, it is easy to see that the orbits of the group Γ_v other than $\{v\}$ all have the same size $|K|$. This implies that the group Γ and hence the group $\mathrm{Aut}(\mathcal{C})$ is 3/2-transitive.

Let $\mathcal{C}$ be an imprimitive scheme. Then the group $\mathrm{Aut}(\mathcal{C})$ is imprimitive. Since any 3/2-transitive group is either primitive or a Frobenius group [14, Theorem 10.4], it follows that $\mathrm{Aut}(\mathcal{C})$ is a Frobenius group. The kernel of this group is of order $|V| = |T|$ and contains all fixed-point-free elements of the group Γ. Thus the kernel coincides with T, which proves statement (1).

Let $\mathcal{C}$ be a primitive scheme. Then the group Γ is primitive and T is a normal Abelian subgroup of it. This implies that the socle of Γ is Abelian and hence coincides with T (see [3, Theorem 4.3.B]). Thus Γ is a uniprimitive 3/2-transitive group of affine type. By Theorem 3.2 this implies that

$$T = \mathrm{soc}(\Gamma) = \mathrm{soc}\big(\Gamma^{(2)}\big) = \mathrm{soc}\big(\mathrm{Aut}(\mathcal{C})\big),$$

which completes the proof of the lemma. □

Proof of Theorem 1.1 Let $f \in \mathrm{Iso}(\mathcal{C}, \mathcal{C}')$. Then the bijection f induces an isomorphism between permutation groups $\mathrm{Aut}(\mathcal{C})$ and $\mathrm{Aut}(\mathcal{C}')$. Since these groups are transitive, without loss of generality we may assume that f leaves the point $0 \in V$ fixed. Then it suffices to verify that f belongs to the group $\mathrm{Aut}(T) = \mathrm{GL}(V)$. However, the schemes $\mathcal{C}$ and $\mathcal{C}'$ and hence the groups $\mathrm{Aut}(\mathcal{C})$ and $\mathrm{Aut}(\mathcal{C}')$ are primitive or not simultaneously. Thus the required statement follows from Lemma 3.3. □

3.3

To make the statements of Theorem 1.1 more precise, given a group $G \le \mathrm{GL}(V)$, we set

$$\overline{G} = G^{(1)} \cap \mathrm{GL}(V). \tag{9}$$

Clearly, $\overline{G}$ coincides with the largest group $H \le \mathrm{GL}(V)$ such that $\mathrm{Orb}(H) = \mathrm{Orb}(G)$.

Theorem 3.4 *Under the conditions of Theorem 1.1, denote by G and G' the base groups of the schemes $\mathcal{C}$ and $\mathcal{C}'$, respectively. Then these schemes are isomorphic iff the groups $\overline{G}$ and $\overline{G'}$ are conjugate in* $\mathrm{GL}(V)$. *Moreover,* $\mathrm{Aut}(\mathcal{C}) = T\overline{G}$.

Proof The first part of the theorem follows from the second one. Indeed, set $\Gamma = \mathrm{Aut}(\mathcal{C})$ and $\Gamma' = \mathrm{Aut}(\mathcal{C}')$. Then by Theorem 1.1 the schemes $\mathcal{C}$ and $\mathcal{C}'$ are isomorphic iff there exists $g \in \mathrm{GL}(V)$ such that $g^{-1}\Gamma g = \Gamma'$ or, equivalently, that $g^{-1}\Gamma_v g = \Gamma'_v$ where v is the zero vector of the linear space V. Since by the second part $\Gamma_v = \overline{G}$ and $\Gamma'_v = \overline{G'}$, we are done.

To prove the second part of the theorem we note that from Theorem 1.1 it follows that $\Gamma = T\Gamma_v$ and $\Gamma_v \le \mathrm{GL}(V)$. Since obviously $\mathrm{Orb}(\Gamma_v) = \mathrm{Orb}(G)$, we conclude that $\Gamma_v \le G^{(1)}$ and $\mathrm{Orb}(\Gamma_v) = \mathrm{Orb}(\overline{G})$. This shows that $\mathrm{Orb}_2(\Gamma) = \mathrm{Orb}_2(T\overline{G})$, whence by maximality of the 2-closure it follows that $T\overline{G} \le \Gamma$. Thus $\mathrm{Aut}(\mathcal{C}) = \Gamma = T\overline{G}$, and we are done. □

For imprimitive cyclotomic schemes, Theorem 3.4 can be slightly simplified. Indeed, in this case, $\mathrm{Aut}(\mathcal{C})$ is a Frobenius group by statement (1) of Lemma 3.3. So

$$|\overline{G}| = \left|\mathrm{Aut}(\mathcal{C})_v\right| = |X| = |G|,$$

where X is an orbit of the group $\mathrm{Aut}(\mathcal{C})_v$ other than $\{v\}$. Since also $G \le \overline{G}$, we have $\overline{G} = G$. Thus by Theorem 3.4 we obtain the following statement.

Corollary 3.5 *Let the cyclotomic schemes $\mathcal{C}$ and $\mathcal{C}'$ be imprimitive. Then they are isomorphic iff their base groups are conjugate in* $\mathrm{GL}(V)$. *Moreover,* $\overline{G} = G$ *and* $\mathrm{Aut}(\mathcal{C}) = TG$.

4 Proof of Theorems 1.3 and 1.4

The main tool of this section is Theorem 4.1 below which is deduced from the classification of linear groups with orders having certain large prime divisors [4]. In our

case such a divisor is a Zsigmondy prime r for a pair (q, n), where q is a prime power and $n \in \mathbb{N}$. Any cyclic group $G \leq \mathrm{GL}(n, q)$ of order r is irreducible [6, Proposition 6.3], and the linear span $L(G)$ of it in $\mathrm{Mat}(n, q)$ is a finite field $\mathbb{F}$ with q^n elements. We will identify the group $\Gamma\mathrm{L}(1, \mathbb{F})$ with a subgroup of $\mathrm{GL}(n, q)$. Below a group $\Gamma \leq \mathrm{GL}(n, q)$ is called *half-transitive* if the action of it on the set V^* of nonzero vectors in the underlying linear space is intransitive and the orbits of this action all have the same size.

Theorem 4.1 *Let $G \leq \Gamma \leq \mathrm{GL}(n, q)$ where $(q, n) \notin \{(2, 4), (2, 6)\}$. Suppose that G is a cyclic group of order $r \in Z_{2n+1}(q, n)$ and that the group Γ is half-transitive. Then $\Gamma \leq \Gamma\mathrm{L}(1, \mathbb{F})$, where $\mathbb{F} = L(G)$.*

Proof It suffices to prove that $\Gamma \leq \Gamma\mathrm{L}(1, q^n)$. Indeed, in this case $\Gamma \leq \Gamma\mathrm{L}(1, \mathbb{F}')$ for some field $\mathbb{F}' \subset \mathrm{Mat}(n, q)$ with q^n elements. So the multiplicative group of $\mathbb{F}'$ normalizes G and hence normalizes the Singer subgroup $\mathbb{F}^\times \subset L(G)$ of the group $\mathrm{GL}(n, q)$. However, the normalizer of $\mathbb{F}^\times$ in $\mathrm{GL}(n, q)$ contains the unique Singer subgroup [2, Proposition 2.5]. This proves that $\mathbb{F}' = \mathbb{F}$.

Suppose that Γ is a solvable group. If r divides the order of the Fitting subgroup of Γ, then this group is isomorphic to a subgroup of $\Gamma\mathrm{L}(1, q^n)$ [6, Lemma 6.4]. Otherwise from Lemma 6.7 of the same book it follows that $r = n + 1$, which contradicts the hypothesis on r. Thus the required statement is true for solvable groups. In particular, we may assume that $n \geq 2$ and that the group Γ is nonsolvable.

Let $n = 2$. From the classification of all subgroups of $\mathrm{GL}(2, q)$ given in [7, Proposition 8.1] it follows that any nonsolvable irreducible subgroup of $\mathrm{GL}(2, q)$, say Γ, has a subgroup H such that $[\Gamma : H]$ divides $q - 1$ and

$$H \geq \mathrm{SL}(2, q') \quad \text{or} \quad H/Z \cong \mathrm{Alt}(5),$$

where $q' \geq 5$ is a divisor of q, and Z is the subgroup of scalar matrices contained in H. However, in the former case, this group acts transitively on the set V^*, and the intransitivity of Γ gives a contradiction. In the latter case, the prime divisors of the number $|\Gamma|$ are over those of the number $(q - 1)5!/2$, which contradicts the assumption that $r \in Z_{2n+1}(q, n)$ for $n = 2$. It should be mentioned that in this case we proved the required statement for the group Γ which is intransitive but not necessary half-transitive.

Let $n \geq 3$. The Zsigmondy prime r for the pair (q, n) is a primitive prime divisor of $q^n - 1$ in the sense of [4]. Since r divides the order of the group Γ, this group satisfies the hypothesis of the Main Theorem of that paper for $d = e = n$. In this case, the Main Theorem shows that, for the group Γ (not necessary half-transitive) and $r > 2n + 1$, one of the following statements holds:

(1) Γ has a normal subgroup Γ' isomorphic to one of the classical groups $\mathrm{SL}(n, q')$, $\mathrm{Sp}(n, q')$, $\mathrm{SU}(n, q'^{1/2})$, or $\Omega^\epsilon(n, q')$, where r divides the order of Γ', q' is the order of a subfield of the ground field, and $\epsilon \in \{\circ, +, -\}$,
(2) $\Gamma \leq \mathrm{GL}(n/m, q^m) \cdot m$, and the number r divides the order of the group $\Gamma \cap \mathrm{GL}(n/m, q^m)$, where m is a divisor of n other than 1,
(3) $(q, n) = (2, 4)$ or $(2, 6)$,

where $\mathrm{GL}(n/m, q^m) \cdot m$ is the general linear group $\mathrm{GL}(n/m, q^m)$ embedded to $\mathrm{GL}(n, q)$ and extended by the group of automorphisms of the field extension $\mathrm{GF}(q^m)/\mathrm{GF}(q)$. However, the case (3) does not arise by the hypothesis of the theorem. Let us prove that the same is true in the other two cases.

We claim that the group Γ contains a normal nonsolvable subgroup H_0 isomorphic to one of the groups $\mathrm{SL}(n_0, q_0)$, $\mathrm{Sp}(n_0, q_0)$, $\mathrm{SU}(n_0, q_0^{1/2})$, or $\Omega^\epsilon(n_0, q_0)$, where r divides the order of H_0, $n_0 \geq 2$ is a divisor of n, and q_0 is the order of a subfield of the field $\mathrm{GF}(q^{n/n_0})$. Indeed, in case (1) we can take $H_0 = \Gamma'$ and $(n_0, q_0) = (n, q')$. Otherwise, case (2) holds. It is easy to see that $\Gamma_0 = \Gamma \cap \mathrm{GL}(n/m, q^m)$ is a normal subgroup of Γ and Γ/Γ_0 is a cyclic group of order coprime to r. This implies that the group Γ has a characteristic subgroup $H \leq \Gamma_0$ such that the factor group Γ/H is solvable and each prime divisor of its order divides m. In particular,

$$G \leq H \leq \mathrm{GL}\big(n/m, q^m\big),$$

and H is solvable iff Γ is so. If case (2) holds for the group H, we repeat this argument with $\Gamma = H$ and $(n, q) = (n/m, q^m)$. Finally, we find a nonsolvable characteristic subgroup H of the group Γ such that $G \leq H \leq \mathrm{GL}(n_1, q_1)$, where $n_1 \geq 2$ is a divisor of n, and q_1 is the order of a subfield of the field $\mathrm{GF}(q^{n/n_1})$. Moreover, we may assume that case (1) holds for $\Gamma = H$ and $(n, q) = (n_1, q_1)$. Since the corresponding classical group Γ' is a characteristic subgroup of H, we are done with $H_0 = \Gamma'$ and $(n_0, q_0) = (n_1, q_1')$.

To complete the proof we will show that the above claim contradicts the half-transitivity of Γ. Without loss of generality we assume that $n_0 \geq 3$ (see above). Then the groups $\mathrm{SL}(n_0, q_0)$ and $\mathrm{Sp}(n_0, q_0)$ act transitively on the set V^* [5, Lemma 2.10.5]. By the intransitivity of Γ this implies that H_0 cannot be one of these groups. Therefore we may assume that H_0 is either the unitary group $\mathrm{SU}(n_0, q_0^{1/2})$ or the orthogonal group $\Omega^\epsilon(n_0, q_0)$. Given an element λ of the ground field $\mathbb{F}$, set

$$V_\lambda^* = \begin{cases} \big\{v \in V^* :\ f(v, v) = \lambda\big\} & \text{if } H_0 = \mathrm{SU}\big(n_0, q_0^{1/2}\big), \\ \big\{v \in V^* :\ Q(v) = \lambda\big\} & \text{if } H_0 = \Omega^\epsilon(n_0, q_0), \end{cases}$$

where f (resp. Q) is the nondegenerate unitary (resp. quadratic) form corresponding to H_0. By the same lemma, for $n_0 \geq 3$, we obtain that

$$\mathrm{Orb}\big(H_0, V^*\big) = \big\{V_\lambda^* :\ \lambda \in \mathbb{F}\big\} \quad \text{unless } n_0 = 3,\ H_0 = \Omega(3, q_0),\ \lambda = 0,$$

and in the exceptional case the set V_λ^* is the union of two H_0-orbits each of size $(q_0^2 - 1)/2$. Clearly, the number $a_\lambda = |V_\lambda^*|$ does not depend on $\lambda \neq 0$. So using the explicit formulas for a_0 (see Lemma 10.4 and Theorem 11.5 in [12]), one can see that q_0 is coprime to a_0 and divides a_λ for all $\lambda \neq 0$. Since Γ acts on the set $\mathrm{Orb}(H_0, V^*)$ (due to the normality of H_0 in Γ), this implies that

$$\big(V_0^*\big)^\Gamma = V_0^* \quad \text{and} \quad \big|\mathrm{Orb}\big(\Gamma, V_0^*\big)\big| \leq 2.$$

By the half-transitivity of Γ this shows that the size of any $X \in \mathrm{Orb}(\Gamma, V^*)$ is coprime to q_0. However, this contradicts the fact that q_0 divides $|X|$ for all $X \not\subset V_0^*$, and we are done. □

Proof of Theorem 1.3 The hypothesis shows that r divides the order m of the base group of the scheme $\mathcal{C}$. So this group contains a cyclic subgroup G of order r. By Theorem 1.1 we have

$$G \le \Gamma \le \mathrm{GL}(k, p),$$

where $\Gamma = \mathrm{Aut}(\mathcal{C})_v$ with $v = 0$. Besides, the orbits in the action of Γ on V^* all have the same size $m < p^k - 1$, and hence the group Γ is half-transitive. Thus by Theorem 4.1 with $(q, n) = (p, k)$ it suffices to check only the cases $(p, k) \in \{(2, 4), (2, 6)\}$. However, the fact that $(2^d, n)$ with $dn \in \{4, 6\}$ is a Dickson pair implies that either $(d, n) = (2, 3)$ or $n = 1$. But, in the former case $k = 6$ and $Z_{2k+1}(2, k) = \emptyset$, whereas in the latter case the near-field is a field, and we are done (see Sect. 1).

The following auxiliary lemma is a combination of some number theoretical results from [10] and [11]; it will be used in the proof of Theorem 1.4. □

Lemma 4.2 *Given a prime power $q = p^d$, there exists an integer $N_q \in \mathbb{N}$ such that the set $Z_{2dn+1}(p, dn)$ is not empty for all $n > N_q$.*

Proof Given $n \in \mathbb{N}$, denote by $D(n)$ the number of distinct prime factors of n, by $P[n]$ the greatest of them, and by $\Phi_n(X)$ the cyclotomic polynomial of degree $\varphi(n)$. Then there exists a constant $C > 0$ such that

$$P\big[\Phi_{dn}(p)\big] > Cn\sqrt{\log n}/\log\log\log n \tag{10}$$

for all sufficiently large n such that $D(dn) \le \kappa \log\log(dn)$ with $\kappa = 1/(2\log 2)$ (see [10, p. 25]).

Denote by S_q the set of all integers $dn \in N$ such that (q, n) is a Dickson pair and n is greater than the minimal number $a \in \mathbb{N}$ for which $D(d)\log q \le \kappa \log\log(da)$. Then given $dn \in S_q$, we have

$$D(dn) \le D(d)D(n) \le D(d)\log q \le \kappa \log\log(dn).$$

By (10) this implies that $P[\Phi_{dn}(p)] > 2dn + 1$ for all sufficiently large $n \in S_q$. However, a prime factor r of the number $\Phi_{dn}(p)$ is not a Zsigmondy prime for (p, dn) iff $r \le dn$ (see [11, Proposition 2]). Thus there exists a positive integer N_q such that $Z_{2dn+1}(p, dn) \ne \emptyset$ for all $n > N_q$. □

Proof of Theorem 1.4 Let $\mathcal{C} = \mathrm{Cyc}(K, \mathbb{K}^\times)$, where $\mathbb{K}$ is a Dickson near-field corresponding to the Dickson pair (q, n), and the group $K \le \mathbb{K}^\times$ is of order $m < q^n$. Suppose that $n > N_q$. Then by Lemma 4.2 the set $Z_{2dn+1}(p, dn)$ is not empty. Set K' to be a maximal subgroup of $\mathbb{K}^\times$ containing K. Since the group $\mathbb{K}^\times \le \Gamma\mathrm{L}(1, q^n)$ is supersolvable, the number $[\mathbb{K}^\times : K']$ is prime. So if $|Z_{2dn+1}(p, dn)| \ne 1$, then the number $m' = |K'|$ has a prime divisor $r' \in Z_{2dn+1}(p, dn)$. This implies that the scheme $\mathcal{C}' = \mathrm{Cyc}(K', \mathbb{K}^\times)$ belongs to the class $\mathrm{Cyc}(q, n, m')$ and satisfies the hypothesis of Theorem 1.3 with r replaced by r'. Thus

$$\mathrm{Aut}(\mathcal{C}) \le \mathrm{Aut}(\mathcal{C}') \le \mathrm{A}\Gamma\mathrm{L}\big(1, q^n\big), \tag{11}$$

and we are done. □

References

1. Brouwer, A. E., Cohen, A. M., & Neumaier, A. (1989). *Distance-regular graphs*. Berlin: Springer.
2. Cossidente, A., & de Resmini, M. J. (2004). Remarks on Singer cyclic groups and their normalizers. *Designs, Codes and Cryptography*, *32*, 97–102.
3. Dixon, J. D., & Mortimer, B. (1996). *Permutation groups*. *Graduate texts in mathematics* (Vol. 163). New York: Springer.
4. Guralnick, R., Penttila, T., Praeger, C. E., & Saxl, J. (1999). Linear groups with orders having certain large prime divisors. *Proceedings of the London Mathematical Society*, *78*, 167–214.
5. Kleidman, P., & Liebeck, M. (1990). *The subgroup structure of the finite classical groups*. *London mathematical society lecture note series* (Vol. 129). Cambridge: Cambridge University Press.
6. Manz, O., & Wolf, T. R. (1993). *Representations of solvable groups*. *London mathematical society lecture note series* (Vol. 185). Cambridge: Cambridge University Press.
7. Neumann, P. M., & Praeger, C. E. (1992). A recognition algorithm for special linear groups. *Proceedings of the London Mathematical Society*, *65*, 555–603.
8. Passman, D. S. (1968). p-Solvable doubly transitive permutation groups. *Pacific Journal of Mathematics*, *26*, 555–577.
9. Praeger, C. E., & Saxl, J. (1992). Closures of finite primitive permutation groups. *The Bulletin of the London Mathematical Society*, *24*, 251–258.
10. Ribenboim, P. (2000). *My numbers, my friends. Popular lectures on number theory*. New York: Springer.
11. Roitman, M. (1997). On Zsigmondy primes. *Proceedings of the American Mathematical Society*, *125*, 1913–1919.
12. Taylor, D. E. (1992). *The geometry of the classical groups*. Berlin: Heldermann.
13. Wähling, H. (1987). *Theorie der Fastkörper*. Essen: Thales.
14. Wielandt, H. (1964). *Finite permutation groups*. New York: Academic.