On cyclotomic schemes over finite near-fields

J. Bagherian
Institute of Advanced Studies in Basic Sciences
P.O.Box: 45195-1159, Zanjan, Iran

Ilia Ponomarenko *
Petersburg Department of V.A.Steklov
Institute of Mathematics
Fontanka 27, St. Petersburg 191023, Russia
inp@pdmi.ras.ru
http://www.pdmi.ras.ru/~inp

A. Rahnamai Barghi †
Institute of Advanced Studies in Basic Sciences
P.O.Box: 45195-1159, Zanjan, Iran

Abstract

We introduce a concept of cyclotomic association scheme $\mathcal{C}$ over a finite near-field. It is proved that if $\mathcal{C}$ is nontrivial, then $\text{Aut}(\mathcal{C}) \leq \text{AGL}(V)$ where $V$ is the linear space associated with the near-field. In many cases we are able to get more specific information about $\text{Aut}(\mathcal{C})$.

Keywords: association scheme, finite near-field, permutation group

AMS Subject Classification: 05E30,12K05,20B20

*Partially supported by RFFI 05-01-00899, NSH-4329.2006.1. The author thanks the Institute for Advanced Studies in Basic Sciences (IASBS) for its hospitality during the time that this paper was written.

†Corresponding author: rahnama@iasbs.ac.ir
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

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

In finite case the group $\mathbb{K}^+$ is elementary abelian and the group $\mathbb{K}^\times$ is abelian iff $\mathbb{K}$ is a field (concerning the theory of near-fields we refer to [11]). Moreover, by the Zassenhaus theorem apart from seven exceptional cases each finite near-field $\mathbb{K}$ is the Dickson near-field, i.e. there exists a finite field $\mathbb{F}_0$ and its extension $\mathbb{F}$ such that $\mathbb{F}^+ = \mathbb{K}^+$ and

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

where $\sigma_x \in \text{Aut}(\mathbb{F}/\mathbb{F}_0)$ 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 which means that 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 $p \mod n$.

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

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

is a binary relation on the set $\mathbb{K}$. Then it is easily seen that any such a relation is a 2-orbit of the permutation group

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

and so the pair $(\mathbb{K}, \mathcal{R})$ forms an association scheme on $\mathbb{K}$ (see Section 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 $\text{Cyc}(K, \mathbb{K})$. 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 $\text{Cyc}(q, n, m)$.

When $\mathbb{K} = \mathbb{F}$ is a field, we come to cyclotomic schemes introduced by P. Delsarte (1973). One can see that any two such schemes of the same rank are isomorphic. Moreover, the automorphism group of such a nontrivial scheme is a subgroup of the group $\text{AGL}_1(\mathbb{F})$ (see [11] 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 containing in the center of $\mathbb{K}$. If there exist isomorphic cyclotomic schemes over near-fields $\mathbb{K}$ and $\mathbb{K}'$, then obviously $|\mathbb{K}| = |\mathbb{K}'|$ and hence 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 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 $\text{Iso}(\mathcal{C}, \mathcal{C}') \subset \text{AGL}(V)$. In particular, $\text{Aut}(\mathcal{C}) \leq \text{AGL}(V)$. 
For the trivial scheme $C$ we obviously have $\text{Aut}(C) = \text{Sym}(K)$. Thus the inclusion $\text{Aut}(C) \leq \text{AGL}(V)$ holds only if $|K| \leq 4$. In general case, the right-hand side of the first inclusion of Theorem 1.1 can not be reduced because $\text{Iso}(C, C) = \text{AGL}(V)$ where $C = \text{Cyc}(K, F)$ with $F$ being a finite field of composite order and $K$ being the multiplicative group of the prime subfield of $F$.

We prove Theorem 1.1 in Section 3. The key point of 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 the affine type. (Here we essentially use the result of [7].) This also gives a criterion for the isomorphism of nontrivial cyclotomic schemes (Theorem 3.4).

The second part of Theorem 1.1 can be made more precise in some cases. For instance, if the cyclotomic scheme $C = \text{Cyc}(K, F)$ is imprimitive, then $\text{Aut}(C) = \Gamma(K, K)$ (Corollary 3.6). In general case it is not true even for a cyclotomic scheme over a finite field because $\text{Aut}(C)$ can contain some automorphisms of the field. However, we are able to restrict 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 $1 \leq i < n$. The set of all such primes greater than a natural number $k$ 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. [9]). Moreover, any such prime is of the form $r = an + 1$ for some $a \geq 1$.

**Theorem 1.3** Let $C \in \text{Cyc}(p^d, n, m)$ be a cyclotomic scheme over a Dickson near-field. Suppose that $m$ has a prime divisor $r \in Z_{2dn+1}(p, dn)$. Then the group $\text{Aut}(C)$ is isomorphic to a subgroup of the group $\text{AGL}_1(p^{dn})$.

From Corollary 2.3 it follows that in the condition of Theorem 1.3 the scheme $C$ is primitive. In fact, this theorem shows also that for a sufficiently large $n$ the group $\text{Aut}(C)$, is isomorphic to a subgroup of the group $\text{AGL}_1(p^d)$ in all but one case.

**Theorem 1.4** Let $C \in \text{Cyc}(p^d, n, m)$ be a cyclotomic scheme over a Dickson near-field. Then for $n \gg q = p^d$ the group $\text{Aut}(C)$ is isomorphic to a subgroup of the group $\text{AGL}_1(q^n)$ unless $Z_{2dn+1}(p, dn) = \{r\}$ with $r^2 \nmid (q^n - 1)$ where $r = (q^n - 1)/m$.

Let $C = \text{Cyc}(K, K)$ and $C' = \text{Cyc}(K', K)$ be cyclotomic schemes of the same valency $m < q^n - 1$ over a Dickson near-field $K$ of order $q^n$. Then

$$[K^\times : K] = \text{rk}(C) - 1 = (q^n - 1)/m = \text{rk}(C') - 1 = [K^\times : K'].$$

Suppose that $r = (q^n - 1)/m$ is a prime and $r^2 \nmid (q^n - 1)$. Then the groups $K$ and $K'$ are the Hall subgroups of the group $K^\times$ and so are conjugate in it. So the schemes $C$ and $C'$, and hence the groups $\text{Aut}(C)$ and $\text{Aut}(C')$, are isomorphic. Thus Theorem 1.4 shows that given a Dickson near-field $K$ corresponding to the Dickson pair $(q, n)$ with $n \gg q$, there is at most one (up to isomorphism) nontrivial cyclotomic scheme $C$ over $K$ for which we don’t know whether $\text{Aut}(C)$ is isomorphic to a subgroup of the group $\text{AGL}_1(q^n)$. 
Theorem 1.4 is proved in Section 4 by means of the classification of linear groups with orders having certain large prime divisors, given in [4]. We believe that more delicate analysis of this classification could improve our result to show that Aut(C) is isomorphic to a subgroup of the group $\Gamma L_1(q^n)$ apart from a finite number of possible n’s for a fixed q.

2 Permutation groups and association schemes

2.1 Concerning basic facts of finite permutation group theory we refer to [3]. For a positive integer $m$ and a group $\Gamma \leq \text{Sym}(V)$ the set of orbits of the induced action of $\Gamma$ on $V^m$ is denoted by $\text{Orb}_m(\Gamma)$; the elements of this set are called $m$-orbits of $\Gamma$. The group $\Gamma$ is called $m$-closed iff it coincides with its $m$-closure $\Gamma^{(m)}$ which is by definition the largest subgroup of $\text{Sym}(V)$ with the same set of $m$-orbits as $\Gamma$.

Let $U$ be a set with at least two elements and $m \geq 2$ be an integer. Following [7] we say that a permutation group $G \leq \text{Sym}(V)$ 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 $\text{Sym}(U) \wr \text{Sym}(m)$ in product action. Any element $g$ of the latter group induces uniquely determined permutations $g_1, \ldots, g_m \in \text{Sym}(U)$ and $\sigma = \sigma_g \in \text{Sym}(m)$ such that

$$(u_1, \ldots, u_m)^g = (u_1^{g_1}, \ldots, u_m^{g_m}) \quad \text{where} \quad i_j = j^{\sigma^{-1}}.$$  \hspace{1cm} (5)$$

If $G$ projects onto a transitive subgroup of $\text{Sym}(m)$, then the subgroup of index $m$ in $G$ stabilizing the first entry of points of $U^m$ induces a subgroup of $\text{Sym}(U)$ on the set of first entries of points of $V = U^m$; this group is called the group induced by $G$ on $U$.

The following statement being a special case of result of [7, Lemma 4.1] will be used in Section 3. Below a primitive group is called uniprimitive if it is not 2-transitive, and it is called affine type if the socle of it is abelian.

**Theorem 2.1** Let $G \leq \text{Sym}(V)$ be a uniprimitive group of the affine type. Suppose that $\text{soc}(G) \neq \text{soc}(G^{(2)})$. 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 $\text{Alt}(U)$.

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

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

does not depend on the choice of $(u, w) \in T$. Two schemes $\mathcal{C} = (V, \mathcal{R})$ and $\mathcal{C}' = (V', \mathcal{R}')$ are called isomorphic if $\mathcal{R}^f = \mathcal{R}'$, for some bijection $f : V \to V'$, called the isomorphism from $\mathcal{C}$ to $\mathcal{C}'$, where $\mathcal{R}^f = \{R^f : R \in \mathcal{R}\}$ and $R^f = \{(u^f, v^f) : (u, v) \in R\}$. The set of all such isomorphisms is denoted by $\text{Iso}(\mathcal{C}, \mathcal{C}')$. The group $\text{Iso}(\mathcal{C}) = \text{Iso}(\mathcal{C}, \mathcal{C})$ contains a normal subgroup

$$\text{Aut}(\mathcal{C}) = \{g \in \text{Sym}(V) : R^g = R, R \in \mathcal{R}\}$$
called the automorphism group of \( C \).

The elements of \( V \) and \( R = R(C) \) are called the points and the basis relations of \( C \) respectively; the numbers \( \deg(C) = |V| \) and \( \text{rk}(C) = |R| \) are called the degree and the rank of \( C \). The scheme \( C \) is called imprimitive if there exists an equivalence relation \( E \) on \( V \) such that \( E \notin \{ \Delta(V), V^2 \} \) and \( E \) is a union of some basis relations of \( C \); otherwise \( C \) is called primitive whenever \( \deg(C) > 1 \).

A wide class of schemes comes from permutation groups as follows. Let \( \Gamma \leq \text{Sym}(V) \) be a permutation group and \( R \) the set of all 2-orbits of \( \Gamma \). Then the pair \( \text{Inv}(\Gamma) = (V, R) \) is a scheme and \( \text{Aut}(\text{Inv}(\Gamma)) = \Gamma(2) \).

In particular, any cyclotomic scheme \( \text{Cyc}(K, \mathbb{K}) \) over a near-field \( \mathbb{K} \) equals the scheme \( \text{Inv}(\Gamma) \) with \( \Gamma = \Gamma(K, \mathbb{K}) \). It is also true that the scheme \( \text{Inv}(\Gamma) \) is primitive iff so is the group \( \Gamma \).

**2.3** Let \( \mathbb{K} \) be a near-field and \( K \leq \mathbb{K}^\times \). Then the group \( \Gamma(K, \mathbb{K}) \) defined by (4) can be naturally identified with a subgroup of the group \( \text{AGL}(V) \) where \( V = V_K \). Under this identification the group \( K \) (considered as the subgroup of the group \( \Gamma(K, \mathbb{K}) \)) goes to a subgroup of the group \( \text{GL}(V) \). This subgroup is called the base group of the corresponding cyclotomic scheme \( \text{Cyc}(K, \mathbb{K}) \). Thus the base group is nothing else than the image of the natural linear representation of \( K \) in \( \text{GL}(V) \).

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

**Proof.** Let \( C = \text{Cyc}(K, \mathbb{K}) \) for some group \( K \leq \mathbb{K}^\times \). Then \( C = \text{Inv}(\Gamma) \) where \( \Gamma = \Gamma(K, \mathbb{K}) \). So the scheme \( C \) is primitive iff the group \( \Gamma \) is primitive. However, from \([10, \text{p.19}]\) it follows that the latter statement holds iff the stabilizer of the point \( 0_K \) in the group \( \Gamma \) is an irreducible subgroup of the group \( \text{GL}(V_K) \). Since this stabilizer coincides with the base group of the scheme \( C \), we are done.

It should be noted that for a primitive cyclotomic scheme \( \text{Cyc}(K, \mathbb{K}) \) the base group can be primitive (as a linear group) or not. The latter case is realized e.g. for \( \mathbb{K} \) being the field of order 9 and for \( K \) being the subgroup of \( \mathbb{K}^\times \) of order 4 (then \( \Gamma(K, \mathbb{K}) \) is isomorphic to the subgroup of the wreath product \( \text{Sym}(3) \wr \text{Sym}(2) \) in the product action).

**Corollary 2.3** Let \( C \) be a cyclotomic scheme satisfying the hypothesis of Theorem 1.3. Then \( C \) is primitive.

**Proof.** Let \( C = \text{Cyc}(K, \mathbb{K}^\times) \) and \( G \) be the base group of \( C \). Then \( G \leq \text{GL}(V) \) where \( V = V_K \) and \( r \) divides \( |G| = |K| = m \). So the group \( G \) is irreducible (see \([3, \text{S 6}]\)) and we are done by Theorem 2.2.

Let \( V \) be a linear space over a prime finite field and \( G \leq \text{GL}(V) \) be an irreducible abelian group. Then \( G \) is cyclic and the linear span \( F_0 = L(G) \) of it (in the algebra \( \text{Mat}(V) \)) is a finite field with \( |V| \) elements (see \([3]\)). In particular, the group \( F_0^\times \) being a Singer subgroup of \( \text{GL}(V) \), acts regularly on the set \( V^\# = V \setminus \{0_V\} \) by the multiplication of matrix to vector. So for a fixed element \( u \in V^\# \) there is a bijection

\[
\tau : F_0 \rightarrow V, \quad f \mapsto uf
\]
translating the field structure from \( \mathbb{F}_0 \) to \( V \). For the corresponding field \( \mathbb{F} = \mathbb{F}(G) \) we have \( \mathbb{F}^+ = V^+ \) and \( K \leq \mathbb{F}^\times \) where \( K \) is the permutation group on \( V \) induced by the group \( G \).

**Theorem 2.4** Any primitive cyclotomic scheme with the abelian base group is a cyclic scheme over a field.

**Proof.** Let \( \mathcal{C} = \text{Cyc}(K, \mathbb{K}) \) be a primitive cyclotomic scheme over a near-field \( \mathbb{K} \) where the group \( K \leq \mathbb{K}^\times \) is abelian. The base group \( G \leq \text{GL}(V) \) where \( V = V_\mathbb{K} \), of this scheme is isomorphic to \( K \) and hence is also abelian. Due to the primitivity of \( \mathcal{C} \) from Theorem 2.2 it follows that \( G \) is irreducible. By the definition of the field \( \mathbb{F} = \mathbb{F}(G) \) we have \( \mathbb{F}^+ = V^+ = \mathbb{K}^+ \) and \( K \leq \mathbb{F}^\times \cap \mathbb{K}^\times \). Thus \( \mathcal{C} = \text{Inv}(\Gamma(K, \mathbb{K})) = \text{Inv}(\Gamma(K, \mathbb{F})) \) is a cyclotomic scheme over the field \( \mathbb{F} \) and we are done.

## 3 An isomorphism criterion for cyclotomic schemes

### 3.1 In this section we prove Theorem 1.1. When the base group of a cyclotomic scheme is primitive as a linear group, the required statement immediately follows from Theorem 2.1. In the imprimitive case we need to strengthen the latter theorem by means of the following lemma. We recall that a transitive group \( \Gamma \leq \text{Sym}(V) \) is called \( 3/2 \)-transitive if all the orbits of its one point stabilizer \( \Gamma_v \) on \( V \setminus \{v\} \) have the same size.

**Lemma 3.1** Let \( G \leq \text{Sym}(V) \) be a \( 3/2 \)-transitive group preserving a product decomposition \( V = U^m \) where \( m \geq 2 \). Then \( G_{u,v} \) is an abelian 2-group for distinct points \( u, v \in V \).

**Proof.** Let us fix a point \( u = (u_0, \ldots, u_0) \in U^m \) where \( u_0 \in U \). Then from (5) it follows that \( u_0^g = u_0 \) for all \( g \in G_u \) and all \( i \in I = \{1, \ldots, m\} \). This implies that the cardinality of the set \( I_v = \{i \in I : v_i \neq u_0\} \) with \( v_i \) being the \( i \)th component of \( v \), does not depend on the choice of \( v \) inside of an orbit of the group \( G_u \). Thus, the sets

\[
V_k = \{v \in V : |I_v| = k\}, \quad k \in \mathbb{Z},
\]

\[
R = \{(v, w) \in V_1 \times V_2 : v_i = w_i \text{ for all } i \in I_v \cap I_w\}
\]

(6) are \( G_u \)-invariant. We note that from the definition of \( R \) it follows that \( |R_{in}(w)| = 2 \) for all \( w \in V_2 \) where \( R_{in}(v) = \{u \in V : (u, v) \in R\} \).

**Claim 1.** Let \( X_1 \in \text{Orb}(G_u, V_1) \), \( X_2 \in \text{Orb}(G_u, V_2) \) and \( S = R_{X_1,X_2} \) (here and below we set \( R_{X,Y} = R \cap (X \times Y) \) for all \( X, Y \subset V \)). Then

\[
|S_{out}(x)| = 2, \quad x \in X_1,
\]

where \( S_{out}(u) = \{v \in V : (u, v) \in S\} \). Indeed, since \( S \) is a \( G_u \)-invariant relation the numbers \( |S_{out}(x)| \) and \( |S_{in}(v)| \) do not depend on \( x \in X_1 \) and \( v \in X_2 \) respectively. Denote them by \( a_1 \) and \( a_2 \). Then \( |X_1|a_1 = |X_2|a_2 \). Taking into account that \( |X_1| = |X_2| \) due to 3/2-transitivity of \( G \), we conclude that \( a_1 = a_2 \). Since \( a_2 = 2 \) by the definition of the relation \( S \) (see (5)), and we are done.

**Claim 2.** The following inequality holds:

\[
|y^{G_u,x}| = 2, \quad x, y \in V_1, \quad I_x \neq I_y.
\]
Indeed, let \( x, y \in V_1 \). Then \( I_x = \{ i \} \) and \( I_y = \{ j \} \) for some distinct \( i, j \in I \). So there exists the uniquely determined element \( v \in V_2 \) such that \( x_i = v_i \) and \( y_j = v_j \). Then \((x,v),(y,v) \in R\). From Claim 1 with \( X_1 \) and \( X_2 \) being the orbits of the group \( G_u \) containing \( x \) and \( v \), it follows that \( S_{\text{out}}(x) = \{ v, v' \} \) for some \( v' \in X_2 \setminus \{ v' \} \) where \( S = R_{X_1,X_2} \). It is easy to see that the set \( S_{\text{out}}(x) \) is \( G_{u,x} \)-invariant and hence so is the set \( R_{\text{in}}(v) \cup R_{\text{in}}(v') \). However, this set contains at most three points and two of them are \( x \) and \( y \). So
\[
|y^{G_{u,x}}| \leq |(R_{\text{in}}(v) \cup R_{\text{in}}(v')) \setminus \{ x \}| = 2
\]
and we are done.

**Claim 3.** Let \( x \in V_1 \) and \( v \in V_2 \). Then \( (G_{u,x})_Y \) is a 2-group where \( Y = v^{G_{u,x}} \). Indeed, let \( I_v = \{ i, j \} \) for some \( i, j \in I \). Since \( i \neq j \), we can assume that \( \{ i \} \neq I_x \). Set \( y \) to be the unique element of \( V_1 \) such that \( y_i = v_i \). Then from Claim 2 it follows that \( y^{G_{u,x}} = \{ y, z \} \) for some \( z \in V_1 \). So
\[
Y \subset S_{\text{out}}(y) \cup S_{\text{out}}(z)
\]
where \( S = R_{X,Y} \) with \( X = y^{G_{u,x}} \). Moreover, by Claim 1 we also have that both of sets in the right-hand side are of cardinality equal 2. Thus taking into account that \( S_{\text{in}}(v) \cap \{ y, z \} = \{ y \} \) we see that either \( |Y| = 4 \) and \( |(G_{u,x,y,z})_Y| = 2 \). In any case \( |(G_{u,x,y})_Y| \in \{ 4 \} \) and we are done.

**Claim 4.** The action of \( G_u \) on \( V_2 \) is faithful. Indeed, let \( g \in G_u \) be such that \( v^g = v \) for all \( v \in V_2 \). Take \( v \in V_2 \) with \( I_v = \{ i, j \} \) and \( v_i = v_j = u' \) where \( u' \in U \setminus \{ u_0 \} \). Then it follows that \( (u')^{g_i} = (u')^{g_j} = u' \). This implies that \( g_i = \text{id}_U \) for all \( i \in I \). On the other hand, taking \( v_i \neq v_j \), we see that \( i^{g_0} = i \) and \( j^{g_0} = j \). Thus \( \sigma = \text{id}_I \) and we are done. \( \blacksquare \)

To complete the proof of Lemma 3.1 take \( v \in V_1 \). By Claim 4 the group \( G_{u,v} \) acts faithfully on \( V_2 \). So it is isomorphic to a subgroup of the direct product of the groups \( (G_{u,v})_X \) where \( X \) runs over the set \( \text{Orb}(G_{u,v},V_2) \). Then it is 2-group by Claim 3 and we are done. \( \blacksquare \)

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

**Proof.** Suppose that \( \text{soc}(G) \neq \text{soc}(G^{(2)}) \). Then from Theorem 2.1 it follows that the groups \( G \) 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 \( \text{Alt}(U) \). This implies that
\[
|G^{(2)}| = am|\text{Alt}(U)| \quad (7)
\]
for some natural number \( a \). On the other hand, the group \( G^{(2)} \) is obviously uniprimitive and 3/2-transitive. So the size of any nontrivial orbit of a one point stabilizer of \( G^{(2)} \) equals to the same number, say \( d \). One can see that \( d = me \) for some divisor \( e \) of \( |U| - 1 \). So by Lemma 3.1 applied to \( G^{(2)} \) we have
\[
|G^{(2)}| = |V|me2^k \quad (8)
\]
for some natural number \( k \). Now from (7) and (8) it follows that
\[
|U|^{|U|(|U| - 1)}|U|(|U| - 2)! \quad 2^k \quad \text{divides} \quad |V|2^k.
\]
However, this is impossible for \(|U| \geq 5\). Indeed, \(|V| = p^b = |U|^m\) for some prime \(p\) and some natural number \(b\), but for \(|U| \geq 5\) the number in the left-hand side has at least one prime divisor different from \(p\) and 2.

Since the 2-closure of 3/2-transitive group is 3/2-transitive, from Theorem 3.2 it follows that the group \(G^{(2)}\) is a uniprimitive 3/2-transitive group of the affine type. If in addition, \(G\) preserves a product decomposition, then the same decomposition is preserved by \(G^{(2)}\). Thus the form of this group can be found by means of the classification of 3/2-transitive imprimitive linear groups given in [6].

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

**Lemma 3.3** If \(\text{rk}(\mathcal{C}) > 2\), then \(T\) is a characteristic subgroup of the group \(\text{Aut}(\mathcal{C})\). More exactly,

1. if \(\mathcal{C}\) is imprimitive, then \(\text{Aut}(\mathcal{C})\) is a Frobenius group with the Frobenius kernel \(T\),
2. if \(\mathcal{C}\) is primitive, then \(T = \text{soc}(\text{Aut}(\mathcal{C}))\).

**Proof.** Set \(\Gamma = TG\) where \(G\) is the base group of \(\mathcal{C}\). Since \(\text{Aut}(\mathcal{C}) = \Gamma^{(2)}\), the orbits of the stabilizer of the point \(0_V\) in the group \(\text{Aut}(\mathcal{C})\) coincide with the orbits of the group \(G\). On the other hand, obviously,

\[
|X| = |G|, \quad X \in \text{Orb}(G, V^#)
\]

where \(V^# = V \setminus \{0_V\}\). So \(\text{Aut}(\mathcal{C})\) is a 3/2-transitive permutation group. Suppose first that the scheme \(\mathcal{C}\) is imprimitive. Then the group \(\text{Aut}(\mathcal{C})\) is imprimitive. Since any 3/2-transitive group is either primitive or a Frobenius group [12 Theorem 10.4], we conclude that \(\text{Aut}(\mathcal{C})\) is a Frobenius group. The Frobenius kernel of this group has the cardinality \(|V| = |T|\) and contains all fixed point free elements of the group \(\Gamma\). Thus the Frobenius kernel coincides with \(T\) which proves statement (1).

Suppose that \(\mathcal{C}\) is a primitive scheme. Then the group \(\Gamma\) is primitive. Clearly, the group \(T\) is a normal abelian subgroup of it. This implies that the socle of \(\Gamma\) is abelian and hence \(\text{soc}(\Gamma) = T\) (see [3 Theorem 4.3.B]). Thus \(\Gamma\) is a group of the affine type. Since it is 3/2-transitive, Theorem 3.2 implies that

\[
T = \text{soc}(\Gamma) = \text{soc}(\Gamma^{(2)}) = \text{soc}(\text{Aut}(\mathcal{C}))
\]

which completes the proof.

**Proof of Theorem 1.1.** Let \(f \in \text{Iso}(\mathcal{C}, \mathcal{C}')\). Then obviously \(f\) is a permutation group isomorphism from \(\text{Aut}(\mathcal{C})\) to \(\text{Aut}(\mathcal{C}')\). Since both of these groups are transitive, without loss of generality we assume that \(f\) leaves the point \(0_V\) fixed. Then it suffices to verify that \(f \in \text{Aut}(T) = \text{GL}(V)\). However, the schemes \(\mathcal{C}\) and \(\mathcal{C}'\) are primitive or not simultaneously. Thus the required statement follows from Lemma 3.3.

3.3 To make statements of Theorem 1.1 more precise given a group \(G \leq \text{GL}(V)\) we set

\[
\overline{G} = G^{(1)} \cap \text{GL}(V).
\]

Clearly, \(\overline{G}\) coincides with the largest group \(H \leq \text{GL}(V)\) such that \(\text{Orb}(H) = \text{Orb}(G)\). We call this group the linear closure of \(G\).
Theorem 3.4  In the conditions of Theorem 1.1 denote by $G$ and $G'$ the base groups of the schemes $C$ and $C'$ respectively. Then these schemes are isomorphic iff the groups $G$ and $G'$ are conjugate in $GL(V)$. Moreover, $Aut(C) = TG$ where $T = T_V$.

Proof. From Lemma 3.3 it follows that $T$ is a normal subgroup of the group $Aut(C) = (TG)^{(2)}$. Thus the second statement of the theorem is the consequence of (3) and the following lemma.

Lemma 3.5  Let $A$ be a group and $G \leq Aut(A)$. Denote by $T$ the permutation group on $A$ induced by the right regular representation of $A$. Suppose that $T$ is a normal subgroup of the group $\Gamma = (TG)^{(2)}$. Then $\Gamma = T(Aut(A) \cap G^{(1)})$.

Proof. Set $H$ to be the stabilizer of the point $e = 1_A$ in the group $\Gamma$. Then $Orb(H) = Orb(G)$ and hence $T \leq G^{(1)}$. On the other hand, since $T$ is normalized by $H$ and $e^H = \{e\}$ we have $h^{-1}t_ah = t_{ah}$ for all $a \in A$ and $h \in H$ where $t_a$ is the element of $T$ taking $x$ to $xa$. So

$$(ab)^h = a^{bh} = (a^h)^{h^{-1}bh} = (a^h)^{t_{bh}} = a^{bh}, \quad a, b \in A.$$  

Thus $H \leq Aut(A)$, and hence $\Gamma = TH \leq T(Aut(A) \cap G^{(1)})$. Conversely, let $g \in Aut(A) \cap G^{(1)}$. Then given $c \in A$ there exists $g_c \in G$ such that $c^g = c^{g_c}$. So given $a, b \in A$ due to the normality of $T$ we have

$$(a, b)^g = (a^t, b^t)^{t^{-1}g} = (e, c)^{g_s} = (e, c^{g_c})^s = (e, c^{g_c})^s = (a^{g_c}, b^{g_c})^s = (a, b)^{g_c} s$$

where $t$ is the element of $T$ such that $a^t = e$, $c = b^t$ and $s = g^{-1}t^{-1}g$. Since $tg_c \in TG$, this means that $g$ preserves the 2-orbit of the group $TG$ containing $(a, b)$ for all $a, b \in A$. Thus $g \in \Gamma$ and hence, $Aut(A) \cap G^{(1)} \leq \Gamma$. This implies that $T(Aut(A) \cap G^{(1)}) \leq \Gamma$ and we are done.

To prove the first statement of Theorem 3.4 suppose that $g^{-1}CG \subseteq C'$ for some $g \in GL(V)$. Then by the second statement of the theorem we have

$$g^{-1}Aut(C)g = g^{-1}(TG)g = (g^{-1}Tg)(g^{-1}CGg) = TG' = Aut(C')$$

whence it follows that $g \in Iso(C, C')$. Conversely, let $g \in Iso(C, C')$. Then $g^{-1}Aut(C)g = Aut(C')$. By Theorem 1.4 without loss of generality we can assume that $g \in GL(V)$. Then $g$ leaves the point $v = 0_V$ fixed and by the first part we have

$$g^{-1}Gg = g^{-1}(Aut(C))v = Aut(C')v = G'$$

which complete the proof.

For imprimitive cyclotomic schemes Theorem 3.4 can be simplified as follows.

Corollary 3.6  Let the cyclotomic schemes $C$ and $C'$ be imprimitive. Then they are isomorphic iff their base groups are conjugate in $GL(V)$. Moreover, $G = G'$ and $Aut(C) = TG$.

Proof. From statement (1) of Lemma 3.3 it follows that $Aut(C)$ is an imprimitive Frobenius group. Since $TG \leq Aut(C)$ and $|TG| = |Aut(C)|$, it follows that $Aut(C) = TG$. Since obviously $G \leq G'$, this also shows that $G = G'$. Now the first part of the required statement is a consequence of Theorem 3.4 after taking into account that two isomorphic schemes are primitive or not simultaneously.
4 Proof of Theorems 1.3 and 1.4

The main tool of this section is the following theorem which is deduced from the classification \([4]\) of linear groups with orders having certain large prime divisors. In our case such a divisor coincides with a Zsigmondy prime \(r\) for a pair \((q, n)\). We observe that any cyclic group \(G \leq \text{GL}(n, q)\) of order \(r\) is irreducible. This is a consequence of the fact that the linear span \(L(G)\) of it is a finite field \(F\) with \(q^n\) elements. Below we consider the group \(\Gamma L_1(F)\) as a subgroup of \(\text{GL}(n, q)\).

**Theorem 4.1** Let \(G \leq \Gamma \leq \text{GL}(n, q)\) where \((q, n) \notin \{(2, 4), (2, 6)\}\). Suppose that \(G\) is a cyclic group of order \(r \in \mathbb{Z}_{2n+1}(q, n)\) and the group \(\Gamma\) acts intransitively on the set of all nonzero vectors of the underlying linear space. Then \(\Gamma \leq \Gamma L_1(F)\) where \(F = L(G)\).

**Proof.** We observe that the Zsigmondy prime \(r\) for \((q, n)\) is a primitive prime divisor of \(q^n - 1\) in terms of [4]. Since \(r\) divides \(|\Gamma|\), the hypothesis of the theorem implies that the group \(\Gamma\) satisfies the condition of the Main Theorem of that paper with \(d = e = n\). So by this theorem one of the following statements holds:

1. \(\Gamma\) has a normal subgroup isomorphic to \(\text{SL}_n(q), \text{Sp}_n(q), \text{SU}_n(q)\) or \(\Omega^-_n(q)\),
2. \(r \leq 2n + 1\),
3. \(\Gamma \leq \text{GL}(n/m, q^m) \cdot m\) for some divisor \(m \neq 1\) of \(n\),
4. \((q, n) = (2, 4)\) or \((2, 6)\)

where \(\text{GL}(n/m, q^m) \cdot m\) is the general linear group \(\text{GL}(n/m, q^m)\) embedded to \(\text{GL}(n, q)\) and extended by the group of automorphisms of the field extension \(\text{GF}(q^m) : \text{GF}(q)\). However, the cases (1), (2) and (4) are contradict to the intransitivity of \(\Gamma\), the conditions on \(r\) and on \((q, n)\) respectively. Let us consider case (3).

Suppose first that \(m \neq n\). Set \(q' = q^n\) and \(n' = n/m\). Then obviously \((q', n') \notin \{(2, 4), (2, 6)\}\) and \(r \geq 2n + 1 > 2n' + 1\). This implies that \(\mathbb{Z}_{2n+1}(q, n) \subset \mathbb{Z}_{2n'+1}(q', n')\) and we can apply the same arguments by induction. Thus we can assume that \(m = n\) and \(\Gamma \leq \text{GL}(n/n, q^n) \cdot n = \Gamma L_1(F')\) for some field \(F' \subset \text{Mat}(n, q)\). To complete the proof we observe that the multiplicative group of \(F'\) is contained in the normalizer \(\Gamma L_1(F)\) of the group \(G\) in \(\text{GL}(n, q)\). Since \(F^\times\) is the unique Singer subgroup of \(\text{GL}(n, q)\) contained in \(\Gamma L_1(F)\) (see [2]), it follows that \(F' = F\) and we are done.\(\blacksquare\)

**Proof of Theorem 1.3.** From the hypothesis of the theorem it follows that \(r\) divides the order \(m\) of the base group of the scheme \(C\). So the latter group contains a cyclic subgroup \(G\) of order \(r\). By Theorem [4.1] we see that \(\Gamma = \text{Aut}(C)\) is a subgroup of \(\text{GL}(nd, p)\). Moreover, \(G \leq \Gamma\) and \(\Gamma\) acts intransitively on the set \(V^\#\) (because \(m < p^d - 1\)). Finally, \((p, nd) \in \{(2, 4), (2, 6)\}\) only if \(n = 1\), because \((2, 4), (4, 2), (8, 2)\) and \((2, 6)\) are not Dickson pairs, and for the Dickson pair \((4, 3)\) we have \((p, d, n) = (2, 2, 3)\) and the set \(\mathbb{Z}_{2d+1}(p, d^n)\) is empty (there are no Zsigmondy primes for \((2, 6)\)). Thus \(\Gamma \leq \Gamma L_1(F)\) with \(F = L(G)\) by Theorem [4.1] and hence the group \(\text{Aut}(C)\) is isomorphic to a subgroup of the group \(\text{AGL}_1(F)\). Since \(|F| = p^d\), we are done.\(\blacksquare\)

**Proof of Theorem 1.4.** First we cite some number theoretical results from [8]. Given \(n \in \mathbb{N}\) denote by \(P[n]\) the greatest prime factor of \(n\) and given \(0 < \kappa < 1/\log 2\) let
\( N_\kappa = \{ n \in \mathbb{N} : D(n) \leq \kappa \log \log n \} \) where \( D(n) \) is the number of distinct prime factors of \( n \). Then according to \([8, \text{p.25}]\) given real numbers \( \alpha, \beta \) there exists a constant \( C_\kappa > 0 \) such that for each \( n \geq 3, n \in N_\kappa \), the following inequality holds:

\[
P[\Phi_n(\alpha, \beta)] > C_\kappa \frac{n \log n^{1-\kappa \log 2}}{\log \log \log n}
\]  

(10)

with \( \Phi_n(\alpha, \beta) = \prod_i (\alpha - \zeta^i \beta) \) where \( \zeta \) is a primitive \( n \)th root of 1 and \( i \) runs over the set of all numbers \( 1, \ldots, n \) coprime to \( n \).

Let us fix a prime power \( q = p^d \) and given a number \( N \in \mathbb{N} \) set

\[ \mathcal{N}(q, N) = \{ dn \in \mathbb{N} : dn \geq N \text{ and } (q, n) \text{ is a Dickson pair} \}. \]

Choose \( N_q \) to be the minimal number \( n \in \mathbb{N} \) for which \( D(d) \log q \leq \kappa \log \log n \) where \( \kappa = 1/(2 \log 2) \). Then given \( dn \in \mathcal{N}(q, N_q) \) we have

\[
D(dn) \leq D(d)D(n) \leq D(d) \log q \leq \kappa \log \log n.
\]

So \( dn \in N_\kappa \) and hence \( \mathcal{N}(q, N_q) \subset N_\kappa \). By (10) this implies that for a fixed \( q \) we have

\[
P[\Phi_{dn}(p, 1)] > C_\kappa \frac{n \sqrt{\log n}}{\log \log \log n} > 2dn + 1
\]  

(11)

for all sufficiently large \( n \in \mathcal{N}(q, N_q) \). On the other hand, a prime factor \( r \) of the number \( \Phi_{dn}(p, 1) \) is not a Zsigmondy prime for \( (p, dn) \) iff \( r \leq dn \) (see \([9, \text{Proposition 2}]\)). Thus from (11) it follows that there exists a natural number \( N'_q > N_q \) such that \( Z_{2dn+1}(p, dn) \neq \emptyset \) for all \( n > N'_q \).

To complete the proof let \( C = \text{Cyc}(K, \mathbb{K}^x) \) where \( \mathbb{K} \) is a Dickson near-field corresponding to the Dickson pair \( (q, n) \). Suppose that \( m = |K| < q^n \) and \( n > N'_q \). Then \( Z_{2dn+1}(p, dn) \neq \emptyset \). Let us show that if

\[
|Z_{2dn+1}(p, dn)| > 1, \text{ or } Z_{2dn+1}(p, dn) = \{ r \} \text{ and } r^2 \mid (q^n - 1)
\]  

(12)

where \( r = (q^n - 1)/m \), then the group \( \text{Aut}(C) \) is isomorphic to a subgroup of the group \( \text{GL}_1(q^n) \). To do this set \( K' \) to be a maximal subgroup of \( \mathbb{K}^x \) containing \( K \). The group \( \mathbb{K}^x \) being isomorphic to a subgroup of the group \( \text{GL}_1(q^n) \), is solvable. Due to the maximality of \( K' \) this implies that there exists a normal elementary abelian subgroup \( K_0 \) of \( \mathbb{K}^x \) such that \( [\mathbb{K}^x : K'] = |K_0| \) is a prime power. Moreover, any Sylow subgroup of \( \mathbb{K}^x \) is a cyclic group or a quaternion group \([11]\). Thus \( K_0 \) is a cyclic group of prime order and so the number \( [\mathbb{K}^x : K'] \) is prime. By (12) this implies that \( m' = |K'| \) has a prime divisor \( r' \in Z_{2dn+1}(p, dn) \). So from Theorem \([13]\) applied to the cyclotomic scheme \( C' = \text{Cyc}(K', \mathbb{K}^x) \) it follows that the group \( \text{Aut}(C') \) is isomorphic to a subgroup of the group \( \text{GL}_1(q^n) \). Since \( \text{Aut}(C) \leq \text{Aut}(C') \), we are done.

References

[1] A. E. Brouwer, A. M. Cohen, A. Neumaier, Distance-regular graphs, Springer, Berlin, 1989.
[2] A. Cossidente, M. J. de Resmini, Remarks on Singer Cyclic Groups and Their Normalizers, Designs, Codes and Cryptography, 32 (2004), 97–102.

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

[4] R. Guralnick, T. Penttila, C. E. Praeger, J. Saxl, Linear groups with orders having certain large prime divisors, Proc. London Math. Soc., 78 (1999) 167–214.

[5] O. Manz, T. R. Wolf, Representations of solvable groups, London Mathematical Society Lecture Note Series, 185, Cambridge University Press, Cambridge, 1993.

[6] D. S. Passman, p-solvable doubly transitive permutation groups, Pacific J. Math., 26 (1968), 555-577.

[7] C. E. Praeger, J. Saxl, Closures of finite primitive permutation groups, Bull. London Math. Soc., 24 (1992), 251–258.

[8] P. Ribenboim, My numbers, my friends. Popular lectures on number theory., Springer-Verlag, New York, 2000.

[9] M. Roitman, On Zsigmondy primes, Proc. Amer. Math. Soc., 125 (1997), 1913–1919.

[10] D. A. Suprunenko, Matrix groups, Transl. Math. Monogr., Vol. 45, American Mathematical Society, Providence, Rhode Island, 1976.

[11] H. Währing, Theorie der Fastkörper, Thales-Verlag, Essen 1987.

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