SPLITTING OF ABELIAN VARIETIES, ELLIPTIC MINUSCULE PAIRS

V. KUMAR MURTY AND YING ZONG

Abstract. We partially answer, in terms of monodromy, Murty and Patankar’s question:

Given an absolutely simple abelian variety over a number field, does it have simple specializations at a set of places of positive Dirichlet density?

The answer is based on the classification of pairs \((G, V)\) consisting of a semi-simple algebraic group \(G\) over a non-archimedean local field and an absolutely irreducible representation \(V\) of \(G\) such that \(G\) admits a maximal torus acting irreducibly on \(V\).

1. Introduction

The purpose of this article is to study the following question (cf. [7], 1.1) through an essentially exhaustive monodromy approach.

Let \(A_K\) be an absolutely simple abelian variety over a number field \(K\). Does there exist a finite extension \(L\) of \(K\) such that the base change of \(A_K\) to every finite extension of \(L\) has simple specializations at a set of places of positive Dirichlet density?

Let us recall some notions before we formulate the question in more precise terms and impose a natural hypothesis on \(A_K\).

Let \(t = \text{Spec}(K)\), \(\overline{t}\) a geometric point of \(t\), \(S\) an open sub-scheme of the normalization of \(\text{Spec}(\mathbb{Z})\) in \(t\) such that \(A_t = A_K\) extends to an abelian scheme \(A\) over \(S\).

We call an arbitrary \(S\)-fiber of \(A\) a specialization of \(A_t\). A specialization \(A_s = A \times_s s\), \(s \in S\), is simple, if it is a simple object in the category of \(s\)-abelian varieties up to isogenies, that is, if \(\text{End}_s(A_s) \otimes_{\mathbb{Z}} \mathbb{Q}\) is a \(\mathbb{Q}\)-division algebra. A specialization \(A_s\) is absolutely simple, if \(A_s \times_s \overline{s}\) is simple, for \(\overline{s}\) a geometric point of \(s\). A subset \(\Xi\) of \(S \setminus \{t\}\) has Dirichlet density \(d\), \(0 \leq d \leq 1\), if asymptotically in \(N \in \mathbb{R}\),

\[
\text{Card}\{s \in \Xi, \text{Card}(k(s)) \leq N\} = d \frac{N}{\log N} + o\left(\frac{N}{\log N}\right).
\]
As a fundamental example, the set
\[ \{ s \in S \setminus \{ t \}, k(s) \text{ is a prime field} \} \]
has Dirichlet density 1.

What we asked above is whether there exists some finite extension \( L \) of \( K \) such that for each finite extension \( K' \) of \( L \), if \( S' \) denotes the normalization of \( S \) in \( t' = \text{Spec}(K') \), the set
\[ \{ s' \in S' \setminus \{ t' \}, A \times_S s' \text{ is simple} \}, \]
or what amounts to the same, the subset
\[ \{ s' \in S' \setminus \{ t' \}, A \times_S s' \text{ is simple} \}, k(s') \text{ is a prime field} \]
has positive Dirichlet density.

Observe that if \( \text{End}_t(A_t) \) is not commutative, \( A_s = A \times_S s \) is not simple at any of the points of \( S \) with values in a finite prime field, for otherwise \( \text{End}_s(A_s) \otimes \mathbb{Z} \mathbb{Q} \) would be a field ([9], p. 98, line 1), but the specialization homomorphism
\[ sp : \text{End}_t(A_t) \xleftarrow{\sim} \text{End}_S(A) \xrightarrow{\sim} \text{End}_s(A_s) \]
is injective.

Therefore, in order that the question does not have a trivial negative answer, it is necessary to impose that \( \text{End}_t(A_t) \otimes \mathbb{Z} \mathbb{Q} \) be a field, as already known to Achter in a different way ([1] Theorem B, and [2]. See, however, Remark 2.11 for a problem in his Theorem A [1]).

Now, given a prime number \( \ell \) invertible on \( S \), consider an \( \ell \)-adic approach to the question.

Choose for each closed point \( s \in S \) a geometric point \( \overline{s} \) localized at \( s \), and a chemin \( ch_s \) connecting \( \overline{s} \) to \( \overline{t} \) (SGA 1, Exposé V, 7). Let \( F_s \in \pi_1(s, \overline{s}) \) be the geometric Frobenius, and \( F_s^* \) the image of \( F_s \) under the composition
\[ \pi_1(s, \overline{s}) \xrightarrow{ch_s} \pi_1(S, \overline{t}) \xrightarrow{\rho_{\overline{t}}} \text{GL}(H^1(A_{\overline{t}}, \mathbb{Q}_\ell)), \]
where \( \rho_{\overline{t}} \) is the \( \ell \)-adic monodromy representation associated to the abelian scheme \( A \). Write \( M_\ell = \text{Im}(\rho_{\overline{t}}) \) for the monodromy, \( M_\ell^{\text{Zar}} \) its Zariski closure in \( \text{GL}(H^1(A_{\overline{t}}, \mathbb{Q}_\ell)) \). Enlarging \( K \) to a finite extension if necessary, suppose \( \text{End}_t(A_t) = \text{End}_{\overline{t}}(A_{\overline{t}}) \) and that \( M_\ell^{\text{Zar}} \) is connected.

Tate’s theorem applied to a closed fibre \( A_s \),
\[ \text{End}_s(A_s) \otimes \mathbb{Z} \mathbb{Q}_\ell \xleftarrow{\sim} \text{End}_{F_s^*}(H^1(A_{\overline{t}}, \mathbb{Q}_\ell))^{\text{opposite}}, \]
shows that \( A_s \) is simple if \( F_s^* \) acts irreducibly on \( H^1(A_{\overline{t}}, \mathbb{Q}_\ell) \). The subset \( X_\ell \) of the compact \( \ell \)-adic Lie group \( M_\ell \) consisting of those elements acting irreducibly on \( H^1(A_{\overline{t}}, \mathbb{Q}_\ell) \) is a union of conjugacy classes, and
by Krasner’s lemma, open in $M_\ell$. By Cebotarev’s density theorem, the volume of $X_\ell$ in the normalized Haar measure of $M_\ell$ equals the Dirichlet density of the set 

\[ \{ s \in S \setminus \{ t \}, F^*_s \in X_\ell \}, \]

which is $\leq$ the density of 

\[ \{ s \in S \setminus \{ t \}, A_s \text{ is simple} \}. \]

Thus, the question has a positive answer, provided that $X_\ell$ is non-empty over every finite extension of $K$.

Each element of $X_\ell$ lies in a maximal torus of $M^{\text{Zar}}_\ell$ acting irreducibly on $H^1(A_t, Q_\ell)$. Conversely, each torus of $M^{\text{Zar}}_\ell$ irreducible on $H^1(A_t, Q_\ell)$ contains an open dense subset whose every $Q_\ell$-point acts irreducibly on $H^1(A_t, Q_\ell)$. Since $M_\ell$ is open in $M^{\text{Zar}}_\ell(\mathbb{Q}_\ell)$ (Bogomolov), the condition that $X_\ell$ be non-empty is equivalent to the condition that some maximal torus of $M^{\text{Zar}}_\ell$ act irreducibly on $H^1(A_t, Q_\ell)$.

However, if $\text{End}_t(A_t) \otimes \mathbb{Z} Q_\ell$ is not a field, one has even that $M^{\text{Zar}}_\ell$ acts reducibly on $H^1(A_t, Q_\ell)$, equivalently, $A/\ell A$, $A$ being any $\pi_1(t, \bar{t})$-stable $\mathbb{Z}_\ell$-lattice of $H^1(A_t, Q_\ell)$, is a reducible $\mathbb{F}_\ell[\pi_1(t, \bar{t})]$-module, for by Faltings,

\[ \text{End}_t(A_t) \otimes \mathbb{Z} Q_\ell \hookrightarrow \text{End}_{M^{\text{Zar}}_\ell(\mathbb{Q}_\ell)}(H^1(A_t, Q_\ell))^\text{opposite}. \]

When, for instance, $E := \text{End}_t(A_t) \otimes \mathbb{Z} Q_\ell$ has an abelian subfield of group $(\mathbb{Z}/p\mathbb{Z})^4$, $p$ prime, or a non-solvable sub-Galois extension of $Q$, no completion $E \otimes Q Q_\ell$ is a field. (On the other hand, by Hilbert’s irreducibility theorem, for a fixed prime $\ell$, plenty totally real fields or totally imaginary quadratic extensions of totally real fields have prescribed $\ell$-adic completions.)

We assume that $\text{End}_t(A_t) \otimes \mathbb{Z} Q_\ell = E_\ell$ is a field for some prime number $\ell$; without this restrictive assumption, there is little for us to say.

Then, $H^1(A_t, Q_\ell)$, as an $E_\ell$-linear representation of $M^{\text{Zar}}_\ell$ or its derived group, is absolutely irreducible.

At least for $\eta = \text{Spec}(E_\ell)$, $G = [M^{\text{Zar}}_\ell, M^{\text{Zar}}_\ell]$, $V = H^1(A_t, Q_\ell)$, one is led to the basic question:

Let $G$ be a semi-simple algebraic group over the spectrum $\eta$ of a finite extension of $Q_\ell$, $\rho_V : G \to \text{GL}(V)$ an absolutely irreducible $\eta$-linear representation with finite kernel. Does some maximal torus of $G$ act irreducibly on $V$?

One may further suppose $G$ simply connected. Let $\bar{\eta}$ be a geometric point of $\eta$. A maximal torus $\mathfrak{T}$ is irreducible on $V$ if and only if the
weights of $V_{\eta}$ relative to $\mathfrak{T}_{\eta}$ are permuted transitively by $\pi_1(\eta, \overline{\eta})$. So if such a torus exists, all the weights have the same length, that is, $V_{\eta}$ is minuscule.

Let $D_{\eta}$ be the Dynkin diagram of $G_{\eta}$, $\rho_D : \pi_1(\eta, \overline{\eta}) \to \text{Aut}(D_{\eta})$, the index, and let $\alpha_i$, $i = 1, \cdots, r$, be the $\pi_1(\eta, \overline{\eta})$-orbits in $D_{\eta}$ consisting of minuscule vertices corresponding to a minuscule representation $V = V_1 \otimes_{\eta} \cdots \otimes_{\eta} V_r$ of $G = G_1 \times_{\eta} \cdots \times_{\eta} G_r$, $G_i$ being the simple factors. Put $D = (D_{\eta}, \rho_D)$, $\alpha_V = \sum \alpha_i$.

That whether $G$ has a maximal torus acting irreducibly on $V$ depends only on $(D, \alpha_V)$ (Theorem 2.3, Lemma 3.1) ; if $G$ admits such a torus, we call $(D, \alpha_V)$ an elliptic minuscule pair, cf. (2.2).

The key technical result of this article, Theorem 3.2, is the enumeration of elliptic minuscule pairs with connected Dynkin diagrams, which is the basis for the following partial answer to the question we started with.

**Theorem 1.1.** Let $\ell$ be a prime number. Suppose $\text{End}_t(A_t) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell = \text{End}_t(A_{\overline{\mathbb{F}}_\ell}) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell = \ell$ is a field, $M_{zar}^{\mathbb{Q}_\ell}$ connected and that the monodromy representation $H^1(A_t, \mathbb{Q}_\ell)$ is minuscule whose associated minuscule pair over $\text{Spec}(\mathbb{F}_\ell)$ is elliptic. Then $A_t$ specializes to absolutely simple abelian varieties at a set of places of positive Dirichlet density.

See (2.9) for why $A_t$ has absolutely simple rather than just simple specializations at a set of places of positive density. Briefly, it results from the assertions i) and ii) below:

i) A specialization $A_s$ is absolutely simple if it is simple and if $\text{End}_s(A_s \times_s \overline{\mathbb{F}})$ is commutative.

ii) Whenever $M_{zar}^{\mathbb{Q}_\ell}$ is connected and the monodromy representation $H^1(A_t, \mathbb{Q}_\ell)$ has no multiple weights, the set

$$\{ s \in S \backslash \{ t \}, \text{End}_s(A_s \times_s \overline{\mathbb{F}}) \text{ is commutative} \}$$

has density 1.

Note that, in case $A_t$ verifies the Mumford-Tate conjecture, the monodromy $E_\ell$-linear representation $H^1(A_{\overline{\mathbb{F}}_\ell}, \mathbb{Q}_\ell)$ is minuscule, and in particular, has no multiple weights, cf. (2.10).

We owe much to M.Aschbacher for answering questions of Y.Z. We thank J.Achter for kind correspondences. We thank especially C.Chai and S.Lu for their critical reading of the manuscript and providing comprehensive advice on writings.
2. Elliptic minuscule pairs

2.1. A Dynkin diagram is a finite set $D$, equipped with the structure of a function $l : D \to \{1, 2, 3\}$ ("longueurs") and of a binary relation $L$ ("liaisons") on $D$, such that $L$ is disjoint with the diagonal of $D \times D$.

Every root system has its Dynkin diagram with connected components labeled according to types as $A, B, \cdots, G_2$ ([3], Chapitre VI, Théorème 3, p. 197).

Let $S$ be a scheme. An $S$-Dynkin diagram is a sheaf of sets $D$ on $S$ for the étale topology, locally constant, constructible, equipped with the structure of a morphism $l : D \to \{1, 2, 3\}_S$ and of a sheaf of $S$-relations $L \subset D \times_S D$, $L$ locally constant, constructible on $S$, such that for any geometric point $s$ of $S$, the fibre $D_s$, with the function $l_s$ and the relation $L_s$, is a Dynkin diagram.

For any $S$-scheme $S'$, $D \times_S S'$ is an $S'$-Dynkin diagram, and every descent data on $D$ relative to $S$ for the étale topology is effective.

The monodromy representation

$$\rho_{D,s} : \pi_1(S, s) \to \text{Aut}(D_s, l_s, L_s)$$

of an $S$-Dynkin diagram $D$ at a geometric point $s \to S$ is the index of $D$ at $s$ (cf. [10], 2.3).

Define $\pi_0(D)$ to be the quotient of $D$ by the equivalence relation generated by $L$. Then $D$ is a $\pi_0(D)$-Dynkin diagram.

Every reductive $S$-group scheme has its $S$-Dynkin diagram, functorial with respect to isomorphisms and compatible with base change (SGA 3, Exposé XXIV, 3.3).

Given an $S$-Dynkin diagram $D$, if at any geometric point $s$ of $S$ the components of the fibre $D_s$ are of types $A, B, \cdots, G_2$, then there is a quasi-épinglé, semi-simple, simply connected $S$-group scheme having $D$ as its $S$-Dynkin diagram (SGA 3, Exposé XXIV, Théorème 3.11).

Also, for any semi-simple, simply connected $S$-group scheme $G$, there exists a pair $(Q, u)$, unique up to unique isomorphisms, consisting of a quasi-épinglé, semi-simple, simply connected $S$-group scheme $Q$ and an “isomorphisme extérieur” $u \in \text{Isom}_{\text{ext}}(Q, G)$ (SGA 3, Exposé XXIV, Corollaire 3.12). The existence of $u$ enables the identification of the $S$-Dynkin diagram $D$ of $Q$ with that of $G$, and permits to define the $S$-scheme of “isomorphismes intérieurs”

$$\text{Isom}_{\text{int}}(Q, G),$$

which is a left torsor under the adjoint group of $G$ and a right torsor under the adjoint group of $Q$. 
Let $T \subset B$ be the canonical maximal torus and Borel subgroup of $Q$, $U$ the unipotent radical of $B$. Let $N$ be the normalizer of $T$ in $Q$, $W = N/T$ the Weyl group. Let

$$\pi : X \to S$$

denote the $S$-scheme $Q/B$, which is projective, smooth, with geometrically connected fibres over $S$.

Suppose

$$\omega : T \to \mathbb{G}_{m,S}$$

is a weight of $Q$ with respect to $T$, dominant relative to the notion of positivity defined by $B$. Let

$$\omega_B : B \to B/U = T \xrightarrow{\omega} \mathbb{G}_{m,S}$$

be the composition; this character, twisted by the $B_X$-torsor $Q \to Q/B = X$,

provides a $\mathbb{G}_{m,X}$-torsor $Q \wedge^{B_X} \mathbb{G}_{m,X}$ and an invertible $\mathcal{O}_X$-module

$$L_{\omega} = Q \wedge^{B_X} \mathbb{G}_{m,X} \wedge^{\mathbb{G}_{m,X}} \mathcal{O}_X.$$ 

Recall that $E_\omega = \pi_*L_{\omega}$ is a representation of $Q$ on a locally free $\mathcal{O}_S$-module of finite rank, of formation compatible with any base change $S' \to S$, and if $S$ is the spectrum of an algebraically closed field of characteristic zero, $E_\omega$ is irreducible of highest weight $\omega$.

In particular, to each section $\alpha \in D(S)$ of the $S$-Dynkin diagram $D$, there corresponds a fundamental representation $E_\alpha$ of $Q$ of fundamental weight $\omega_\alpha$.

A section $\alpha \in D(S)$ is minuscule if the Weyl orbit

$$W\omega_\alpha \subset \text{Hom}_S(T, \mathbb{G}_{m,S})$$

is the sheaf of weights of $E_\alpha$ relative to $T$.

More generally, $\alpha = \sum^{r}_{i=1} \alpha_i$, $\alpha_i \in D(S)$, is minuscule, if each $\alpha_i$ is minuscule and for any geometric point $s$ of $S$, $\alpha_i, s$ lie in distinct components of $D_s$. Let $W\omega_\alpha := W\omega_{\alpha_1} \times_S \cdots \times_S W\omega_{\alpha_r}$.

**Definition 2.2.** Suppose $S$ connected and $\alpha = \sum^{r}_{i=1} \alpha_i$ minuscule. The pair $(D, \alpha)$ is said to be an elliptic minuscule pair, or simply elliptic, if there is a $W$-torsor $x$ on $S$ such that

$$x \wedge^W W\omega_\alpha.$$
is a connected object in the Galois category of locally constant, constructible sheaves on $S$, that is, at any geometric point $s$ of $S$, the image of the monodromy representation

$$\rho_{x,s} : \pi_1(S, s) \to \text{Aut}((x \wedge^W W \omega_s)_s)$$

acts transitively on the fibre $(x \wedge^W W \omega_s)_s$. Any such $W$-torsor $x$ is said to be elliptic for $(D, \alpha)$.

**Theorem 2.3.** Let $\eta$ be the spectrum of a complete discretely valued field of characteristic zero with finite residue field, $G$ a semi-simple algebraic group over $\eta$ with Dynkin diagram $D$, $\rho_V : G \to \text{GL}(V)$ an absolutely irreducible representation with finite kernel. Then some maximal torus of $G$ acts irreducibly on $V$ if and only if $V$ is minuscule and $(D, \alpha)$ is elliptic, $\alpha$ being the minuscule section corresponding to $V$.

For the proof, we may and do assume $G$ simply connected.

If a maximal torus $\Xi$ of $G$ acts irreducibly on $V$, the weights of $V_{\eta}$ relative to $\Xi_{\eta}$ are permuted transitively by $\pi_1(\eta, \eta)$; a priori, all the weights have the same length, i.e. $V$ is minuscule ($\mathbf{3}$, Chapitre VIII, §7, Proposition 6, p. 127).

In the following, suppose $V$ minuscule, and let $\alpha = \sum \alpha_i, \alpha_i \in D(\eta)$, be the corresponding section.

**Lemma 2.4.** For any anisotropic maximal torus $\Xi$ of $G$, with image $\Xi^{\text{ad}}$ in the adjoint group $G^{\text{ad}}$, the map

$$H^1(\eta, \Xi^{\text{ad}}) \to H^1(\eta, G^{\text{ad}})$$

is surjective, and $H^2(\eta, \Xi) = 0$.

**Proof.** Write $Z$ for the center of $G$. The extension

$$1 \to Z \to G \to G^{\text{ad}} \to 1$$

induces the cohomology sequence

$$H^1(\eta, G) \to H^1(\eta, G^{\text{ad}}) \xrightarrow{\partial} H^2(\eta, Z).$$

As $G$ is simply connected, $H^1(\eta, G) = 0$ (Kneser). Hence

$$\partial : H^1(\eta, G^{\text{ad}}) \to H^2(\eta, Z)$$

is injective.

To show that

$$H^1(\eta, \Xi^{\text{ad}}) \to H^1(\eta, G^{\text{ad}})$$

is surjective, it suffices to show that the composition

$$\delta : H^1(\eta, \Xi^{\text{ad}}) \to H^1(\eta, G^{\text{ad}}) \xrightarrow{\partial} H^2(\eta, Z)$$

is surjective.
is surjective.

Note that
\[ \delta : H^1(\eta, \mathfrak{F}^{\text{ad}}) \rightarrow H^2(\eta, Z) \]
is a coboundary of the extension
\[ 1 \rightarrow Z \rightarrow \mathfrak{F} \rightarrow \mathfrak{F}^{\text{ad}} \rightarrow 1, \]
whose cohomology sequence
\[ H^1(\eta, \mathfrak{F}^{\text{ad}}) \xrightarrow{\delta} H^2(\eta, Z) \rightarrow H^2(\eta, \mathfrak{F}) \]
implies that
\[ \delta : H^1(\eta, \mathfrak{F}^{\text{ad}}) \rightarrow H^2(\eta, Z) \]
is surjective if
\[ H^2(\eta, \mathfrak{F}) = 0. \]

Show \( H^2(\eta, \mathfrak{F}) = 0 \):

Since the Yoneda pairing
\[ \text{Hom}_\eta(\mathfrak{F}, G_m) \times H^2(\eta, \mathfrak{F}) \rightarrow H^2(\eta, G_m) = \text{Br}(\eta) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z} \]
is non-degenerate (Nakayama-Tate), one needs verify that
\[ \text{Hom}_\eta(\mathfrak{F}, G_m) = 0, \]
which is precisely the condition that \( \mathfrak{F} \) be anisotropic. \( \square \)

Let the quasi-épinglé, semi-simple, simply connected \( \eta \)-group scheme \( Q \), the “isomorphisme extérieur” \( u \in \text{Isom}_{\text{ext}}(Q, G) \), and the bitorsor \( \text{Isom}_{\text{int}}(Q, G) \) be as in (2.1).

Let \( T \subset B \) be the canonical maximal torus and Borel subgroup of \( Q \), \( N \) the normalizer of \( T \) in \( Q \), \( W = N/T \), \( C \) the center of \( Q \), \( T^{\text{ad}} \) (resp. \( N^{\text{ad}} \)) the image of \( T \) (resp. \( N \)) in the adjoint group \( Q^{\text{ad}} \).

Let \( E_\alpha = \otimes E_\alpha \), be the minuscule representation of \( Q \) of fundamental weight \( \omega_\alpha \).

**Lemma 2.5.** 1) The \( Q^{\text{ad}}(\eta) \)-conjugacy classes of maximal tori of \( Q \) are in bijective correspondence with the elements of \( H^1(\eta, N) \).

2) The map \( H^1(\eta, N) \rightarrow H^1(\eta, W) \) is injective, whose image contains the isomorphism classes of \( W \)-torsors \( x \) on \( \eta \) such that \( x \wedge^W T \) are anisotropic.

**Proof.** 1) The set \( (Q/N)(\eta) \) classifies the maximal tori of \( Q \) because locally on \( \eta \) for the étale topology they are all conjugate to \( T \) by sections of \( Q \).

The exact sequence of pointed sets
\[ Q^{\text{ad}}(\eta) \rightarrow (Q/N)(\eta) \rightarrow H^1(\eta, N^{\text{ad}}) \rightarrow H^1(\eta, Q^{\text{ad}}) \]
shows that the $Q^\text{ad}(\eta)$-orbits in $(Q/N)(\eta)$ are in one-to-one correspondence with the elements in the kernel of

$$H^1(\eta, N^\text{ad}) \to H^1(\eta, Q^\text{ad}).$$

Observe that in the cohomology sequence

$$H^1(\eta, Q) \to H^1(\eta, Q^\text{ad}) \xrightarrow{\partial} H^2(\eta, C)$$

of the extension

$$1 \to C \to Q \to Q^\text{ad} \to 1,$$

the map

$$\partial : H^1(\eta, Q^\text{ad}) \to H^2(\eta, C)$$

is injective, since

$$H^1(\eta, Q) = 0,$$

$Q$ being simply connected.

Hence, the kernel of

$$H^1(\eta, N^\text{ad}) \to H^1(\eta, Q^\text{ad})$$

equals the kernel of the composition

$$\delta : H^1(\eta, N^\text{ad}) \to H^1(\eta, Q^\text{ad}) \xrightarrow{\partial} H^2(\eta, C).$$

This

$$\delta : H^1(\eta, N^\text{ad}) \to H^2(\eta, C)$$

is a coboundary of the central extension

$$1 \to C \to N \to N^\text{ad} \to 1.$$

From the exact sequence

$$H^1(\eta, C) \to H^1(\eta, N) \to H^1(\eta, N^\text{ad}) \xrightarrow{\delta} H^2(\eta, C),$$

it follows that $\text{Ker}(\delta)$ equals the image of

$$H^1(\eta, N) \to H^1(\eta, N^\text{ad}).$$

To conclude that $H^1(\eta, N)$ is isomorphic to this image, it needs to show that the map

$$H^1(\eta, C) \to H^1(\eta, N)$$

is 0.

By the factorization

$$H^1(\eta, C) \to H^1(\eta, T) \to H^1(\eta, N),$$

it suffices to show that

$$H^1(\eta, T) = 0.$$
This follows from the identity
\[ H^1(\eta, T) = H^1(D, G_m) \]
(SGA 3, Exposé XXIV, Corollaire 3.14) and Satz 90,
\[ H^1(D, G_m) = 0, \]
the Dynkin diagram \( D \) being representable by a scheme, finite, étale over \( \eta \).

2) That
\[ H^1(\eta, N) \to H^1(\eta, W) \]
is injective results from the cohomology sequence
\[ H^1(\eta, T) \to H^1(\eta, N) \to H^1(\eta, W) \]
and that \( H^1(\eta, T) = 0 \).

The class of a \( W \)-torsor \( x \) on \( \eta \) lies in the image of
\[ H^1(\eta, N) \to H^1(\eta, W) \]
if and only if an obstruction
\[ o(x) \in H^2(\eta, x \wedge^W T) \]
vanishes.

When \( x \wedge^W T \) is anisotropic, \( H^2(\eta, x \wedge^W T) = 0 \) (2.4).

\textbf{Lemma 2.6.} \textit{If a sub-torus of} \( G \) \textit{acts irreducibly on} \( V \), \textit{it is anisotropic.}

\textit{Proof.} A torus is anisotropic if and only if it has no diagonalizable sub-torus other than 1.

Recall that the kernel of the representation
\[ \rho_V : G \to \text{GL}(V) \]
is finite. And as \( G \) is semi-simple, \( \det(\rho_V) = 1 \).

Suppose that a certain sub-torus of \( G \) acts irreducibly on \( V \).

If a \( G_m \) were in this torus, it would act on \( V \) by a character \( z \mapsto z^n \), for some integer \( n \), thus on \( \det(V) \) by the character \( z \mapsto z^{nd}, d = \text{dim}(V) \). So \( nd = 0 \), i.e. \( n = 0 \), and \( G_m \) was contained in \( \text{Ker}(\rho_V) \).

\textbf{Lemma 2.7.} \textit{The group} \( G \) \textit{has a maximal torus acting irreducibly on} \( V \) \textit{if and only if the group} \( Q \) \textit{has a maximal torus acting irreducibly on} \( E_\alpha \).
Proof. Suppose a maximal torus $T$ of $G$ acts irreducibly on $V$. By (2.6), $T$ is anisotropic, and

$$H^1(\eta, T^{\text{ad}}) \to H^1(\eta, G^{\text{ad}})$$

is surjective (2.4). The $G^{\text{ad}}$-torsor

$$\text{Isom}_{\eta}(Q, G)$$

is in particular the image of a $T^{\text{ad}}$-torsor, which means (SGA 3, Éxposé XXIV, Proposition 2.11) that $T$ imbeds into $Q$ as a maximal torus and the scheme

$$I = \text{Isom}_{\eta}(Q, G; \text{Id on } T)$$

of “isomorphismes intérieurs” from $Q$ to $G$ that induce the identity automorphism on $T$ is not empty.

Let $\eta$ be a geometric point of $\eta$. The choice of a section $\iota \in I(\eta)$ identifies the sheaves of weights of $V$ and $E_\alpha$ relative to $T$. So $E_\alpha$ is isomorphic to $V$ as a $T$-module, therefore is irreducible.

The other direction is proven similarly. \hfill \Box

2.8. Proof of Theorem 2.3.

By (2.7), it suffices to show that $(D, \alpha)$ is elliptic if and only if a maximal torus of $Q$ acts irreducibly on $E_\alpha$.

Suppose first $Q$ admits a maximal torus acting irreducibly on $E_\alpha$.

This torus has the form $z \wedge^N T$ for an $N$-torsor $z$ (2.5). Relative to it the sheaf of weights of $E_\alpha$ is

$$z \wedge^N W \omega_\alpha \subset z \wedge^N \text{Hom}_\eta(T, G_m).$$

The condition that $z \wedge^N T$ be irreducible on $E_\alpha$ is equivalent to that $z \wedge^N W \omega_\alpha$ be a connected object in the Galois category of locally constant constructible sheaves on $\eta$. So $z \wedge^N W$ is an elliptic $W$-torsor for $(D, \alpha)$.

Next, suppose $(D, \alpha)$ elliptic, with $x$ being an elliptic $W$-torsor.

Let $\rho : Q \to \text{GL}(E_\alpha)$ be the representation, $\rho_T$ its restriction to $T$. One has that $\text{Ker}(\rho_T)$ is finite and $\det(\rho_T) = 1$.

The torsor $x$ twists $\rho_T$ to a representation

$$\rho_{x,T} : x \wedge^W T \to \text{GL}(E_x)$$

with $x \wedge^W W \omega_\alpha$ as its sheaf of weights.

Hence, $\rho_{x,T}$ is irreducible, and being a twist of $\rho_T$, it has finite kernel and determinant 1. As in (2.6), $x \wedge^W T$ is anisotropic, thus can be imbedded into $Q$ (2.5) ; it is the sought-for maximal torus of $Q$ acting irreducibly on $E_\alpha$. 

2.9. **Proof of Theorem 1.1.**

Let \( g = \dim(A_t) \). Let \( s \) be a closed point of \( S \). The Frobenius \( F_s^* \), being semi-simple on \( H^1(A_t, Q_\ell) \), lies in a maximal torus \( \Xi(s) \) of \( M_{\ell}^{\text{Zar}} \), with eigenvalues \( \chi_i(F_s^*) \), where \( \chi_i, 1 \leq i \leq 2g \), are the weights of \( H^1(A_t, Q_\ell) \) relative to \( \Xi(s) \).

If \( \chi_i(F_s^*)^N = \chi_j(F_s^*)^N \), for some \( i \neq j \), \( N \geq 1 \),

\[
\chi_i(F_s^*)/\chi_j(F_s^*) \in K_s := \mathbb{Q}(\chi_1(F_s^*), \cdots, \chi_{2g}(F_s^*))
\]

is a root of unity. As the characteristic polynomial of \( F_s^* \) has coefficients in \( \mathbb{Z} \) (Weil), \( [K_s : \mathbb{Q}] \leq (2g)! \). The roots of unity in \( K_s \) have order \( d(g) \) bounded by a constant depending only on \( g \).

The set

\[
\{ u \in M_\ell, u^d(g) \text{ has } 2g \text{ distinct eigenvalues on } H^1(A_t, Q_\ell) \}
\]

is Zariski open in \( M_\ell \), stable under conjugation, of measure equal to the density of

\[
\Sigma = \{ s \in S \setminus \{ t \}, (F_s^*)^N \text{ has } 2g \text{ distinct eigenvalues, } \forall \ N \geq 1 \}.
\]

The measure is 1, since the characters \( \chi_i \) are all distinct.

Consider \( s' \to s \), irreducible, finite, étale, of degree \( N \geq 1 \), \( s \in \Sigma \). As \( (F_s^*)^N \) has \( 2g \) distinct eigenvalues, \( \text{End}_{s'}(A_{s'}) \) is commutative, for

\[
\text{End}_{s'}(A_{s'}) \otimes \mathbb{Z} Q_\ell \to \text{End}_{(F_s^*)^N}(H^1(A_t, Q_\ell))^{\text{opposite}}.
\]

Now, \( A_s \) is isogenous to a product of simple abelian varieties \( A_i \), \( i \in I \). If one factor appears with multiplicity \( > 1 \), or if \( A_i \times_s A_{s'} \) is not simple, or if \( A_i \times_s s' \) and \( A_j \times_s s' \) are isogenous for \( i \neq j \), \( \text{End}_{s'}(A_{s'}) \) is not commutative. So, these factors \( A_i \) are absolutely simple, mutually non-isogenous.

The assumptions of Theorem 1.1 imply, as in the introduction, that the specializations of \( A_t \) are simple at a set of places, say \( \Pi \), of positive density. For any \( s \in \Pi \cap \Sigma \), \( A_s \) is absolutely simple, and \( \Pi \cap \Sigma \) has positive density.

2.10. **Complements.**

Let \( A_t \) be as in the introduction, \( g = \dim(A_t) \), \( \ell \) a prime number.

Suppose \( E = \text{End}_t(A_t) \otimes \mathbb{Z} Q_\ell \) is a field, \( M_{\ell}^{\text{Zar}} \) is connected. Write \( E_\ell = E \otimes_Q Q_\ell \).

1) Suppose \( A_t \) specializes to simple abelian varieties at a set of places of positive density.

Then

\[
\Xi := \{ s \in S \setminus \{ t \}, \text{Card}(k(s)) \text{ is prime, } A_s \text{ is simple} \}.
\]
has positive density, and \( \forall s \in \Xi, \text{End}_s(A_s) \otimes \mathbb{Z} \mathbb{Q} = \mathbb{Q}(F_s^*) \) is a field of degree \( 2g \) over \( \mathbb{Q} \) ([9], p. 98, line 1), in particular, \( F_s^* \) has \( 2g \) distinct eigenvalues on \( H^1(A_{\mathfrak{r}}, \mathbb{Q}_\ell) \). A priori, \( H^1(A_{\mathfrak{r}}, \mathbb{Q}_\ell) \) has no multiple weights relative to any maximal torus of \( M_{\mathfrak{Zar}}^{\text{zar}} \), therefore (Howe [5], Theorem 4.6.3), the tensor components of the \( E_\ell \)-linear representation \( H^1(A_{\mathfrak{r}}, \mathbb{Q}_\ell) \) are minuscule or of the types \((A_n, r\omega_i), i = 1, n, n \geq 1, r > 1, (B_n, \omega_1), n > 1, (C_3, \omega_3), (G_2, \omega_1)\).

2) If \( A_{\mathfrak{r}} \) verifies the Mumford-Tate conjecture, any tensor component of the monodromy \( E_\ell \)-linear representation \( H^1(A_{\mathfrak{r}}, \mathbb{Q}_\ell) \) is minuscule, cf. [4], Table 1.3.9.

2.11. Remark.

Let \( A_{\mathfrak{r}} \) be as in the introduction. Let \( E := \text{End}_\ell(A_{\mathfrak{r}}) \otimes \mathbb{Z} \mathbb{Q} \). In [1], Theorem A, Achter claimed that \( A_{\mathfrak{r}} \) specializes to absolutely simple abelian varieties at a set of places of density 1, if either \( E \) is a totally real field, \( \dim(A_{\mathfrak{r}})/[E : \mathbb{Q}] \) is odd, or \( E \) is a totally imaginary quadratic extension of a totally real field, and the action of \( E \) on \( A_{\mathfrak{r}} \) is not “special”. The argument, outlined in loc.cit, p. 2–3, pre-postulated the existence of infinitely many prime numbers inert in \( E \), like:

Let \( \ell \) be any prime at which \( E \) is inert, p. 2, last paragraph.

Since ... we may take an arbitrarily large set of primes inert in \( E \), ... and the density of ... is therefore one, p. 3, second paragraph.

But, as we emphasized in the introduction, even the existence of a single prime \( \ell \) such that \( E \otimes \mathbb{Q} \mathbb{Q}_\ell \) is a field is a rather restrictive assumption on \( E \).

3. Simple elliptic pairs

Let \( S \) be a connected scheme, \((D, \alpha)\) be as in (2.2).

Suppose \( \pi_0(D) = 1 \). Thus, in the notations of Bourbaki–Tits (cf. [3], Chapitre VI, Planches I–IX, p. 250–275, and [10], p. 54–61), if \( D \) is non-constant, \((D, \alpha)\) can only be \((^2A_n, \alpha_{\pm 1}), n \text{ odd } \geq 3, (^2D_n, \alpha_1), n \geq 5, \) or \((^2D_4, \alpha_i), i = 1, 3, 4\).

Let \( s \) be a geometric point of \( S \). We write down the condition that \((D, \alpha)\) be elliptic.

**Lemma 3.1.** 1) \((A_n, \alpha_r), r \in [1, n],\) is elliptic if and only if there is a representation

\[
\rho : \pi_1(S, s) \to \mathfrak{S}_{n+1}
\]

whose image permutes transitively the subsets of \( \{1, \cdots, n+1\} \) of cardinality \( r \).
2) \((B_n, \alpha_n)\) is elliptic if and only if there is a representation
\[ \rho: \pi_1(S, s) \to \text{GL}_n(Z) \]
whose image lies in the group generated by the diagonal matrices and monomial matrices, and acts transitively on
\[ \{ \pm e_1 \pm \cdots \pm e_n \}, \]
where \(e_1, \ldots, e_n\) denote the standard basis of \(Z^n\).

3) \((C_n, \alpha_1)\) is elliptic if and only if there is a representation
\[ \rho: \pi_1(S, s) \to \text{GL}_n(Z) \]
whose image lies in the group generated by the diagonal matrices and monomial matrices, and acts transitively on
\[ \{ e_1, \ldots, e_n, -e_1, \ldots, -e_n \}, \]
where \(e_1, \ldots, e_n\) denote the standard basis of \(Z^n\).

4) \((D_n, \alpha_1)\) is elliptic if and only if there is a representation
\[ \rho: \pi_1(S, s) \to \text{GL}_n(Z) \]
whose image lies in the group generated by the diagonal matrices of determinant 1 and monomial matrices, and acts transitively on
\[ \{ e_1, \ldots, e_n, -e_1, \ldots, -e_n \}, \]
where \(e_1, \ldots, e_n\) denote the standard basis of \(Z^n\).

5) \((D_n, \alpha_{n-1})\) (resp. \((D_n, \alpha_n)\)) is elliptic if and only if there is a representation
\[ \rho: \pi_1(S, s) \to \text{GL}_n(Z) \]
whose image lies in the group generated by the diagonal matrices of determinant 1 and monomial matrices, and permutes transitively the vectors
\[ s_1 e_1 + \cdots + s_n e_n, \]
where \(s_i \in \{1, -1\}\), \(s_1 \cdots s_n = -1\) (resp. \(s_1 \cdots s_n = 1\)), and \(e_1, \ldots, e_n\) denote the standard base of \(Z^n\).

6) \((E_6, \alpha_i), i = 1, 6,\) is elliptic if and only if there is a representation
\[ \rho: \pi_1(S, s) \to \text{O}(F_2^6, q) \]
whose image permutes transitively the non-zero singular vectors in \(F_2^6\), where \(q\) is the quadratic form such that
\[ q(e_i) = q(f_j) = 1, q(e_i + e_j) = q(f_i + f_j) = 0, q(e_i + f_j) = \delta_{ij}, \]
\(e_i, f_j, 1 \leq i, j \leq 3,\) are a basis of \(F_2^6\), \(\delta_{ij} = 1\), if \(i = j\), and 0, if \(i \neq j\).
7) \((E_7, \alpha_7)\) is elliptic if and only if there is a representation
\[
\rho : \pi_1(S, s) \to \{1, -1\} \times \text{Sp}_6(F_2)
\]
whose image acts transitively on \(\{1, -1\} \times (\text{Sp}_6(F_2)/\text{O}(q))\), \(q\) being the quadratic form on \(F_2^6\) with
\[
q(e_i) = q(f_j) = 1, \quad q(e_i + e_j) = q(f_i + f_j) = 0, \quad q(e_i + f_j) = \delta_{ij},
\]
where \(e_i, f_j\) are the standard symplectic base of \(F_2^6\), \(\delta_{ij} = 1\), if \(i = j\), and 0, if \(i \neq j\).

8) \((2A_n, \alpha_{n+1})\), \(n\) odd \(\geq 3\), is elliptic if and only if there is a representation
\[
\rho = (\rho_1, \rho_2) : \pi_1(S, s) \to \{1, -1\} \times S_{n+1}
\]
whose image permutes transitively the subsets of \(\{1, \ldots, n+1\}\) of cardinality \((n+1)/2\), and whose component \(\rho_1\) is the index of \(2A_n\). Here
\[-1 : Y \mapsto \{1, \ldots, n+1\} \setminus Y, \text{ for any } Y \subset \{1, \ldots, n+1\} \text{ of cardinality } (n+1)/2.\]

9) \((2D_n, \alpha_1)\), \(n \geq 5\), or \((2D_4, \alpha_i)\), \(i = 1, 3, 4\), is elliptic if and only if there is a representation
\[
\rho : \pi_1(S, s) \to \text{GL}_n(\mathbb{Z})
\]
whose image acts transitively on \(\{\pm e_1, \ldots, \pm e_n\}\) and lies in the group \(\mathcal{W}\) generated by the diagonal matrices and monomial matrices, and such that the composition
\[
\pi_1(S, s) \xrightarrow{\rho} \mathcal{W} \to \mathcal{W}/\mathcal{W}_1 = \{1, -1\}
\]
is the index of \(2D_n\), where \(\mathcal{W}_1\) is the subgroup of \(\mathcal{W}\) generated by the diagonal matrices of determinant 1 and monomial matrices, and where \(e_1, \ldots, e_n\) denote the standard base of \(\mathbb{Z}^n\).

**Proof.** Let \(R\) be the root system of \(Q\) with respect to \(T\).

The extension
\[
1 \to W \to \text{Aut}_{\mathcal{S}}(R) \to \text{Aut}_{\mathcal{S}}(D) \to 1,
\]
with its cohomology sequence
\[
H^1(S, W) \to H^1(S, \text{Aut}_{\mathcal{S}}(R)) \to H^1(S, \text{Aut}_{\mathcal{S}}(D))
\]
shows that an \(S\)-form \(R'\) of \(R\) is equal to some \(x \wedge^W R\) for a \(W\)-torsor \(x\) if and only if \(R'\) has Dynkin diagram isomorphic to \(D\), or equivalently, if and only if the composition
\[
\pi_1(S, s) \xrightarrow{\rho_{R', s}} \text{Aut}(R_s) \to \text{Aut}(D_s)
\]
is the index of \(D\) at \(s\), where the monodromy representation associated to \(R'\) at \(s\) is written as \(\rho_{R', s}\).
Given any $R' = x \wedge^W R$, the monodromy $\text{Im}(\rho_{R',s})$ normalizes the weights $W_\omega_n$, and the condition “$x$ is an elliptic $W$-torsor for $(D, \alpha)$” can be translated as “$\text{Im}(\rho_{R',s})$ is transitive on $W_\omega_n$”.

If $D$ is constant, $W$ is constant. The class of a $W$-torsor $x$ on $S$ is a $W$-conjugacy class of representations $\rho : \pi_1(S, s) \to W$.

Type by type,

1)–6), 8)–9) the description of $\text{Aut}(R_n)$, the Weyl groups, the minuscule vertices $\alpha$, and the weights $W_\omega_n$, for $(A_n, \alpha_r), (B_n, \alpha_n), (C_n, \alpha_1), (D_n, \alpha_i), i = 1, n - 1, n, (E_6, \alpha_i), i = 1, 6, (2A_n, \alpha_{n+1}), (2D_n, \alpha_1), (2D_4, \alpha_1), i = 1, 3, 4$, follows Bourbaki [3], Chapitre VI, Planches, and Chapitre VI, n°4, Exercice 2.

7) given a root system of base $\{\alpha_1, \cdots, \alpha_7\}$, of root lattice $Q(E_7)$, weight lattice $P(E_7)$, then $2P(E_7) \subset Q(E_7)$, and $E = Q(E_7)/2P(E_7)$ is a 6-dimensional $\mathbf{F}_2$-vector space on which the Killing form $(,) \text{ induces a symplectic form.}$ The Weyl group $W(E_7)$ maps onto $\text{Sp}(E)$ with kernel $\{1, -1\}$, where $-1$ has maximal length relative to $\{\alpha_1, \cdots, \alpha_7\}$ (3, Chapitre VI, n°4, Exercice 3). The central extension

$$1 \to \{1, -1\} \to W(E_7) \to \text{Sp}(E) \to 1$$

splits. Let $E_6$ be the sub-system of base $\{\alpha_1, \cdots, \alpha_6\}$; its roots

$$e_1 = \alpha_1 + \alpha_2 + 2\alpha_3 + 2\alpha_4 + \alpha_5 + \alpha_6,$$

$$e_2 = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5,$$

$$e_3 = \alpha_2 + \alpha_4,$$

$$f_1 = \alpha_1 + \alpha_3 + \alpha_4,$$

$$f_2 = \alpha_4 + \alpha_5 + \alpha_6,$$

$$f_3 = \alpha_3 + \alpha_4 + \alpha_5$$

satisfy the orthogonality relations

$$(e_i, e_j) = 2\delta_{ij}, \ (f_i, f_j) = 2\delta_{ij}, \ (e_i, f_j) = \delta_{ij},$$

and their images in $E$ are a symplectic base. Consequently,

$$F = Q(E_6)/2Q(E_6) \to Q(E_7)/2P(E_7) = E$$

is a bijection, where $Q(E_6)$ is the root lattice of $E_6$. When $F$ is equipped with the quadratic form $q = \frac{1}{2}(,)$, $W(E_6)$ is identified with $O(q)$, and $W(E_7)\omega_7 = W(E_7)/W(E_6) = \{1, -1\} \times (\text{Sp}(E)/O(q))$. \qed
Theorem 3.2. Let $S$ be the spectrum of a complete discrete valuation ring, with generic point $\eta$ of characteristic zero, with closed point $s$, $k(s)$ finite of characteristic $\ell$. Then the elliptic minuscule pairs $(D, \alpha)$ over $\eta$ with $\pi_0(D) = 1$ are

A) $(A_n, \alpha_1), (A_n, \alpha_n),$

$(A_{d-1}, \alpha_2), (A_{d-1}, \alpha_{d-2}), d \geq 1,$

$(A_{p-1}, \alpha_2), (A_{p-1}, \alpha_{p-2}), p$ prime, either $p \equiv 1 \mod 4$, Card$(k(s))$ mod $p$ generates $F_p^\times$, or $p \equiv 3 \mod 4$, Card$(k(s))$ mod $p$ generates a subgroup of $F_p^\times$ of index $\leq 2$,

$(A_7, \alpha_3), (A_7, \alpha_5), \ell = 2,$

$(A_{31}, \alpha_3), (A_{31}, \alpha_{29}), \ell = 2, 5 \nmid [s : F_2];$

$2A) (2, A_3, \alpha_2),$

$(2, A_5, \alpha_3)$, either $(\ell, 5) = 1, 2A_5$ ramified over $S$, Card$(k(s))$ mod $5$ generates $F_5^\times$, or $\ell = 5;$

B) $(B_3, \alpha_3), (B_4, \alpha_4),$

$(B_n, \alpha_n), n \geq 5, \ell = 2;$

C) $(C_n, \alpha_1), n \geq 2;$

D) $(D_n, \alpha_1)$, either $n$ odd $\geq 5, \ell = 2, \text{ or } n$ even $\geq 4,$

$(D_5, \alpha_4), (D_5, \alpha_5),$

$(D_6, \alpha_5), (D_6, \alpha_6), \text{ either Card}(k(s)) \equiv 5 \mod 8, \text{ or } \ell = 2,$

$(D_n, \alpha_{n-1}), (D_n, \alpha_n), n \geq 7, \ell = 2;$

$2D) (2, D_n, \alpha_1);$

$E_6) (E_6, \alpha_1), (E_6, \alpha_6), \text{ either Card}(k(s)) \equiv \pm 4 \mod 9, \text{ or } \ell = 3;$

$E_7) (E_7, \alpha_7), \ell = 2.$

This list is justified in the remaining sections.

4. Two lemmas

Let $S$ be the spectrum of a complete discrete valuation ring, with generic point $\eta$ of characteristic zero, with closed point $s$, $k(s)$ finite of characteristic $\ell$.

Lemma 4.1. Let $d$ be an integer $\geq 1, \zeta \in \text{GL}_d(F_\ell)$ such that

$\zeta : e_1 \mapsto e_2, e_2 \mapsto e_3, \cdots, e_d \mapsto e_1,$

where $e_1, \cdots, e_d$ are the standard basis of $F_\ell^d$. 
The semi-direct product \(\langle \zeta \rangle F_{\ell}^d\) is a quotient of \(\pi_1(\eta, \overline{\eta})\). If \((\ell, d) = 1\) and \(V\) is an irreducible \(F_{\ell}\)-linear representation of \(\langle \zeta \rangle\), then \(\langle \zeta \rangle V\) is a quotient of \(\pi_1(\eta, \overline{\eta})\).

**Proof.** Let \(\eta' \rightarrow \eta\) be connected, unramified over \(S\) of degree \(d\). Let \(S'\) be the normalization of \(S\) in \(\eta', s' \in S'\) the closed point, \(\zeta \in \text{Gal}(\eta'/\eta)\) a generator, \(\pi \in \Gamma(O_S)\) a uniformizer, and \(u' \in \Gamma(O_{S'})^\times\) such that the images of \(u', \zeta(u'), \ldots, \zeta^{d-1}(u')\) in \(k(s')\) are a normal base over \(k(s)\).

Then
\[
\eta'[x_1, \ldots, x_d]/(x_1^d - x_1 - \zeta(u')\pi^{-1}, \ldots, x_d^d - x_d - \zeta^d(u')\pi^{-1})
\]
is connected, Galois over \(\eta\) of group \(\langle \zeta \rangle F_{\ell}^d\). If \((\ell, d) = 1\), \(\langle \zeta \rangle V\) is a quotient of \(\langle \zeta \rangle F_{\ell}^d\), thus is a quotient of \(\pi_1(\eta, \overline{\eta})\). \(\square\)

**Lemma 4.2.** Let \(p\) be a prime number different from \(\ell\).

1) If the underlying group of an \(F_{\ell}\)-vector space \(V\) is normal in a group \(\mathcal{G}\) such that \(\mathcal{G}\) acts irreducibly by conjugation on \(V\), then \(\mathcal{G}\) is a quotient of \(\pi_1(\eta, \overline{\eta})\) only if \(\dim V = 1\).

2) There is a unique group of affine linear transformations of \(F_{\ell}\) that contains all the translations and is a quotient of \(\pi_1(\eta, \overline{\eta})\) ramified over \(S\). This group has cardinality \(pd\), where \(d\) is the order of the element \(\text{Card}(k(s)) \mod p\) in \(F_{\ell}^\times\).

**Proof.**

1) Suppose \(\mathcal{G}\) is a quotient of \(\pi_1(\eta, \overline{\eta})\), with inertia group \(\mathcal{R}\), wild inertia subgroup \(\mathfrak{P}\). The intersection \(V \cap \mathcal{R}\), being normal in \(\mathcal{G}\), is a \(\mathcal{G}\)-module. Thus, \(V \cap \mathcal{R} = 1\) or \(V\).

If \(V \cap \mathcal{R} = 1\), \(V \hookrightarrow \mathcal{G}/\mathcal{R}\), so \(V\) is cyclic.

If \(V \cap \mathcal{R} = V\), as \(V \cap \mathfrak{P} = 1\), then \(V \hookrightarrow \mathcal{R}/\mathfrak{P}\), which also implies that \(V\) is cyclic.

2) Let \(\tau: x \mapsto x + 1, x \in F_{\ell}\). For any \(a \in F_{\ell}^\times\), let \(\sigma_a: x \mapsto ax, x \in F_{\ell}\). In the group of affine linear transformations of \(F_{\ell}\), \(\langle \tau \rangle\) is its own centralizer.

Suppose for some \(z \in F_{\ell}^\times\), \(\langle \tau, \sigma_z \rangle\) is a ramified quotient of \(\pi_1(\eta, \overline{\eta})\); let \(\mathcal{R}\) be its inertia subgroup, \(\mathfrak{P}\) the wild inertia subgroup.

Show \(\mathfrak{P} = 1\); for, \(\mathfrak{P}\) intersects \(\langle \tau \rangle\) in 1, thus commutes with \(\tau\), thus is contained in \(\langle \tau \rangle\), i.e. \(1\).

The group \(\mathcal{R} = \mathcal{R}/\mathfrak{P}\) is cyclic. And, \(\mathcal{R} \cap \langle \tau \rangle = 1\) or \(\langle \tau \rangle\); in any case, \(\mathcal{R}\) commutes with \(\tau\), hence is a subgroup of \(\langle \tau \rangle\), hence \(\mathcal{R} = \langle \tau \rangle\).

Write \(\pi'_1(\eta, \overline{\eta})\) for the maximal tame-along-\(s\) quotient of \(\pi_1(\eta, \overline{\eta})\). From its structure,
\[
\pi'_1(\eta, \overline{\eta}) = \langle \tau, \sigma | \sigma \tau \sigma^{-1} = \tau^s \rangle,
\]
where \( q = \text{Card}(k(s)) \), it follows that \( \langle \sigma_z \rangle \) is generated by \( \sigma_{z'} \), \( z' := \text{Card}(k(s)) \mod p \). Now, 2) is clear. \( \square \)

5. Type A

Let \( (S, \eta, s) \), \( \text{char}(s) = \ell \), be as in §4.

**Proposition 5.1.** For any integer \( n \geq 1 \), \( (A_n, \alpha_1) \), \( (A_n, \alpha_n) \) are elliptic over \( \eta \).

**Proof.** The subgroup of \( \eta \) elliptic over \( n \), \( \{ 1, \ldots, n + 1 \} \) and on the collection of subsets of \( \{ 1, \ldots, n + 1 \} \) of cardinality \( n \). As \( \langle (12 \cdots n + 1) \rangle = \mathbb{Z}/(n+1)\mathbb{Z} \) is a quotient of \( \pi_1(\eta, \overline{\eta}) \), the pairs \( (A_n, \alpha_i) \), \( i = 1, n \), are elliptic over \( \eta \), (3.1), 1). \( \square \)

**Lemma 5.2.** Let \( X \) be a finite set of cardinality \( q \geq 4 \), \( \mathcal{G} \) a solvable subgroup of \( \text{Aut}(X) \) permuting transitively the subsets of \( X \) of cardinality \( r \), \( 2 \leq r \leq q/2 \). Then \( r < 4 \).

1) If \( r = 2 \), \( \mathcal{G} \) is 2-transitive on \( X \), unless \( X = F_q \), \( q \equiv 3 \mod 4 \), and \( \mathcal{G} \) is the group of transformations

\[
x \mapsto a \sigma(x) + b, \ x \in F_q, \ a \in (F_q^*)^2, \ b \in F_q, \ \sigma \in \text{Gal}(F_q/k)
\]

where \( k \) is a subfield of \( F_q \).

2) If \( r = 3 \), \( X = F_{32} \) or \( F_8 \). If \( X = F_{32} \), \( \mathcal{G} \) consists of all affine semi-linear transformations of \( X \). If \( X = F_8 \), \( \mathcal{G} \) consists of either all affine semi-linear transformations or only the affine linear transformations of \( X \).

**Proof.** That \( r < 4 \), as well as 2), is extracted from [6], p. 402–403.

If \( r = 2 \) and \( \mathcal{G} \) is not 2-transitive on \( X \), then by loc.cit., \( X = F_{p^d} \), \( p \) prime \( \equiv 3 \mod 4 \), \( d \) is odd, \( \mathcal{G} = \mathfrak{L} F^d_p, \ \mathfrak{L} \leq \text{GL}_d(F_p), \ \text{Card}(\mathfrak{L}) \) is odd. In this situation, \( -1 : x \mapsto -x, \ x \in X \), normalizes \( \mathcal{G} \), \( \{ 1, -1 \} \mathcal{G} \) is 2-transitive on \( X \), and 1) follows from the well-known classification of 2-transitive solvable permutation groups. \( \square \)

**Corollary 5.3.** If \( 4 \leq r \leq (n+1)/2 \), \( (A_n, \alpha_r) \), \( (A_n, \alpha_{n+1-r}) \) are not elliptic over \( \eta \). The pairs \( (A_n, \alpha_3) \), \( (A_n, \alpha_{n-2}) \) are elliptic over \( \eta \) only if \( n = 7 \) or 31. The pairs \( (A_n, \alpha_2) \), \( (A_n, \alpha_{n-1}) \) are elliptic over \( \eta \) only if \( n = p^d - 1, \ p \) prime, \( d \geq 1 \).

**Proof.** This is immediate from (5.2), (3.1), 1). \( \square \)

**Proposition 5.4.** Let \( p \) be a prime number, \( d \geq 1 \), \( n = p^d - 1 \). Then \( (A_n, \alpha_2) \), \( (A_n, \alpha_{n-1}) \) are elliptic over \( \eta \) if \( p = \ell \), and only if \( p = \ell \), when \( d \geq 2 \).
Proof. Any solvable subgroup of $S_{n+1}$ transitive on the collection of subsets of $\{1, \cdots , n+1\}$ of cardinality 2 is of the form $S = LF^d$, where $L$ is a subgroup of $GL_d(F_p)$ irreducible on $F^d$. When $d \geq 2$, by (4.2), 1), $S$ is a quotient of $\pi_1(\eta, \ell)$ only if $p = \ell$, therefore, $(A_n, \alpha_2)$, as well as $(A_n, \alpha_{n-1})$, is elliptic only if $p = \ell$, (3.1), 1).

Suppose $p = \ell$. The group of affine linear transformations of $F_p \{1, \cdots , n+1\}$ is 2-transitive, and is a quotient of $\pi_1(\eta, \ell)$ (4.1), thus, $(A_n, \alpha_2), (A_n, \alpha_{n-1})$ are elliptic. \hfill $\Box$

**Proposition 5.5.** Let $p$ be an odd prime different from $\ell$, $n = p-1$. For $p \equiv 1 \mod 4$, $(A_n, \alpha_2), (A_n, \alpha_{n-1})$ are elliptic over $\eta$ if and only if Card($k(s)$) mod $p$ generates $F^\times_p$. For $p \equiv 3 \mod 4$, $(A_n, \alpha_2), (A_n, \alpha_{n-1})$ are elliptic over $\eta$ if and only if Card($k(s)$) mod $p$ generates a subgroup of $F^\times_p$ of index $\leq 2$.

**Proof.** The pairs $(A_n, \alpha_2), (A_n, \alpha_{n-1})$ are elliptic over $\eta$ if and only if some representation $\rho : \pi_1(\eta, \ell) \rightarrow S_p$ has image transitive on the collection of 2-point subsets of $\{1, \cdots , p\} = F_p$, (3.1), 1).

By (5.2), 1), and the classification of 2-transitive solvable permutation groups of degree $p$, the image of $\rho$ has to be either the group of all affine linear transformations of $F_p$, or, if $p \equiv 3 \mod 4$, the group of affine linear transformations of $F_p$ generated by the translations and the scalar multiplications $x \mapsto ax, a \in (F^\times_p)^2$.

Now, (4.2), 2) applies. \hfill $\Box$

**Proposition 5.6.** The pairs $(A_7, \alpha_3), (A_7, \alpha_5)$ are elliptic over $\eta$ if and only if $s$ is of characteristic 2.

**Proof.** Either of the two solvable subgroups of $S_8$ transitive on the collection of 3-point subsets of $\{1, \cdots , 8\} = F_8$, contains an $F_8$, (5.2), 2). So $(A_7, \alpha_3), (A_7, \alpha_5)$ are elliptic over $\eta$ only if $s$ is of characteristic 2, (3.1), 1).

If char($s$) = 2, the group of affine transformations of $F_8$ is a quotient of $\pi_1(\eta, \ell)$, (4.1), therefore, $(A_7, \alpha_3), (A_7, \alpha_5)$ are elliptic over $\eta$, (3.1), 1). \hfill $\Box$

**Proposition 5.7.** The pairs $(A_{31}, \alpha_3), (A_{31}, \alpha_{29})$ are elliptic over $\eta$ if and only if $s$ is of characteristic 2 and $5 \nmid [s : F_2]$.

**Proof.** The pairs $(A_{31}, \alpha_3), (A_{31}, \alpha_{29})$ are elliptic over $\eta$ if and only if the group $S$ of affine semi-linear transformations of $F_{32}$ is a quotient of $\pi_1(\eta, \ell)$, (3.1), 1), (5.2), 2).
As $G$ contains $F_{32}$, it is a quotient of $\pi_1(\eta, \overline{\eta})$ only if $s$ is of characteristic 2.

Suppose $\text{char}(s) = 2$.

Evidently, when $G$ is a Galois group, its wild inertia subgroup must consist of all translations, its inertia subgroup all affine linear transformations, and the group $G^t$, generated by the Frobenius and scalar multiplications, be isomorphic to the maximal tame quotient of $G$.

By (4.2), $G^t$ is a quotient of $\pi_1(\eta, \overline{\eta})$ if and only if $\text{Card}(k(s)) \mod 31$ is of order 5 in $F_{31}^\times$, or equivalently, $5 \nmid [s : F_2^\times]$ for $\text{Card}(k(s)) = 2^{[s : F_2]}$ and 2 is of order 5 in $F_{31}^\times$.

Suppose $5 \nmid [s : F_2^\times]$.

Let $\eta' \to \eta$ be connected, unramified over $S$ of degree 5, let $S'$ be the normalization of $S$ in $\eta'$, $s' \in S'$ the closed point, $\zeta \in \text{Gal}(\eta'/\eta)$ a generator, $\pi \in \Gamma(O_S)$ a uniformizer, and $u' \in \Gamma(O_{S'})^\times$ such that the images of $u'$, $\zeta(u')$, $\cdots$, $\zeta^4(u')$ in $k(s')$ form a normal basis over $k(s)$.

Then

$$\eta'[z, x_1, \cdots, x_5]/(z^{31} - \pi, x_2^2 - 1 - z\zeta(u'), \cdots, x_5^2 - 1 - z\zeta^5(u'))$$

is connected, Galois over $\eta$ of group $G$.

\[\Box\]

6. Type $^2A$

**Lemma 6.1.** Let $d$ be an integer $\geq 1$, $X$ a set with $2d - 1$ elements, $G$ a solvable subgroup of $\text{Aut}(X)$ permuting transitively the subsets of $X$ of cardinality $d$. Then $X, G$ are

1) $X = 1$, $G = 1$.

2) $X = \{1, 2, 3\}$, $G = S_3$ or $A_3$.

3) $X = F_5$, $G$ consists of all affine linear transformations $A_{a,b} : x \mapsto ax + b$, $x \in F_5$, $a \in F_5^\times$, $b \in F_5$.

**Proof.** If $d = 1$, $X = 1$, $G = 1$, hence 1). Suppose $d > 1$.

Show $G$ is transitive on $X$: otherwise, some $G$-orbit, say $O$, has cardinality $< d$. Imbed $O$ into a set $Y$ with $d$ elements. Then $O = gO \subset gY$, $\forall g \in G$, that is, $O$ is contained in every subset of $X$ of cardinality $d$. But as $\text{Card}(X \setminus O) > (2d - 1) - d = d - 1$, $X \setminus O$ contains a set $Y'$ with $d$ elements, which is disjoint with $O$.

Fix a point $o \in X$, let $G_o$ be its stabilizer in $G$. 


Show $G_o$ is a maximal subgroup of $G$: assume $G_o < H < G$, for a group $H$. Then $1 < (G : H), (H : G_o) < d$, because

$$(G : H)(H : G_o) = (G : G_o) = \text{Card}(G_o) = \text{Card}(X) = 2d - 1.$$ 

As $H.o \simeq H/G_o$, $X \setminus H.o$ has cardinality $>(2d - 1) - d = d - 1$. Pick a $Y \subset X \setminus H.o$ with $d$ elements so that $gY \cap gH.o = \emptyset$, $\forall g \in G$. Hence any subset of $X$ of cardinality $d$ is disjoint with some $gH.o$. But if $R$ is a set of representatives for $G/H$, as $\text{Card}(R.o) \leq \text{Card}(R) = (G : H) < d$, a set $Y' \supset R.o$ with $d$ elements intersects all $gH.o$, $g \in G$.

Show $G_o$ does not contain normal subgroups of $G$ other than $1$: given $N \leq G_o$, $N$ normal in $G$, then $Ng.o = gN.o = o$, $\forall g \in G$, i.e. $N$ fixes pointwise $G.o = X$. So $N = 1$.

Let $U$ be the last term $> 1$ in the derived series of $G$. Since $G$ is solvable, $[U, U] = 1$, i.e. $U$ is abelian, thus is a $G$-module. Let $V \subset U$ be a simple sub-$G$-module; it is an $\mathbb{F}_p$-vector space for a prime number $p$. Let $f = \dim V$.

Show $V G_o = G$: since $V$ is not a subgroup of $G_o$, $V G_o$ contains $G_o$ properly. So $V G_o = G$, for $G_o$ is maximal in $G$.

Show $V \cap G_o = 1$ : the group $V \cap G_o$ is normalized by $G_o$ and by $V$, $V$ being abelian, thus by $V G_o = G$. Hence, $V \cap G_o$ is a sub-$G$-module of $V$, and is different from $V$, therefore is $1$.

Show $V \to X$, $v \mapsto v.o$, is a bijection: it is surjective because $X = G.o = V G_o.o = V.o$. It is injective because if $v.o = v'.o$, then $v^{-1}v' \in V \cap G_o = 1$, that is, $v = v'$.

Now, $p^f = \text{Card}(V) = \text{Card}(X) = 2d - 1$, so $p > 2$.

Show the representation $G_o \to \text{GL}(V)$, $g \mapsto \text{int}(g)$, is faithful: if $g \in G_o$ and $\text{int}(g) = 1$, then $gv.o = gvg^{-1}.o = \text{int}(g)(v.o) = v.o$, $\forall v \in V$, i.e. $g$ stabilizes each point of $V.o = X$. So $g = 1$.

Let $p'$ be a prime number with $d < p' < 2d$ (Bertrand’s postulate).

Show $p' = p$: suppose $p' \neq p$. Note that $p'$ divides $\binom{2d - 1}{d}$, the number of subsets of $X$ of cardinality $d$, thus divides $\text{Card}(G) = p^f \text{Card}(G_o)$, thus divides $\text{Card}(G_o)$, then divides $\text{Card}(\text{GL}(V))$. So $p'$ divides $p^i - 1$, for some $i = 1, \cdots, f$, i.e. $p' = p^i - 1$, since $p^i - 1 = 2d - 2 < 2p' - 2$. But $p'$ is odd, $p^i - 1$ is even.

Show $f = 1$: it is because $p^f = 2d - 1 < 2p' - 1 = 2p - 1$.

Show $d \leq 3$: one has the division

$$\binom{2d - 1}{d} \mid \text{Card}(G) \mid p \text{.Card}(\text{GL}(V)) = p(p - 1) = (2d - 1)(2d - 2).$$
If $d = 4$, $(\frac{2^d-1}{d}) = 35$ does not divide $(2d - 1)(2d - 2) = 42$. If $d \geq 5$, $(\frac{2^d-1}{d}) > (2d - 1)(2d - 2)$.

If $d = 2$, $X = \{1, 2, 3\}$. As $\mathfrak{G}$ is transitive on $X$, it may be $\mathfrak{S}_3$ or $\mathfrak{A}_3$.

Both do permute transitively the 2-point subsets of $X$, hence 2).

If $d = 3$, $X \simeq V$ has 5 elements, 10 subsets of cardinality 3. Since $\mathfrak{G} \leq V\text{GL}(V)$, $\text{Card}(\mathfrak{G})$ divides 20, thus $\text{Card}(\mathfrak{G}) = 20$ or 10. Accordingly, $\mathfrak{G}$ may be $V\text{GL}(V)$, the group of affine linear transformations of $V = \mathbb{F}_5$, or its subgroup $\mathfrak{H}$ consisting of those $A_{a,b}: x \mapsto ax + b$, such that $a \in (\mathbb{F}_5^\times)^2$.

The group $V\text{GL}(V)$ is transitive on the 3-point subsets of $X$, for it is 2-transitive on $X$: given $u, v \in \mathbb{F}_5$, $u \neq v$, there is an affine linear transformation $A_{a,b}: x \mapsto ax + b$ such that $A_{a,b}(0) = u$, $A_{a,b}(1) = v$. Indeed, $b = u$, $a = v - u$.

The group $\mathfrak{H}$ permutes the 2-point subsets of $X$ in two orbits, namely, the collection of $\{u, v\} \subset X$, where respectively $u - v$ is or is not a square of $\mathbb{F}_5^\times$. So on the 3-point subsets of $X$, $\mathfrak{H}$ has two orbits as well.

Therefore, when $d = 3$, $\mathfrak{G} = V\text{GL}(V)$, hence 3). □

Now, suppose given an integer $d \geq 1$, a set $X$ with $2d$ elements, a solvable subgroup $\mathfrak{G}$ of $\text{Aut}(X)$ permuting the subsets of $X$ of cardinality $d$ in 2 orbits.

**Lemma 6.2.** If $\mathfrak{G}$ is not transitive on $X$, 1) or 2) or 3) hold:
1) $X = \{o, 1\}$, $\mathfrak{G} = 1$.
2) $X = \{o, 1, 2, 3\}$, $\mathfrak{G}$ fixes $o$; on $\{1, 2, 3\}$, it is either $\mathfrak{S}_3$ or $\mathfrak{A}_3$.
3) $X = \{o\} \cup \mathbb{F}_5$, $\mathfrak{G}$ fixes $o$ and is the group of affine linear transformations of $\mathbb{F}_5$.

**Proof.** Let $O \subset X$ be a $\mathfrak{G}$-orbit of cardinality $\leq d$. Pick $Y' \subset Y \subset X$ with $d$ elements such that $Y' \supset O$, $Y \cap O = \emptyset$. Then $gY' \supset O$, $gY \cap O = \emptyset$, $\forall g \in \mathfrak{G}$. Thus any subset of $X$ of cardinality $d$ either contains $O$ or is disjoint with it. Let $o \in O$, $y \in Y$. The set $\{o\} \cup Y \setminus \{y\}$ has $d$ elements and intersects $O$ in $\{o\}$. So $O = \{o\}$.

Since $X \setminus \{o\}$ has $2d - 1$ elements and its subsets of cardinality $d$ are permuted transitively by $\mathfrak{G}$, the previous lemma applies. □

**Lemma 6.3.** Let $o \in X$, $\mathfrak{G}_o$ its stabilizer in $\mathfrak{G}$. If $\mathfrak{G}$ is transitive on $X$, $\mathfrak{G}_o \lhd \mathfrak{H} \lhd \mathfrak{G}$ for a group $\mathfrak{H}$, with $(\mathfrak{G} : \mathfrak{H})$ even, then either 1) or 2) holds:
1) $X = \mathbb{Z}/4\mathbb{Z}$, $\mathfrak{G}$ consists of either all transformations

\[ A_{a,b}: x \mapsto ax + b, \; x \in \mathbb{Z}/4\mathbb{Z} \]
Proof. Let \( G : H \approx 2r \). Note that
\[
d = \frac{\text{Card}(X)}{2} = \frac{(G : H)}{2} = r \text{Card}(H,o).
\]

If \( R = \{g_1, \ldots, g_{2r}\} \subset G \) is a set of representatives for \( G/H \), \( Z := \{g_1, \ldots, g_r\}H.o \) has \( d \) elements.

As \( \text{Card}(R,o) \leq \text{Card}(R) = 2r \leq d \), a set \( Z' \supset R,o \) with \( d \) elements intersects all \( gH,o, g \in G \).

Thus any subset of \( X \) of cardinality \( d \) either equals \( \tau H.o \) for some \( \tau \in R \) of cardinality \( r \), or intersects all \( gH,o, g \in G \).

Necessarily, \( r = 1 \) : if \( r > 1 \), \( \{g_1, \ldots, g_r\}H.o \cup \{g_{r+1},o\}\} \{g_{r+1},o\} \) has \( d \) elements, is disjoint with \( g_{2r},H,o \), but is not a \( JH,o \), for any \( J \subset R \).

So \( R = \langle g_1, g_2 \rangle \), \( \text{Card}(H,o) = d \), \( X = H.o \cup \tau H.o, \tau = g_2^{-1}g_2 \), and the subsets of \( X \) of cardinality \( d \) distinct from \( H.o, \tau H.o \) are permuted transitively by \( G \).

Show \( d \leq 3 \): if \( d > 3 \), if \( o' \in H.o \setminus \{o\} \), both
\[
Y = \{o\} \cup \tau H.o \setminus \{\tau.o\}, \quad Y' = \{o, o'\} \cup \tau H.o \setminus \{\tau.o, \tau.o'\}
\]
are of cardinality \( d \), different from \( H.o, \tau H.o \), but \( Y \neq gY', \forall g \in G \), for \( Y \cap H.o \) has 1 element, while \( gY' \cap H.o, \) as \( Y' \cap g^{-1}H.o \), has either 2 or \( d - 2 \) elements.

If \( d = 2 \), \( \text{Card}(X) = 4 \), \( \text{Card}(H,o) = 2 \), \( H \leq \text{Aut}(H.o) \times \text{Aut}(\tau H.o), \)
\( \text{Card}(H) = 4 \) or 2, \( \text{Card}(G) = 8 \) or 4.

If \( \text{Card}(G) = 8 \), \( G \) is a 2-Sylow subgroup of \( \text{Aut}(X) = G_4 \), therefore is isomorphic to the group of transformations \( A_{a,b} : x \mapsto ax + b, a \in (\mathbb{Z}/4\mathbb{Z})^\times, b \in \mathbb{Z}/4\mathbb{Z}, \text{ on } X = \mathbb{Z}/4\mathbb{Z} \). The subgroup \( H \) consists of those \( A_{a,b} : x \mapsto ax + b, \) where \( b \equiv 0 \mod 2 \); it is the Klein group and permutes the 2-point subsets of \( X \) in 3 orbits.

If \( \text{Card}(G) = 4 \), \( G \) is of index 2 in a 2-Sylow subgroup of \( G_4 \), but cannot be a Klein group, thus must be the group of translations \( x \mapsto x + b, b \in \mathbb{Z}/4\mathbb{Z}, \text{ on } X = \mathbb{Z}/4\mathbb{Z} \). And \( H \) consists of those \( x \mapsto x + b, \) where \( b \equiv 0 \mod 2 \).
In either case, the 2-point subsets \( \{0, 2\}, \{1, 3\} \) of \( X = \mathbb{Z}/4\mathbb{Z} \) form one \( \mathcal{G} \)-orbit, and \( \{0, 1\}, \{0, 3\}, \{2, 1\}, \{2, 3\} \) form the other orbit, hence 1).

Consider the situation \( d = 3 \), \( \text{Card}(X) = 6 \) : evidently, \( \mathcal{G} \) is not contained in \( \text{Aut}(\mathcal{H} \circ) \times \text{Aut}(\tau \mathcal{H} \circ) \). Let \( \mathcal{N} \) be the normalizer in \( \text{Aut}(X) \) of the partition \( X = \mathcal{H} \circ \cup \tau \mathcal{H} \circ \); the cardinality of \( \mathcal{N} \) is 72. As the 3-point subsets of \( X \) distinct from \( \mathcal{H} \circ \) and \( \tau \mathcal{H} \circ \), 18 in number, are permutated transitively by \( \mathcal{G} \), \( \text{Card}(\mathcal{G}) \) is divisible by 18, thus \( (\mathcal{N} : \mathcal{G}) = 1, 2 \) or 4.

Write \( X = \{1, \ldots, 6\} \), \( \mathcal{H} \circ = \{1, 2, 3\} \), \( \tau \mathcal{H} \circ = \{4, 5, 6\} \). Then \( \mathcal{G} = \mathcal{P} \mathcal{Q} \), where \( \mathcal{P} = \text{Alt}(\{1, 2, 3\}) \times \text{Alt}(\{4, 5, 6\}) \) is the 3-Sylow subgroup of \( \mathcal{G} \), \( \mathcal{Q} \) is a 2-Sylow subgroup of \( \mathcal{G} \), of order 2, 4 or 8.

i) If \( \text{Card}(\mathcal{Q}) = 2 \), i.e. \( \mathcal{Q} = \{1, \gamma\} \), \( \gamma \) is of order 2. If say \( \gamma : 1 \mapsto 4, 2 \mapsto 5, 3 \mapsto 6 \), then \( \gamma = (14)(25)(36) \).

ii) Suppose \( \mathcal{Q} \) is cyclic of order 4 of generator \( \gamma \), and \( \gamma : 1 \mapsto 4, 2 \mapsto 5, 3 \mapsto 6 \). As \( \gamma^2 \) is of order 2, normalizes \( \{1, 2, 3\} \), it fixes a point, say 3. Then \( \gamma^2(6) = \gamma^2(\gamma(3)) = \gamma(\gamma^2(3)) = \gamma(3) = 6 \), so \( \gamma = (1425)(36) \).

iii) Consider \( \mathcal{Q} = \{1, \alpha, \beta, \gamma\} \) of order 4, non cyclic, \( \gamma \) normalizing \( \{1, 2, 3\} \). Then \( \gamma \) fixes a point, say 3. If \( \beta : 1 \mapsto 4, 2 \mapsto 5, 3 \mapsto 6 \), i.e. \( \beta = (14)(25)(36) \), then \( \alpha(3) = \alpha(\gamma(3)) = \beta(3) = 6 \), and \( \alpha = (15)(24)(36) \), \( \gamma = (12)(45) \).

iv) If \( \text{Card}(\mathcal{Q}) = 8 \), \( \mathcal{G} = \mathcal{N} \).

Observe that \( \mathcal{P} \) has 4 orbits on the 3-point subsets of \( X \); and, one inspects that in all the cases i)--iv) \( \mathcal{G} \) permutes the 3-point subsets of \( X \) in 2 orbits, hence 2).

\[ \square \]

**Lemma 6.4.** Let \( o \in X \), \( \mathcal{G}_o \) its stabilizer in \( \mathcal{G} \). If \( \mathcal{G} \) is transitive on \( X \), \( \mathcal{G}_o \subset \mathcal{H} \circ < \mathcal{G} \), with \( (\mathcal{G} : \mathcal{H}) \) odd, then \( X = \{1, \ldots, 6\} \), \( \mathcal{G} \) is either the normalizer \( \mathcal{N} \) in \( \text{Aut}(X) \) of a partition \( X = \{a, a'\} \cup \{b, b'\} \cup \{c, c'\} \), or the subgroup of \( \mathcal{N} \) generated by \( (aa'), (bb'), (cc'), (abc)(a'b'c') \).

**Proof.** Let \( (\mathcal{G} : \mathcal{H}) = 2r + 1, r \geq 1 \), \( \mathcal{R} = \{g_1, \ldots, g_{2r+1}\} \subset \mathcal{G} \) a set of representatives for \( \mathcal{G}/\mathcal{H} \). Since

\[ d = \frac{\text{Card}(X)}{2} = \frac{(\mathcal{G} : \mathcal{H})}{2}(\mathcal{H} : \mathcal{G}_o) = (r + \frac{1}{2}) \text{Card}(\mathcal{H} \circ \circ), \]

\( \text{Card}(\mathcal{H} \circ \circ) \) is even, \( = 2f \), \( f \geq 1 \). Pick \( B \subset g_{r+1}\mathcal{H} \circ \circ \setminus \{g_{r+1} \circ \circ\} \) of cardinality \( f \). Then \( Y = \{g_1, \ldots, g_r\} \mathcal{H} \circ \circ \cup B \) has \( d \) elements. As \( \text{Card}(\mathcal{R} \circ) \leq \text{Card}(\mathcal{R}) \leq d \), a set \( Y' \supset \mathcal{R} \circ \circ \cup B' \), for some \( J \subset \mathcal{R} \circ \circ \), of cardinality
r, some $B' \subset z\mathfrak{H}.o$ of cardinality $f$, $z \in \mathfrak{R}\setminus\mathfrak{I}$. In the latter case, $Z$ intersects precisely $r + 1$ members of $\{g_1\mathfrak{H}.o, \ldots, g_{2r+1}\mathfrak{H}.o\}$.

Show $f = 1$ : if $f > 1$, the set

$$\{g_1, \cdots, g_{r-1}\} \mathfrak{H}.o \cup (g_r\mathfrak{H}.o\setminus\{g_r.o\}) \cup (B \cup \{g_{r+1}.o\})$$

has $d$ elements, is disjoint with $g_{2r+1}\mathfrak{H}.o$, but is not a $\mathfrak{H}.o \cup B'$ for any $\mathfrak{J} \subset \mathfrak{R}$ of cardinality $r$, $B' \subset z\mathfrak{H}.o$ of cardinality $f$, $z \in \mathfrak{R}\setminus\mathfrak{I}$.

Thus $\text{Card}(B) = f = 1$, $d = 2r + 1$.

Show $r = 1$ : if $r > 1$, the set

$$\{g_1, \cdots, g_{r-1}\} \mathfrak{H}.o \cup (g_r\mathfrak{H}.o\setminus\{g_r.o\}) \cup (g_{r+1}.o \cup \{g_{2r+1}.o\})$$

has $d$ elements, is disjoint with $g_{2r+1}\mathfrak{H}.o$, but intersects $r + 2$, rather than $r + 1$, members of $\{g_1\mathfrak{H}.o, \cdots, g_{2r+1}\mathfrak{H}.o\}$.

This gives $d = 2r + 1 = 3$, $\mathfrak{R} = \{g_1, g_2, g_3\}$, $\text{Card}(\mathfrak{H}.o) = 2$, and $X$ has 6 elements, 20 subsets of cardinality 3, among which 8 intersect all $g_j\mathfrak{H}.o$, $j \in \{1, 2, 3\}$. So $\mathfrak{G}$ has order divisible by 8 and by $20 - 8 = 12$, thus divisible by 24 ; it is either $\mathfrak{N}$, the normalizer in $\text{Aut}(X)$ of the partition $X = g_1\mathfrak{H}.o \cup g_2\mathfrak{H}.o \cup g_3\mathfrak{H}.o$, or the subgroup of $\mathfrak{N}$ of index 2, generated by $\text{Aut}(g_j\mathfrak{H}.o)$ and an element $\gamma \in \text{Aut}(X)$ of order 3, which rotates $g_j\mathfrak{H}.o$, $j = 1, 2, 3$.

In either case, $\mathfrak{G}$ permutes the 3-point sets of $X$ in 2 orbits, hence the lemma. \hfill $\square$

**Lemma 6.5.** Let $o \in X$, $\mathfrak{G}_o$ its stabilizer in $\mathfrak{G}$. If $\mathfrak{G}$ is transitive on $X$, and $\mathfrak{G}_o$ is a maximal subgroup of $\mathfrak{G}$, then $X = \mathbb{F}_8$, $\mathfrak{G}$ consists of either all affine semi-linear transformations

$$A_{a,b,c} : x \mapsto ax^{2^c} + b, \quad x \in \mathbb{F}_8,$$

$a \in \mathbb{F}_8^\times$, $b \in \mathbb{F}_8$, $c \in \mathbb{Z}/3\mathbb{Z}$, or only the affine linear transformations

$$A_{a,b} : x \mapsto ax + b, \quad x \in \mathbb{F}_8,$$

$a \in \mathbb{F}_8^\times$, $b \in \mathbb{F}_8$.

**Proof.** One has that $\mathfrak{G} = V\mathfrak{G}_o$, for a group $V$, where $V$ is normal in $\mathfrak{G}$, simply transitive on $X$, isomorphic to a vector space over a prime field $\mathbb{F}_p$, and is a faithful irreducible representation of $\mathfrak{G}_o$. Identify $V$ with $X$ via the bijection $v \mapsto v.o$. If $f = \dim V$, $p^f = \text{Card}(V) = \text{Card}(X) = 2d$. So $p = 2$, $d = 2^{f-1}$. Clearly, $f > 1$.

Show $f > 2$ : otherwise, $\mathfrak{G}_o$ being irreducible on $V$, cannot be a 2-group, thus is of order divisible by 3. So, $\mathfrak{G} = \mathfrak{S}_3$ or $\mathfrak{A}_4$. But both are transitive, rather than have 2 orbits, on the 2-point subsets of $X$.

Therefore, $d = 2^{f-1} \geq 4$. 

A hyperplane $H$ of $V$ has $2^f - 1 = d$ elements. Given different hyperplanes $H_1, H_2$, the intersection $H_1 \cap H_2$ has dimension $f - 2$, cardinality $2^{f-2} = d/2$, and $\text{Card}(H_2 \backslash H_1) = d/2$. For any $g \in \mathfrak{G}$, either $gH$ or $V \backslash gH$ is a hyperplane. Consequently, $\text{Card}(gH \backslash H) \in \{0, d, d/2\}$.

Fix $v \in V \backslash H$. The set $Y := \{v\} \cup H \backslash \{0\}$ has $d$ elements. As $\text{Card}(Y \backslash H) = 1 \notin \{0, d, d/2\}$, neither $Y$ nor its complement is a hyperplane.

Hence the subsets of $V$ of cardinality $d$ are $gH$, and $gY$, $g \in \mathfrak{G}$.

Show $f = 3$: if $f \geq 4$, if $u \in H \backslash \{0\}$, the set

$$Z = \{v, u + v\} \cup H \backslash \{0, u\}$$

is of cardinality $d$, $\neq gH, gY$, because $\text{Card}(gH \backslash H) \in \{0, d, d/2\}$, $\text{Card}(gY \backslash H) = \text{Card}(Y \backslash g^{-1}H) \in \{1, d - 1, d/2, (d/2) \pm 1\}$, while $\text{Card}(Z \backslash H) = 2 \neq 0, 1, d, d - 1, d/2, (d/2) \pm 1$, as $d \geq 8$.

Now $P(V) = \mathbb{P}^2$; it has 7 points rational over $\mathbb{F}_2$, that is, $V$ has 7 hyperplanes. So 7 divides $\text{Card}(\mathfrak{G})$ and $\text{Card}((\mathfrak{G})_o)$. Once choosing an identification $V = \mathbb{F}_8$, a 7-Sylow subgroup of $\mathfrak{G}_o$ is the group of scalar multiplications $\sigma_a : x \mapsto ax, x \in \mathbb{F}_8, a \in \mathbb{F}_8^\times$.

Suppose $g \in \text{GL}(V)$ normalizes $\{\sigma_a\}$. As $\det(T - g \sigma_a g^{-1}, V) = \det(T - \sigma_a, V) = (T - a)(T - a^2)(T - a^4)$, there exists a $c \in \mathbb{Z} / 3\mathbb{Z}$ such that $g \sigma_a g^{-1} = \sigma_{F^c(a)} = F^c \sigma_a F^{-c}$, where $F : x \mapsto x^2$ is the Frobenius. It follows that $F^c g$ commutes with $\{\sigma_a\}$, thus lies in $\{\sigma_a\}$. Hence the normalizer $\mathfrak{N}$ of $\{\sigma_a\}$ in $\text{GL}(V)$ is the group of transformations $x \mapsto ax^{2^c}, a \in \mathbb{F}_8^\times, c \in \mathbb{Z} / 3\mathbb{Z}$. Note that $\text{Card}(\mathfrak{N}) = 21$.

Show 2 \mho Card(\mathfrak{G}_o): otherwise, $\mathfrak{G}_o$ being solvable, let $\mathfrak{H} \leq \mathfrak{G}_o$ be a Hall subgroup containing $\{\sigma_a\}$ and of order $7^j, j \geq 1$. Necessarily, $j \leq 3$, because $\text{Card}(\text{GL}(V)) = 2^3 \cdot 3 \cdot 7$. As $\text{Card}(\mathfrak{N}) = 21$, $\mathfrak{H}$ is not a subgroup of $\mathfrak{N}$; that is, $\{\sigma_a\}$ is not normal in $\mathfrak{H}$, so $j \neq 1, 2$. If $j = 3$, $\mathfrak{H}$ has a unique 2-Sylow subgroup $\mathfrak{Q}$, for the number of 7-Sylow subgroups of $\mathfrak{H}$ is $\equiv 1 \mod 7$, i.e. 8. Then since $\mathfrak{Q}$ is 2-Sylow in $\text{GL}(V)$, the center of $\mathfrak{Q}$ is of order 2, normalized by $\{\sigma_a\}$, thus centralized by $\{\sigma_a\}$, therefore contained in $\mathfrak{N}$. This is absurd.

As $\text{Card}(\mathfrak{G}_o) = 7$ or 21, $\{\sigma_a\}$ is normal in $\mathfrak{G}_o$, i.e. $\mathfrak{G}_o \leq \mathfrak{N}$, and $\mathfrak{G}$ may be $V \mathfrak{N}$, the group of affine semi-linear transformations

$$A_{a,b,c} : x \mapsto ax^{2^c} + b, x \in \mathbb{F}_8,$$

$a \in \mathbb{F}_8^\times, b \in \mathbb{F}_8, c \in \mathbb{Z} / 3\mathbb{Z}$, or its subgroup $V\{\sigma_a\}$ consisting of the affine linear transformations

$$A_{a,b} : x \mapsto ax + b, x \in \mathbb{F}_8,$$

$a \in \mathbb{F}_8^\times, b \in \mathbb{F}_8$. 

In \( \mathbb{F}_8 \), there are 70 subsets of cardinality 4. So both groups have > 1 orbits on these subsets. The 7 hyperplanes and their complements evidently form one orbit under either group. Given a \( Y \) in the rest \( 70 - 14 = 56 \) subsets of cardinality 4, if \( \mathcal{S} \) denotes the stabilizer of \( Y \) in \( V\{\sigma_a\} \), then \( \mathcal{S} \leq \text{Aut}(Y) = \mathcal{S}_4 \), in particular, \( 7 \nmid \text{Card}(\mathcal{S}) \), so \( \mathcal{S} \) is contained in the group of translations, thus \( \mathcal{S} = 1 \), by the choice of \( Y \), whence the orbit \( V\{\sigma_a\}.Y \) consists of 56 members. This concludes the proof. \( \square \)

Summarizing (6.2)–(6.5), one obtains

**Proposition 6.6.** Let \( d \) be an integer \( \geq 1 \), \( X \) a set with \( 2d \) elements, \( \mathcal{G} \leq \text{Aut}(X) \) a solvable subgroup permuting the subsets of \( X \) of cardinality \( d \) in 2 orbits. Then \( X, \mathcal{G} \) are classified as

1) \( X = \{o, 1\}, \mathcal{G} = 1 \).
2) \( X = \{o, 1, 2, 3\}, \mathcal{G} \) fixes \( o \); on \( \{1, 2, 3\} \), it is \( \mathcal{S}_3 \) or \( \mathcal{A}_3 \).
3) \( X = \{o\} \cup \mathbb{F}_5, \mathcal{G} \) fixes \( o \) and is the group of affine linear transformations of \( \mathbb{F}_5 \).
4) \( X = \mathbb{Z}/4\mathbb{Z}, \mathcal{G} \) consists of either all transformations
   \[ A_{a,b} : x \mapsto ax + b, \ x \in \mathbb{Z}/4\mathbb{Z}, \ a \in (\mathbb{Z}/4\mathbb{Z})^\times, b \in \mathbb{Z}/4\mathbb{Z}, \text{ or only } x \mapsto x + b, b \in \mathbb{Z}/4\mathbb{Z}. \]
5) \( X = \{1, \cdots, 6\}, \mathcal{G} \) is either the normalizer in \( \text{Aut}(X) \) of a partition \( X = \{a, b, c\} \cup \{u, v, w\} \), or a group \( \Omega.\text{Alt}(\{a, b, c\}).\text{Alt}(\{u, v, w\}) \), where \( \Omega \) has generators in i), or ii) or iii):
   i) \( (au)(bv)(cw) \)
   ii) \( (aubv)(cw) \)
   iii) \( (au)(bv)(cw), (ab)(uv) \).
6) \( X = \{1, \cdots, 6\}, \mathcal{G} \) is either the normalizer \( \mathcal{N} \) in \( \text{Aut}(X) \) of a partition \( X = \{a, a'\} \cup \{b, b'\} \cup \{c, c'\} \), or the subgroup of \( \mathcal{N} \) generated by \( (aa'), (bb'), (cc'), (abc)(a'b'c') \).
7) \( X = \mathbb{F}_8, \mathcal{G} \) consists of either all affine semi-linear transformations
   \[ A_{a,b,c} : x \mapsto ax^2 + b, \ x \in \mathbb{F}_8, \]
   \( a \in \mathbb{F}_8^\times, b \in \mathbb{F}_8, c \in \mathbb{Z}/3\mathbb{Z}, \text{ or only the affine linear transformations} \]
   \[ A_{a,b} : x \mapsto ax + b, \ x \in \mathbb{F}_8, \]
   \( a \in \mathbb{F}_8^\times, b \in \mathbb{F}_8. \)

**Lemma 6.7.** Let \( d \) be an integer \( \geq 1 \), \( X \) a set with \( 2d \) elements, \( \mathcal{G} \) a solvable subgroup of \( \text{Aut}(X) \) permuting transitively the subsets of \( X \) of cardinality \( d \). Then \( X, \mathcal{G} \) are
1) $X = \{1, 2\}$, $\mathcal{G} = \mathcal{S}_2$.

2) $X = \{1, 2, 3, 4\}$, $\mathcal{G} = \mathcal{S}_4$ or $\mathcal{A}_4$.

**Proof.** Let $o \in X$ be a point, $\mathcal{G}_o$ its stabilizer in $\mathcal{G}$. As usual, $\mathcal{G} = V\mathcal{G}_o$, $V$ normal in $\mathcal{G}$, simply transitive on $X$, isomorphic to a vector space over a prime field $F_p$, and is a faithful irreducible representation of $\mathcal{G}_o$. Write $f = \dim V$. Then $p^f = \text{Card}(V) = \text{Card}(X) = 2d$, so $p = 2$, $d = 2^{f-1}$.

Identify $V$ with $X$ through the bijection $v \mapsto v.o$. Every subset of $V$ of cardinality $d$ is some $gH$, $g \in \mathcal{G}$, where $H$ is a fixed hyperplane in $V$. So $f \leq 2$, for otherwise, neither $Y := \{v\} \cup H\setminus\{0\}$ nor its complement is a hyperplane, if a vector $v$ is chosen in the complement of $H$.

If $f = 1$, $X = \{1, 2\}$, on which $\mathcal{G}$ is transitive, so $\mathcal{G} = \mathcal{S}_2$.

If $f = 2$, as $\mathcal{G}_o$ is irreducible on $V$, it is not a 2-group, thus has order divisible by 3. Hence, $\mathcal{G} = \mathcal{S}_4$ or $\mathcal{A}_4$. Both do permute transitively the 2-point subsets of $X$. \hfill \Box

**Proposition 6.8.** Let $d$ be an integer $\geq 2$, $X$ a set with $2d$ elements, $\mathcal{G} \leq \{1, -1\} \times \text{Aut}(X)$ a solvable subgroup permuting transitively the subsets of $X$ of cardinality $d$, $\mathcal{G} \not\leq \text{Aut}(X)$. Here $-1$ sends any $Y$ of cardinality $d$ to $X \setminus Y$. Then $X, \mathcal{G}$ are

1) $X = \{o, a, b, c\}$, $\mathcal{G} = \{1, -1\} \mathcal{S}_4$, $\{1, -1\} \mathcal{A}_4$, $\{1, -1\} \text{Alt}(\{a, b, c\})$, $\{1, -1\} \mathcal{A}(\{a, b, c\})$.

2) $X = \{o\} \cup \mathcal{F}_5$, $\mathcal{G} = \{1, -1\} \times \mathcal{H}$, where $\mathcal{H}$ fixes $o$ and is the group of affine linear transformations of $\mathcal{F}_5$.

**Proof.** The subgroup $\mathcal{H} := \mathcal{G} \cap \text{Aut}(X)$ is of index 2 in $\mathcal{G}$. Let $Y$ be a subset of $X$ of cardinality $d$, $\mathcal{G}$ be its normalizer in $\mathcal{G}$. If $\mathcal{G} \not\leq \mathcal{H}$, $\mathcal{H}$ is transitive on $\mathcal{G}/\mathcal{H}$. If $\mathcal{G} \leq \mathcal{H}$, $\mathcal{H}/\mathcal{G} \leq \mathcal{G}/\mathcal{H}$ exhausts half among all subsets of $X$ of cardinality $d$; in particular, $\mathcal{H}$ has 2 orbits on $\mathcal{G}/\mathcal{H}$.

If $\mathcal{H}$ is transitive on $\mathcal{G}/\mathcal{H}$, then $\text{Card}(X) = 4$, $\mathcal{H} = \mathcal{S}_4$ or $\mathcal{A}_4$ (6.7). Accordingly, $\mathcal{G}$ is either $\{1, -1\} \mathcal{S}_4$ or a subgroup of $\{1, -1\} \mathcal{S}_4$ of index 2 containing $\mathcal{A}_4$, i.e. $\{1, -1\} \mathcal{A}_4$ or $\{1, -1(ab)\} \mathcal{A}_4$, for some $(ab)$.

If $\mathcal{H}$ permutes $\mathcal{G}/\mathcal{H}$ in 2 orbits of the same size, then by the proof of (6.6), either i) or ii) holds:

i) $X = \{o, 1, 2, 3\}$, $\mathcal{H} = \text{Aut}(\{1, 2, 3\})$ or $\mathcal{A}(\{1, 2, 3\})$.

ii) $X = \{o\} \cup \mathcal{F}_5$, $\mathcal{H}$ fixes $o$ and is the group of affine linear transformations of $\mathcal{F}_5$.

Let $\mathcal{N}$ be the normalizer of $\mathcal{H}$ in $\{1, -1\} \text{Aut}(X)$. Clearly, $\mathcal{G} \leq \mathcal{N}$.

In case i), both $\text{Aut}(\{1, 2, 3\})$ and $\mathcal{A}(\{1, 2, 3\})$ have normalizer equal to $\{1, -1\} \text{Aut}(X) = \mathcal{N}$. If $\mathcal{H} = \text{Aut}(\{1, 2, 3\})$, $\mathcal{G} = \mathcal{N}$.
If \( \mathcal{H} = \text{Aut}(\{1, 2, 3\}) \), \( (\mathfrak{N} : \mathfrak{G}) = 2 \), \( \mathfrak{G} = \{1, -1\} \text{Aut}(\{1, 2, 3\}) \) or \( \{1, -1.\text{(oa)}\} \text{Aut}(\{1, 2, 3\}) \), for some \( a \in \{1, 2, 3\} \).

In case ii), \( \mathfrak{N} = \{1, -1\} \times \mathcal{H} : \text{if } g \in \mathfrak{N} \cap \text{Aut}(X), \mathcal{H}g.o = g\mathcal{H}.o = g.o \).

So \( g.o = o \), and \( g \) preserves \( F_5 \). Let

\[
A : x \mapsto (g(1) - g(0))x + g(0), \quad x \in F_5
\]

Then \( h := g^{-1}A \) fixes \( o, 0, 1 \), normalizes \( \{T_b : x \mapsto x + b\} \), the unique 5-Sylow subgroup of \( \mathcal{H} \).

As \( hT_1h^{-1}(0) = 1 = T_1(0), hT_1h^{-1} = T_1 \), that is, \( h \) commutes with \( \{T_b\} \), therefore \( 1 \), for \( h(b) = hT_1b(0) = T_1b(0) = b, \forall b \in F_5 \). One finds that \( g = A \in \mathcal{H} \). Finally, \( \mathfrak{G} \) can only be \( \mathfrak{N} \).

\[ \Box \]

**Proposition 6.9.** Let \( S, \eta, s \) be as in \( \S 4 \). Any \( (2A_3, \alpha_2) \) over \( \eta \) is elliptic. If \( n > 5 \), \( (2A_n, \alpha_{2n+1}) \) is not elliptic.

**Proof.** That \( (2A_n, \alpha_{2n+1}) \), \( n \) odd > 5, is not elliptic follows immediately from (3.1), (8), and (6.8).

Given any \( (2A_3, \alpha_2) \) over \( \eta \), then with the notations of (6.8), (1), the group \( \{1, -1\} \text{Aut}(\{a, b, c\}) = \mathbb{Z}/6\mathbb{Z} \) is clearly realizable as a quotient of \( \pi_1(\eta, \overline{\eta}) \) lifting the given index of \( 2A_3 \), that is to say, \( (2A_3, \alpha_2) \) is elliptic over \( \eta \), (3.1), (8).

\[ \Box \]

**Proposition 6.10.** Let \( S, \eta, s \) be as in \( \S 4 \), \( \text{char}(s) = \ell \). If \( \ell = 5 \), any \( (2A_5, \alpha_3) \) over \( \eta \) is elliptic. When \( (\ell, 5) = 1 \), a pair \( (2A_5, \alpha_3) \) over \( \eta \) is elliptic if and only if \( 2A_5 \) ramified over \( S \), and \( \text{Card}(k(s)) \) mod 5 generates \( F_5^\times \).

**Proof.** By (3.1), (8), and (6.8), (2), a pair \( (2A_5, \alpha_3) \) over \( \eta \) is elliptic if and only if there is a surjection

\[
\rho = (\rho_1, \rho_2) : \pi_1(\eta, \overline{\eta}) \rightarrow \{1, -1\} \times \mathcal{H} = \mathfrak{G}
\]

with the index of \( 2A_5 \) being the first component. Here, \( \mathcal{H} \) denotes the group of affine linear transformations of \( F_5 \).

Note that \( \mathcal{H} \) is a quotient of \( \pi_1(\eta, \overline{\eta}) \) if and only if either \( \ell = 5 \) (4.1), or \( (\ell, 5) = 1 \), \( \text{Card}(k(s)) \) mod 5 generates \( F_5^\times \), (4.2), (2).

The index of \( 2A_5 \) corresponds, by Galois theory, to an \( \eta \)-scheme \( 2A'_5 \), connected, finite, étale over \( \eta \) of degree 2.

Suppose first \( 2A'_5 \) is unramified over \( S \).

If \( \rho = (\rho_1, \rho_2) \) exists, \( \rho_2 \) has to be totally ramified over \( S \), so \( \ell = 5 \). When \( \ell = 5 \), choosing a uniformizer \( \pi \in \Gamma(O_S) \), then

\[
2A'_5 \times_\eta \eta[z, x]/(z^4 - \pi, x^5 - x - z^{-1})
\]

is connected, Galois over \( \eta \) of group \( \mathfrak{G} \).
Next, suppose $2A'_5$ is ramified over $S$.

If $\ell = 5$, letting $\pi \in \Gamma(O_S)$ be a uniformizer, $\eta' \to \eta$ be connected, unramified over $S$ of degree 4, $S'$ the normalization of $S$ in $\eta$, $s' \in S'$ the closed point, $\zeta \in \text{Gal}(\eta'/\eta)$ a generator, and $u' \in \Gamma(O_{S'})^\times$ such that the images of $u'$, $\zeta(u')$, $\zeta^2(u')$, $\zeta^3(u')$ in $k(s')$ form a normal base over $k(s)$, then

$$2A'_5 \times_{\eta} \eta'[x_1, \cdots, x_4]/(x_1^5 - x_1 - \zeta(u')\pi^{-1}, \cdots, x_4^5 - x_4 - \zeta^4(u')\pi^{-1})$$

is connected, Galois over $\eta$ of group $G$.

If $(\ell, 5) = 1$, and $\text{Card}(k(s)) \mod 5$ generates $F_5^\times$, then $2A'_5 \times_{\eta} \eta'$ is connected, Galois over $\eta$ of group $G$, where $\eta' \to \eta$ is connected, tame along $s$, Galois, of group $H$, cf. (4.2), 2).

\[\square\]

7. **Type B**

Let $S, \eta, s$ be as in §4.

Let $n$ be an integer $\geq 3$, $e_1, \cdots, e_n$ the standard basis of $\mathbb{Z}^n$.

Write $\mathfrak{M}$ for the subgroup of $\text{GL}_n(\mathbb{Z})$ generated by the diagonal matrices $\mathfrak{D}$ and the monomial matrices $\mathfrak{M}$.

**Proposition 7.1.** If $\text{char}(s) = 2$, $(B_n, \alpha_n)$ is elliptic over $\eta$.

*Proof.* The group $\mathfrak{G}$, generated by $\mathfrak{D}$ and the rotation

$$\zeta : e_1 \mapsto e_2, \quad e_2 \mapsto e_3, \quad \cdots, \quad e_n \mapsto e_1,$$

acts transitively on the vectors

$$\pm e_1 \pm \cdots \pm e_n.$$

If $\text{char}(s) = 2$, $\mathfrak{G}$ is a quotient of $\pi_1(\eta, \overline{\eta})$ (4.1), whence, $(B_n, \alpha_n)$ is elliptic, (3.1), 2).

**Proposition 7.2.** The pair $(B_3, \alpha_3)$ is elliptic over $\eta$.

*Proof.* The elements of $\text{GL}_3(\mathbb{Z})$,

$$a : e_1 \mapsto e_1, \quad e_2 \mapsto e_3, \quad e_3 \mapsto -e_2$$

$$b : e_1 \mapsto -e_1, \quad e_2 \mapsto e_2, \quad e_3 \mapsto e_3$$

verify the identities

$$a^4 = b^2 = 1, \quad ab = ba.$$

The group with $a, b$ as generators,

$$\langle a, b \rangle \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

is a quotient of $\pi_1(\eta, \overline{\eta})$, and permutes the vectors

$$\pm e_1 \pm e_2 \pm e_3$$
Proposition 7.3. If $\text{char}(s) > 2$, $(B_4, \alpha_4)$ is elliptic over $\eta$.

Proof. The matrices in $\text{GL}_4(\mathbb{Z})$,

\begin{align*}
a : & e_1 \mapsto e_2, \ e_2 \mapsto -e_1, \ e_3 \mapsto e_3, \ e_4 \mapsto e_4 \\
b : & e_1 \mapsto e_1, \ e_2 \mapsto e_2, \ e_3 \mapsto e_4, \ e_4 \mapsto -e_3 \\
c : & e_1 \mapsto e_2, \ e_2 \mapsto e_3, \ e_3 \mapsto e_4, \ e_4 \mapsto -e_1 \\
d : & e_1 \mapsto e_3, \ e_2 \mapsto -e_4, \ e_3 \mapsto -e_1, \ e_4 \mapsto e_2
\end{align*}

are subject to the relations

\begin{align*}
a^4 = b^4 = 1, & \quad ab = ba, \ c^8 = d^4 = 1, \ cdc^{-1} = d^{-1}.
\end{align*}

The group $\langle a, b \rangle$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, and $\langle c, d \rangle$ is quaternion of order 16. Both are simply transitive on the vectors

\begin{align*}
\pm e_1 \pm e_2 \pm e_3 \pm e_4.
\end{align*}

If $\text{Card}(k(s)) \equiv 1 \pmod{4}$ (resp. $\text{Card}(k(s)) \equiv -1 \pmod{4}$), $\langle a, b \rangle$ (resp. $\langle c, d \rangle$) is a quotient of $\pi_1^t(\eta, \overline{\eta})$. Hence, $(B_4, \alpha_4)$ is elliptic over $\eta$, when $\text{char}(s)$ is odd, (3.1), 2). □

Proposition 7.4. If $\text{char}(s) > 2$, $(B_5, \alpha_5)$ is not elliptic over $\eta$.

Proof. Otherwise, there would exist a representation

\begin{align*}
\rho : \pi_1(\eta, \overline{\eta}) \to \mathfrak{W}
\end{align*}

whose image permuted the vectors

\begin{align*}
\pm e_1 \pm \cdots \pm e_5
\end{align*}

transitively. Changing the base $\eta$ to an extension, finite, étale, connected, of odd relative degree if necessary, one could arrange that $\mathfrak{G}$, the image of $\rho$, be a 2-group, in particular tame, with generators $\sigma, \tau$ satisfying

\begin{align*}
\sigma \tau \sigma^{-1} = \tau^q,
\end{align*}

where $q = \text{Card}(k(s))$. The order $\text{Card}(\mathfrak{G})$ is divisible by 32, and

\begin{align*}
\tau^8 = \sigma^8 = 1,
\end{align*}

for $\text{GL}_5(\mathbb{Z})$ contains no element of order 16. Certainly, $\tau$ has to be of order 8 or 4. Write $p(T)$ for the characteristic polynomial of $\tau$, and

\begin{align*}
X = \{e_1, \cdots, e_5, -e_1, \cdots, -e_5\}.
\end{align*}

If $\tau$ is of order 8, $p(T)$ equals $(T^4 + 1)(T - 1)$ or $(T^4 + 1)(T + 1)$. Some $v \in X$ is an eigenvector of $\tau$ of eigenvalue $\varepsilon = 1$ or $-1$. From

\begin{align*}
\tau^q \sigma(v) = \sigma \tau(v) = \varepsilon \sigma(v),
\end{align*}

simply transitively. Therefore, $(B_3, \alpha_3)$ is elliptic, (3.1), 2). □
it follows that $\sigma(v)$ is an eigenvector of $\tau^q$ in $X$, thus of $\tau$, of eigenvalue $\varepsilon$, so $\sigma(v) = v$ or $-v$, and $\sigma$ normalizes $X \setminus \{v, -v\}$. Since $q^2 \equiv 1 \mod 8, \forall q \equiv 1, 3, 5, 7 \mod 8$, one has

$$\sigma^2 \tau = \tau^q \sigma^2 = \tau \sigma^2,$$

that is, $\sigma^2$ commutes with $\tau$. Hence, there is an integer $d \in \{0, 2, 4, 6\}$ such that the equation $\sigma^2 = \tau^d$ holds, on $X \setminus \{v, -v\}$, as $X \setminus \{v, -v\}$ is acted simply transitively by $\langle \tau \rangle$, and clearly on $\{v, -v\}$ as well. So, $\sigma^2 = \tau^d$, and the order of $G = \langle \tau \rangle \cup \langle \sigma \rangle$ is $\leq 16$.

Next, suppose $\tau$ is of order 4. Then

$$\sigma \tau \sigma^{-1} = \tau^q = \tau \text{ or } \tau^{-1},$$

and $\sigma$ has to be of order 8.

If $p(T) = (T^2 + 1)(T - 1)$ or $(T^2 + 1)^2(T + 1)$, $\tau$ admits an eigenvector $v$ in $X$ of eigenvalue $\varepsilon = 1$ or $-1$. The identity

$$\tau^q \sigma(v) = \sigma \tau(v) = \varepsilon \sigma(v)$$

says that $\sigma(v)$ is an eigenvector of $\tau^q$, thus of $\tau$, of eigenvalue $\varepsilon$, therefore, $\sigma(v) = v$ or $-v$, and $\sigma$ normalizes $X \setminus \{v, -v\}$, which is acted simply transitively by $\langle \sigma \rangle$. Similarly argued as above, one deduces that $\tau^2 = \sigma^4$. But

$$\mathfrak{G} = \langle \sigma \rangle \cup \tau \langle \sigma \rangle \cup \tau^{-1} \langle \sigma \rangle$$

is of order $\leq 24$.

There remain the cases when $p(T) = (T^2 + 1)(T + 1)^{d}(T - 1)^{3-d}$, $d = 0, 1, 2, 3$. Let $u, v, w \in X$ be linear independent eigenvectors of $\tau$ of eigenvalues $1$ or $-1$. The set $\{u, v, w, -u, -v, -w\}$ is normalized by $\sigma$, as a consequence of the equality $\sigma \tau = \tau^q \sigma$. Now, $\sigma$ is of order $\leq 4$.

**Proposition 7.5.** If $\text{char}(s) > 2, n \geq 6$, then $(B_n, \alpha_n)$ is not elliptic over $\eta$.

**Proof.** Otherwise, there would exist a representation

$$\rho : \pi_1(\eta, \overline{\eta}) \to \mathfrak{W}$$

whose image permuted the vectors

$$\pm e_1 \pm \cdots \pm e_n$$
transitively. Changing the base \( \eta \) to a finite extension of odd relative degree if necessary, one could arrange that \( \mathfrak{G} \), the image of \( \rho \), be a 2-group, of order divisible by \( 2^n \).

Write \( \mathfrak{P} \) for the image of \( \mathfrak{G} \) in \( \mathfrak{S}_n = \mathfrak{W}/\mathfrak{D} \). Being a sub-quotient of \( \pi_1(\eta, \bar{\eta}) \), the elementary 2-group \( \mathfrak{D} \cap \mathfrak{G} \) is of order \( \leq 4 \), therefore, \( \mathfrak{P} \) is of order divisible by \( 2^{n-2} \).

Note that \( \text{ord}_2(n!) \leq n - 1 \); the equality holds if and only if \( n \) is a power of 2.

If \( n \) is not a power of 2, \( \mathfrak{P} \) is a 2-Sylow subgroup of \( \mathfrak{S}_n \), hence, \( \mathfrak{P} \) contains a subgroup \( \langle (aa'), (bb'), (cc') \rangle \). But \( \langle (aa'), (bb'), (cc') \rangle \) cannot be a sub-quotient of \( \pi_1(\eta, \bar{\eta}) \).

If \( n \) is a power of 2, thus \( n \geq 8 \), \( \mathfrak{P} \) is of index \( \leq 2 \) in a 2-Sylow subgroup of \( \mathfrak{S}_n \). Thus, a conjugate of \( \langle (12), (34), \cdots, (n-1, n) \rangle \), say \( \mathfrak{Q} \), satisfies \( \langle \mathfrak{Q} : \mathfrak{Q} \cap \mathfrak{P} \rangle \leq 2 \). But \( \mathfrak{Q} \cap \mathfrak{P} \), being an elementary 2-group of order \( \geq 8 \), cannot be a sub-quotient of \( \pi_1(\eta, \bar{\eta}) \) either. \[\Box\]

8. Type C

Let \( S, \eta, s \) be as in §4.

**Proposition 8.1.** For any integer \( n \geq 1 \), \( (C_n, \alpha_1) \) is elliptic over \( \eta \).

**Proof.** The subgroup \( \langle \tau \zeta \rangle \) of \( \text{GL}_n(\mathbb{Z}) \), where \( \zeta : e_1 \mapsto e_2, \cdots, e_n \mapsto e_1 \), and \( \tau : e_1 \mapsto -e_1, e_i \mapsto e_i, \forall i > 1 \), is simply transitive on the vectors \( e_1, \cdots, e_n, -e_1, \cdots, -e_n \).

Since \( \mathbb{Z}/2n\mathbb{Z} = \langle \tau \zeta \rangle \) is a quotient of \( \pi_1(\eta, \bar{\eta}) \), \( (C_n, \alpha_1) \) is elliptic over \( \eta \), (3.2), 3). \[\Box\]

9. Type D

Let \( S, \eta, s \) be as in §4.

Let \( n \) be an integer \( \geq 4 \), \( e_1, \cdots, e_n \) the standard basis of \( \mathbb{Z}^n \).

Write \( \mathfrak{W}_1 \) for the subgroup of \( \text{GL}_n(\mathbb{Z}) \) generated by the diagonal matrices \( \mathfrak{D}_1 \) of determinant 1 and the monomial matrices \( \mathfrak{M} \).

By conjugation, \( \mathfrak{W}_1 \) acts on \( \mathfrak{D}_1 \), \( \mathfrak{m} : \mathfrak{W}_1 \to \text{Aut}(\mathfrak{D}_1) \). This action gives rise to the canonical split exact sequence \[1 \to \mathfrak{D}_1 \to \mathfrak{W}_1 \xrightarrow{\mathfrak{m}} \mathfrak{M} \to 1.\]

**Lemma 9.1.** A group of monomial matrices is normalized by a diagonal matrix \( \delta \) if and only if it is centralized by \( \delta \).
Proof. Let such a group of monomial matrices be \( \mathfrak{H} \). For any \( h \in \mathfrak{H} \), the element \( \delta h \delta^{-1} h^{-1} \) is at the same time diagonal and monomial, so \( \delta h \delta^{-1} h^{-1} = 1 \), and \( \delta \) commutes with \( \mathfrak{H} \).

**Lemma 9.2.** Any subgroup \( \mathfrak{H} \) of \( W_1 \) of odd order is conjugate to \( m(\mathfrak{H}) \) by an element of \( D_1 \).

Proof. Write any element of \( \mathfrak{H} \) as

\[
h = \delta(h)m(h), \quad \delta(h) \in D_1, \quad m(h) \in M.
\]

The function \( h \mapsto \delta(h) \) is a cocycle of \( \mathfrak{H} \) with values in \( D_1 \):

\[
\delta(gh) = \delta(g)m(g)\delta(h)m(g)^{-1}, \quad \forall \ g, h \in \mathfrak{H}
\]

therefore, as \( H^1(\mathfrak{H}, D_1) = 0 \), is a coboundary:

\[
\exists \delta \in D_1, \forall h \in \mathfrak{H}, \quad \delta(h) = \delta m(h)\delta^{-1} m(h)^{-1}.
\]

For any \( h \in \mathfrak{H} \), one has

\[
h = \delta(h)m(h) = \delta m(h)\delta^{-1} m(h)^{-1} m(h) = \delta m(h)\delta^{-1},
\]

and

\[
\mathfrak{H} = \delta m(\mathfrak{H})\delta^{-1}.
\]

□

**Proposition 9.3.** If \( n \) is even, \( (D_n, \alpha_1) \) is elliptic over \( \eta \). If \( \text{char}(s) = 2 \), \( (D_n, \alpha_1), (D_n, \alpha_{n-1}), (D_n, \alpha_n) \) are elliptic over \( \eta \). The pairs \( (D_4, \alpha_3), (D_4, \alpha_4) \) are elliptic over \( \eta \).

Proof. Let \( \zeta : e_1 \mapsto e_2, e_2 \mapsto e_3, \ldots, e_n \mapsto e_1 \).

If \( n \) is even, \(-1\) has determinant \( 1 \), the subgroup of \( W_1 \),

\[
\langle -1, \zeta \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},
\]

is a quotient of \( \pi_1(\eta, \overline{\eta}) \), and permutes the vectors

\[
e_1, \ldots, e_n, -e_1, \ldots, -e_n
\]

simply transitively. So, for \( n \) even, \( (D_n, \alpha_1) \) is elliptic over \( \eta \), (3.1), 4).

In particular, \( (D_4, \alpha_1) \), thus \( (D_4, \alpha_i) \), \( i = 3, 4 \), are elliptic.

The group \( D_1(\zeta) \) is transitive on

\[
\{e_1, \ldots, e_n, -e_1, \ldots, -e_n\},
\]

on

\[
\{s_1e_1 + \cdots + s_ne_n, \ s_i \in \{1, -1\}, \ s_1 \cdots s_n = -1\},
\]

and on

\[
\{s_1e_1 + \cdots + s_ne_n, \ s_i \in \{1, -1\}, \ s_1 \cdots s_n = 1\}.
\]

If \( \text{char}(s) = 2 \), \( D_1(\zeta) \) is a quotient of \( \pi_1(\eta, \overline{\eta}) \) :
Let \( \eta' \to \eta \) be connected, unramified over \( S \) of degree \( n \), let \( S' \) be the normalization of \( S \) in \( \eta \), \( s' \in S' \) the closed point, \( \pi \in \Gamma(\mathcal{O}_S) \) a uniformizer, \( \zeta \in \operatorname{Gal}(\eta'/\eta) \) a generator, and \( u' \in \Gamma(\mathcal{O}_{S'})^\times \) such that the images of \( u', \zeta(u'), \ldots, \zeta^{n-1}(u') \) in \( k(s') \) are a normal basis over \( k(s) \). Put \( b' := 1 + u'\pi \). Then

\[
\eta'[z_1, \ldots, z_n]/(z_1^2 - \frac{\zeta(b')}{b'}, \ldots, z_{n-1}^2 - \frac{\zeta^{n-1}(b')}{\zeta^{-2}(b')}, z_n^2 - \frac{b'}{\zeta^{-1}(b')}, 1-z_1 \cdots z_n)
\]

is Galois over \( \eta \) of group \( \mathcal{D}_1(\zeta) \). Hence, if \( \operatorname{char}(s) = 2 \), \((D_n, \alpha_1), (D_n, \alpha_{n-1}), (D_n, \alpha_n) \) are elliptic over \( \eta \), (3.1), 4), 5). \( \square \)

**Proposition 9.4.** Suppose \( \operatorname{char}(s) > 2 \). For any odd integer \( n \geq 5 \), \((D_n, \alpha_1)\) is not elliptic over \( \eta \).

**Proof.** It suffices to show that for any odd integer \( n \geq 5 \) and for \( n = 3 \), no representation of \( \pi_1(\eta, \mathcal{P}) \) in \( \mathcal{M}_1 \) has image acting transitively on

\[ X = \{e_1, \ldots, e_n, -e_1, \ldots, -e_n\} \]

Assume the contrary holds, and \( n \) be the smallest odd integer \( \geq 3 \) so that such a representation \( \rho : \pi_1(\eta, \mathcal{P}) \to \mathcal{M}_1 \) exists with image \( \mathcal{S} \).

Let \( X^+ = \{e_1, \ldots, e_n\} \). Let \( \mathcal{A} \) be the inertial subgroup of \( \mathcal{S} \), \( \mathcal{P} \) the wild inertia subgroup.

Write \( \mathcal{A} = \mathcal{S} \langle \tau \rangle \) as a semi-direct product, where \( \tau \) is of order a power of 2, and \( \mathcal{S} \) is of odd order, characteristic in \( \mathcal{A} \), containing \( \mathcal{P} \) as a subgroup.

Let \( \mathcal{Q} \) be a 2-Sylow subgroup of \( \mathcal{S} \) containing \( \tau \). Let \( \mathcal{H} \) a Hall subgroup containing \( \mathcal{S} \), of order equal to \( \operatorname{Card}(\mathcal{S}/\mathcal{Q}) \).

For certain \( \delta \in \mathcal{D}_1 \), \( \delta \mathcal{H} \delta^{-1} \) is monomial (9.2). Changing \( \rho \) to \( \int(\delta) \circ \rho \), one could arrange that \( \mathcal{H} \) be monomial. Then \( \mathcal{H} \), a priori \( \mathcal{S} \), normalizes \( X^+ \). Let the \( \mathcal{S} \)-orbits in \( X^+ \) be denoted by \( O_1, \ldots, O_d \); these orbits all have the same cardinality \( c \), since \( \mathcal{S} \) is normal in \( \mathcal{G} \).

Hence, \( n = dc \). Both \( d \) and \( c \) are odd.

Write any \( g \in \mathcal{S} \) as \( g = \delta(g) \mathcal{m}(g) \in \mathcal{S} \), \( \delta(g) \in \mathcal{D}_1 \), \( \mathcal{m}(g) \in \mathcal{M} \).

Show that \( \delta(g) \) is constant on each \( O_j \), \( j = 1, \ldots, d \) : the equality \( g \mathcal{S} g^{-1} = \mathcal{S} \) implies that \( \delta(g) \mathcal{S} \delta(g)^{-1} = \delta(g)^{-1} \mathcal{S} \delta(g) = \mathcal{m}(g) \mathcal{S} \mathcal{m}(g)^{-1} \).

In particular, \( \delta(g) \mathcal{S} \delta(g)^{-1} \) is monomial. Consequently, \( \forall o \in O_j, \forall z \in \mathcal{S} \), and \( o' := z.o \), one has \( \delta(g) o' = \delta(g) z.o = \delta(g) z \delta(g)^{-1}. \delta(g) o = \delta(g) o \), because \( \delta(g) z \delta(g)^{-1} \) is monomial.

It follows that \( \delta(g) \mathcal{S} \delta(g)^{-1} = \mathcal{m}(g) \mathcal{S} \mathcal{m}(g)^{-1} = \mathcal{S} \), and that \( \mathcal{m}(g) \) permutes the orbits \( O_j \), \( j = 1, \ldots, d \).
Considering \(O_1, \cdots, O_d\) as the standard base of \(\mathbb{Z}^d\), the image of \(\mathfrak{g}\) in \(\text{GL}_d(\mathbb{Z})\) lies in the group generated by the diagonal matrices of determinant 1 and monomial matrices.

Thus, by our choice of \(n, d\) must be 1 or \(n\).

If \(d = 1\), \(\mathfrak{g}\) is transitive on \(X^+\). For any \(g \in \mathfrak{g}\), either \(g\) or \(-g\) is monomial. As \(-1 \notin \mathfrak{W}_1\), \(\mathfrak{g}\) is monomial, in particular, has \(> 1\) orbits on \(X\).

If \(d = n\), then \(\mathfrak{g} = 1\), \(\mathfrak{g}\) is tame, \(\mathfrak{R} = \langle \tau \rangle\), \(\mathfrak{H}\) is normal in \(\mathfrak{g}\). Say, on \(X\), \(\tau\) has orbits \(X_1, \cdots, X_r\); these orbits all have the same cardinality \(e\), a power of 2, as \(\langle \tau \rangle\) is a normal 2-subgroup of \(\mathfrak{g}\). One deduces that \(2n = re\). Either \(r = 2n\), \(e = 1\), or \(r = n\), \(e = 2\). Accordingly, either \(\tau = 1\), \(\mathfrak{g}\) is cyclic, or \(\tau^2 = 1\), \(\tau\) is central in \(\mathfrak{g}\), thus \(= 1\) or \(-1\), i.e. \(\mathfrak{g}\) is tame, either \(\tau\) does not belong to \(\mathfrak{W}_1\). So, \(\tau = 1\), \(\mathfrak{g}\) is cyclic of order \(2n\). If \(\sigma\) is a generator of \(\mathfrak{g}\), \(\mathfrak{G} = \langle \sigma^n \rangle\), and \(\mathfrak{H} = \langle \sigma^2 \rangle\) is simply transitive on \(X^+\). The involution \(\sigma^n\), commuting with \(\sigma^2\), is a scalar matrix, i.e. \(\equiv -1\). But \(-1 \notin \mathfrak{W}_1\). □

**Proposition 9.5.** For an integer \(n \geq 4\), if \((B_{n-1}, \alpha_{n-1})\) is elliptic over \(\eta\), so are \((D_n, \alpha_{n-1})\), \((D_n, \alpha_n)\).

**Proof.** This is clear, by comparing (3.1), 2) with (3.1), 5). □

**Proposition 9.6.** The pairs \((D_5, \alpha_4)\), \((D_5, \alpha_5)\) are elliptic over \(\eta\).

**Proof.** Because \((B_4, \alpha_4)\) is elliptic, (7.1), (7.3), (9.5). □

**Proposition 9.7.** Suppose \(\text{char}(s) > 2\). Then \((D_6, \alpha_5)\), \((D_6, \alpha_6)\) are elliptic over \(\eta\) if and only if \(\text{Card}(k(s)) \equiv 5 \text{ mod } 8\).

**Proof.** It needs consider \((D_6, \alpha_6)\) only, the case of \((D_6, \alpha_5)\) being the same. Let \(\ell = \text{char}(s)\). The condition \(\text{Card}(k(s)) \equiv 5 \text{ mod } 8\) says equivalently that \(\ell \equiv 5 \text{ mod } 8\), \([s:F_\ell]\) is odd.

If \(\text{Card}(k(s)) \equiv 5 \text{ mod } 8\), \((D_6, \alpha_6)\) is elliptic : the matrices in \(\mathfrak{W}_1\),

\[
\tau : e_1 \mapsto e_2, \quad e_2 \mapsto e_3, \quad e_3 \mapsto e_4, \quad e_4 \mapsto -e_1, \quad e_5 \mapsto e_6, \quad e_6 \mapsto -e_5
\]
\[
\sigma : e_1 \mapsto e_2, \quad e_2 \mapsto -e_3, \quad e_3 \mapsto e_4, \quad e_4 \mapsto e_1, \quad e_5 \mapsto e_6, \quad e_6 \mapsto -e_6
\]

verify the identities

\[
\tau^8 = \sigma^8 = 1, \quad \sigma \tau \sigma^{-1} = \tau^5.
\]

The group with \(\sigma, \tau\) as generators acts simply transitively on

\[
\mathfrak{X} = \{s_1e_1 + \cdots + s_6e_6, s_i = 1, -1, s_1 \cdots s_6 = 1\},
\]

and when \(\text{Card}(k(s)) \equiv 5 \text{ mod } 8\), is also a quotient of \(\pi^1(\eta, \overline{\eta})\), whence \((D_6, \alpha_6)\) is elliptic, (3.1), 5).
Next, suppose \((D_6, \alpha_6)\) elliptic, \(\rho : \pi_1(\eta, \mathcal{F}) \to \mathfrak{M}_1\) is a representation with image acting transitively on \(X\). To show that \(\ell \equiv 5 \mod 8\) and that \([s : \mathcal{F}_\ell]\) is odd, one may change the base \(\eta\) to an extension of odd relative degree and further suppose that \(\mathfrak{G}\), the image of \(\rho\), is a 2-group, in particular tame, with generators \(\sigma, \tau\) satisfying
\[
\sigma \tau \sigma^{-1} = \tau^q,
\]
where \(q = \text{Card}(k(s))\). The order \(\text{Card}(\mathfrak{G})\) is divisible by 32, and
\[
\tau^8 = \sigma^8 = 1,
\]
since \(\text{GL}_6(\mathbb{Z})\) contains no elements of order 16. Let
\[
X^+ = \{e_1, \cdots, e_6\}, \quad X = \{e_1, \cdots, e_6, -e_1, \cdots, -e_6\}.
\]
Write \(p(T)\) for the characteristic polynomial of \(\tau\).
As \(\tau \in \mathfrak{M}_1\), \(p(T)\) may be
\[
(T^4+1)(T^2 \pm 1), \quad (T^2+1)^2(T^2 \pm 1)^2, \quad (T^2+1)(T-1)^d(T+1)^{4-d}, \quad d = 1, 3.
\]
Show \(p(T) \neq (T^4+1)(T^2 - 1)\):
Otherwise, say \(u, v \in X^+\) satisfy \(\tau(u) = u, \tau(v) = -v\). Then,
\[
\tau^q \sigma(u) = \sigma \tau(u) = \sigma(u),
\]
that is, \(\sigma(u)\) is an eigenvector of \(\tau^q\), thus of \(\tau\), of eigenvalue 1, therefore, \(\sigma(u) = u,\) or \(-u\). Similarly, \(\sigma(v) = v,\) or \(-v\). On \(X \setminus \{u, v, -u, -v\}\), \(\sigma^2\), commuting with \(\tau\), equals a power of \(\tau\): \(\sigma^2 = \tau^a\), where \(a = 2, 6\) (resp. \(a = 4\)), if \(\sigma\) is of order 8 (resp. 4). For any \(a = 2, 4, 6\), the relation \(\sigma^2 = \tau^a\) holds on \(\{u, v, -u, -v\}\). So \(\sigma^2 = \tau^a\), some \(a \in \{2, 4, 6\}\), and
\[
\mathfrak{G} = \langle \tau \rangle \cup \langle \tau \rangle \sigma
\]
is of order \(\leq 16\).
Show \(p(T) \neq (T^2+1)(T-1)^d(T+1)^{4-d}, \quad d = 1, 3\):
Otherwise, let \(x, u, v, w \in X^+\) be linearly independent eigenvectors of \(\tau\) of eigenvalues 1 or \(-1\). For any \(z\) in \(Z^+ := \{x, u, v, w\}\) of eigenvalue \(\varepsilon\), one has \(\tau^q \sigma(z) = \sigma \tau(z) = \varepsilon. \sigma(z)\), so \(\sigma(z) \in Z^+ \cup -Z^+\), \(\sigma\) is of order \(\leq 4\), and \(\mathfrak{G}\) is of order \(\leq 16\).
Show \(p(T) \neq (T^2+1)^2(T \pm 1)^2\):
Otherwise, write \(X^+ = \{a, b\} \cup \{c, d\} \cup \{u, v\}\) in such a way that \(\tau\) normalizes separately \(\{a, b, -a, b\}\) and \(\{c, d, -c, -d\}\), and admits \(u, v\) as eigenvectors of eigenvalues \(\varepsilon \in \{1, -1\}\). In particular, \(\tau\) is of order \(\leq 4\), \(\sigma\) has to be of order 8, and \(\sigma \tau^2 = \tau^2 \sigma\). From the identity \(\sigma \tau = \tau^q \sigma\), one deduces that \(\sigma\) normalizes separately \(Z = \{u, v, -u, -v\}\) and
\( Y = \{a, b, c, d, -a, -b, -c, -d\} \). The relation \( \tau^2 = \sigma^4 \) holds on \( Y \), \( Y \) being a \( \langle \sigma \rangle \)-torsor, and evidently on \( Z \) as well. So \( \tau^2 = \sigma^4 \), and 
\[
\mathfrak{G} = \langle \sigma \rangle \cup \tau \langle \sigma \rangle \cup \tau^{-1} \langle \sigma \rangle
\]
is of order \( \leq 24 \).

It can only be that \( p(T) = (T^4 + 1)(T^2 + 1) \).

Write \( X^+ = Y^+ \cup Z^+ \), where \( Y^+ = \{a, b, c, d\} \) (resp. \( Z^+ = \{u, v\} \)) has cardinality 4 (resp. 2), and \( \tau \) normalizes separately \( Y = Y^+ \cup -Y^+ \) and \( Z = Z^+ \cup -Z^+ \). Both \( Y \) and \( Z \) are \( \mathfrak{G} \)-sets, as easily seen using \( \sigma \tau = \tau^0 \sigma \).

Show \( q \equiv 5 \mod 8 \):

If \( q \equiv 1 \mod 8 \), \( \sigma \tau = \tau^q \sigma = \tau \sigma \). So on \( Y \), for certain \( r \in \mathbb{Z}/8\mathbb{Z}, \sigma = \tau^r \). But then \( \mathfrak{G} \) has two orbits on \( \{\pm a \pm b \pm c \pm d\} \), thus has at least two orbits on \( \mathbb{X} \).

If \( q \equiv 7 \mod 8 \), \( \sigma \tau = \tau^{-1} \sigma \). On \( Y \), \( \sigma^2 = 1 \). And, \( \mathfrak{G} \) has two orbits on \( \{\pm a \pm b \pm c \pm d\} \), so at least two orbits on \( \mathbb{X} \).

If \( q \equiv 3 \mod 8 \), \( \sigma \) is of order \( \leq 4 \). On \( Y \), \( \sigma^2 = \tau^4 \). The characteristic polynomial of \( \sigma \) equals \((T^2 + 1)^2(T - 1)^2\) or \((T^2 + 1)^2(T + 1)^2\). In either case, the relation \( \sigma^2 = \tau^4 \) holds also on \( Z \). Thus, \( \sigma^2 = \tau^4 \), and \( \mathfrak{G} = \langle \tau \rangle \cup \langle \tau \rangle \sigma \) is of order \( \leq 16 \). \( \square \)

**Proposition 9.8.** If \( \text{char}(s) > 2 \), \((D_7, \alpha_6), (D_7, \alpha_7)\) are not elliptic over \( \eta \).

*Proof.* Otherwise, there would exist a representation \( \rho : \pi_1(\eta, \eta) \to \mathfrak{M}_1 \) whose image \( \mathfrak{G} \) permuted transitively the vectors 
\[
s_1e_1 + \cdots + s_7e_7, \text{ where } s_i \in \{1, -1\}, \ s_1 \cdots s_7 = 1.
\]

The quotient \( \mathfrak{G}/\mathfrak{D}_1 \cap \mathfrak{G} \) is of order divisible by 16, for \( \mathfrak{D}_1 \cap \mathfrak{G} \), being at the same time an elementary 2-group and a sub-quotient of \( \pi_1(\eta, \eta) \), is of order \( \leq 4 \). Consequently, \( \mathfrak{G}/\mathfrak{D}_1 \cap \mathfrak{G} \) contains a 2-Sylow subgroup of \( \mathfrak{M} = \mathfrak{G}_7 \), thus contains a subgroup \( \langle (aa'), (bb'), (cc') \rangle \). But \( \langle (aa'), (bb'), (cc') \rangle \) cannot be a sub-quotient of \( \pi_1(\eta, \eta) \). \( \square \)

**Proposition 9.9.** If \( \text{char}(s) > 2 \), \((D_8, \alpha_7), (D_8, \alpha_8)\) are not elliptic over \( \eta \).

*Proof.* It suffices to show that \((D_8, \alpha_8)\) is not elliptic, the case of \((D_8, \alpha_7)\) being similar.

Assume the contrary holds, and \( \rho : \pi_1(\eta, \eta) \to \mathfrak{M}_1 \) be a representation having image \( \mathfrak{G} \) acting transitively on 
\[
\{s_1e_1 + \cdots + s_7e_7, \ s_i = 1, -1, \ s_1 \cdots s_7 = 1\}.
\]
Extending the base $\eta$ to a finite extension of odd relative degree if necessary, one could arrange that $G$ be a 2-group, in particular, tame, with generators $\sigma, \tau$ satisfying $\sigma \tau \sigma^{-1} = \tau^q$, $q = \text{Card}(k(s))$.

Necessarily, $\tau^8 = \sigma^8 = 1$, as no element of $\text{GL}_8(\mathbb{Z})$ of order 16 belongs to $\mathfrak{W}_1$. But then, $G$ is of order $\leq 64 < 2^7$. \[\square\]

**Proposition 9.10.** If $\text{char}(s) > 2$, $n \geq 9$, then $(D_n, \alpha_n-1)$, $(D_n, \alpha_n)$ are not elliptic over $\eta$.

**Proof.** It needs consider only $(D_n, \alpha_n)$, which we assume is elliptic over $\eta$. Let $\rho : \pi_1(\eta, \eta) \rightarrow \mathfrak{W}_1$ be a representation with image $G$ acting transitively on the set

$$\{s_1 e_1 + \cdots + s_n e_n, \ s_i = 1, -1, \ s_1 \cdots s_n = 1\}.$$ 

Base changing $\eta$ to an extension of odd relative degree if necessary, one may further assume that $G$ be a 2-group, of order divisible by $2n-1$.

Then $\mathfrak{P} = G/D_1 \cap G$ is of order divisible by $2^{n-3}$, for the elementary 2-group $D_1 \cap G$, being a sub-quotient of $\pi_1(\eta, \eta)$, is of order $\leq 4$.

Note that $\text{ord}_2(n!) \leq n - 1$, and that the equality holds if and only if $n$ is a power of 2.

If $n$ is not a power of 2, $\mathfrak{P}$ is of index $\leq 2$ in a 2-Sylow subgroup of $\mathfrak{M} = \mathfrak{G}_n$, therefore a group $\mathfrak{Q} = \langle (aa'), (bb'), (cc'), (dd') \rangle$ satisfies $(\mathfrak{Q} : \mathfrak{Q} \cap \mathfrak{P}) \leq 2$. But $\mathfrak{Q} \cap \mathfrak{P}$, being an elementary 2-group of order $\geq 8$, cannot be a sub-quotient of $\pi_1(\eta, \eta)$.

If $n$ is a power of 2, thus $n \geq 16$, $\mathfrak{P}$ is of index $\leq 4$ in a 2-Sylow subgroup of $\mathfrak{G}_n$, so a conjugate of $(12), (34), \cdots, (n-1, n)$, say $\mathfrak{Q}$, satisfies $(\mathfrak{Q} : \mathfrak{Q} \cap \mathfrak{P}) \leq 4$. But $\mathfrak{Q} \cap \mathfrak{P}$ cannot be a sub-quotient of $\pi_1(\eta, \eta)$ either. \[\square\]

10. Type $^2D$

Let $S, \eta, s$ be as in $\S 4$.

Let $n$ be an integer $\geq 4$. Write $n = 2^g r$, where $g \geq 0$, $r$ is odd. Identify $\mathbb{Z}^n$ with $\mathbb{Z}^{2g} \otimes \mathbb{Z}^r$, the base $e_1, \cdots, e_n$ with $e_1' \otimes e_1'', \cdots, e_{2g} \otimes e_r''$, where $e_1', \cdots, e_1''$ (resp. $e_{2g}', \cdots, e_r''$) are the standard base of $\mathbb{Z}^{2g}$ (resp. $\mathbb{Z}^r$).

The subgroup of $\text{GL}_n(\mathbb{Z})$ generated by the diagonal matrices and monomial matrices is denoted by $\mathfrak{W}$. The subgroup of $\mathfrak{W}$ generated by the diagonal matrices of determinant 1 and monomial matrices is denoted by $\mathfrak{W}_1$. 
Proposition 10.1. A pair \((^2D_n, \alpha_1)\), with \(^2D_n\) unramified over \(S\), is elliptic over \(\eta\).

Proof. The cyclic subgroup \(\langle \sigma \rangle\) of \(\mathcal{W}\), where
\[
\sigma : e_1 \mapsto e_2, \ldots, e_{n-1} \mapsto e_n, e_n \mapsto -e_1,
\]
permutes the vectors
\[
e_1, \ldots, e_n, -e_1, \ldots, -e_n
\]
simply transitively, and realizable as a quotient of \(\pi_1(\eta, \overline{\eta})\) unramified over \(S\). Hence, \((^2D_n, \alpha_1)\) is elliptic, (3.1), 9).

Proposition 10.2. If \(\text{char}(s) > 2\), any \((^2D_n, \alpha_1)\), with \(^2D_n\) ramified over \(S\), is elliptic.

Proof. Let \(q = \text{Card}(k(s))\).

Define \(\tau', \sigma' \in \text{GL}_{2^g}(\mathbb{Z})\) by
\[
\tau' : e_1' \mapsto e_2', \ldots, e_{2g-1}' \mapsto e_{2g}', e_{2g}' \mapsto -e_1', \\
\sigma' \tau' = \tau'^q \sigma', \quad \sigma' : e_1' \mapsto e_1'.
\]

Let \(\tau \in \text{GL}_n(\mathbb{Z})\) be such that
\[
\tau : e_i' \otimes e_j'' \mapsto \tau'^{q-1} (e_i') \otimes e_j'',
\]
for any \(j = 1, \ldots, r\), any \(i = 1, \ldots, 2^g\).

Let \(\sigma \in \text{GL}_n(\mathbb{Z})\) be such that
\[
\sigma : e_i' \otimes e_1'' \mapsto e_i' \otimes e_2'', \ldots, e_i' \otimes e_{r-1}'' \mapsto e_i' \otimes e_r'', e_i' \otimes e_r'' \mapsto \sigma'(e_i') \otimes e_1'',
\]
for any \(i = 1, \ldots, 2^g\).

Clearly, \(\tau\) is of order \(2^{g+1}\), \(\sigma^r = \sigma' \otimes 1\), \(\sigma \tau \sigma^{-1} = \tau^q\).

The group \(\langle \sigma, \tau \rangle\) is transitive on
\[
\{e_1, \ldots, e_n, -e_1, \ldots, -e_n\},
\]
and realizable as a quotient of \(\pi_1(\eta, \overline{\eta})\) lifting the tamely ramified index of \(^2D_n\). So \((^2D_n, \alpha_1)\) is elliptic, (3.1), 9). \(\square\)

Let \(d \geq 1, f > 1\) be integers. Define pro-2-groups
\[
F_1 = \langle x_1, \ldots, x_d, x_{d+2} | x_1^{2^f} [x_1, x_2][x_3, x_4] \cdots [x_{d+1}, x_{d+2}] = 1, \text{ d even} \rangle,
\]
\[
F_2 = \langle x_1, \ldots, x_{d+2} | x_1^{2} [x_2, x_3] \cdots [x_{d+1}, x_{d+2}] = 1, \text{ d odd} \rangle,
\]
\[
F_3 = \langle x_1, \ldots, x_{d+2} | x_1^{2+2^f} [x_1, x_2][x_3, x_4] \cdots [x_{d+1}, x_{d+2}] = 1, \text{ d even} \rangle,
\]
\[
F_4 = \langle x_1, \ldots, x_{d+2} | x_1^2 [x_1, x_2]x_2^{2^f} [x_3, x_4] \cdots [x_{d+1}, x_{d+2}] = 1, \text{ d even} \rangle,
\]
where
\[
[x, y] := x^{-1}y^{-1}xy
\]
is the commutator.

If \( \text{char}(s) = 2 \), recall that for \( d = [\eta : Q_2] \) and some integer \( f \), \( \pi_1(\eta, \eta) \) has one of the groups \( F_1, F_2, F_3, F_4 \) as the maximal pro-2 quotient, cf. [2], p. 107-108.

**Proposition 10.3.** If \( \text{char}(s) = 2 \), any \( (2D_n, \alpha_1) \) is elliptic over \( \eta \).

*Proof.* Define \( a', b' \in \text{GL}_{29}(Z) \) by

\[
a': e'_1 \mapsto -e'_1, \quad e'_i \mapsto e'_i, \quad \forall \ i > 1, \\
b': e'_1 \mapsto e'_2, \quad \cdots, \quad e'_{29-1} \mapsto e'_{29}, \quad e'_{29} \mapsto e'_1,
\]

and \( c'' \in \text{GL}_r(Z) \) by

\[
c'': e''_1 \mapsto e''_r, \quad \cdots, \quad e''_{r-1} \mapsto e''_r, \quad e''_r \mapsto e''_{r-1}.
\]

Let \( a := a' \otimes 1, b := b' \otimes 1, c := 1 \otimes c'' \in \text{GL}_n(Z) \).

The group \( (ab) \times \langle c \rangle \) is simply transitive on the vectors

\[
e_1, \cdots, e_n, -e_1, \cdots, -e_n.
\]

To prove the proposition, it suffices to show that either \( (ab) \times \langle c \rangle \) or \( (a, b) \times \langle c \rangle \) is a quotient of \( \pi_1(\eta, \eta) \) lifting the given index of \( 2D_n \), (3.1), 9). Note that \( a \) (resp. \( b \)) has image \(-1\) (resp. \( 1 \)) under the homomorphism

\[MM \to MM/\mathfrak{M}_1 = \{1, -1\}.\]

Let \( F \) be the maximal pro-2-quotient of \( \pi_1(\eta, \eta) \). The index of \( 2D_n \) factors as a composition

\[\pi_1(\eta, \eta) \to F \xrightarrow{\chi} \{1, -1\}.
\]

As \( \langle c \rangle \) is of odd order and realizable as a quotient of \( \pi_1(\eta, \eta) \) unramified over \( S \), it even suffices to show that the surjection \( \chi : F \to \{1, -1\} \) lifts to a homomorphism \( \rho : F \to \langle a, b \rangle \) with image \( \langle ab \rangle \) or \( \langle a, b \rangle \). The verification is straightforward from the structure of \( F \). For instance, consider \( g \geq 2 \), and \( F = \langle x, y, z | x^2y^4[y, z] = 1 \rangle \). According to the values of \( (x, y, z) \) in \( \{1, -1\} \), choose \( \rho : F \to \langle a, b \rangle \) as follows:

1) \((-1, 1, 1)\), let \( \rho : (x, y, z) \mapsto (a, 1, b) \).

2) \((1, -1, 1)\), let \( \rho : (x, y, z) \mapsto ((ab)^{-1}, ab, 1) \).

3) \((1, 1, -1)\), let \( \rho : (x, y, z) \mapsto (1, 1, ab) \).

4) \((-1, 1, -1)\), let \( \rho : (x, y, z) \mapsto (a, 1, ab) \).

5) \((1, -1, -1)\), let \( \rho : (x, y, z) \mapsto ((ab)^{-1}, ab, ab) \).

6) \((-1, -1, 1)\), let \( \rho : (x, y, z) \mapsto (a, ab, ab^2ab^{-2}) \), if \( g = 2 \), and \( \rho : (x, y, z) \mapsto (ab^2, ab^{-1}, ab^3ab^{-3}) \), if \( g > 2 \).

7) \((-1, -1, -1)\), let \( \rho : (x, y, z) \mapsto (ab^2, ab, ab^{-1}) \), if \( g = 2 \), and \( \rho : (x, y, z) \mapsto (b^{-1}ab^2aba, ab^{-1}, ab) \), if \( g > 2 \). \( \square \)
11. **Type $E_6$**

Let $E$ be a 6-dimensional $\mathbf{F}_2$-vector space of base $e_i, f_j$, $1 \leq i, j \leq 3$, let $V_i = \mathbf{F}_2 e_i + \mathbf{F}_2 f_i$, $i = 1, 2, 3$, and let $q$ be the quadratic form on $E$ such that

$$q(e_i) = q(f_j) = 1, \quad q(e_i + e_j) = q(f_i + f_j) = 0, \quad q(e_i + f_j) = \delta_{ij},$$

where $\delta_{ij} = 1$, if $i = j$, and $0$, if $i \neq j$, $\forall \ i, j = 1, 2, 3$.

Write $O(q)$ for the orthogonal group of $q$; it is of order $2^7 3^4 5$. Write $X$ for the set of non-zero singular vectors in $E$,

$$X = \{ v \in E \setminus \{0\}, \ q(v) = 0 \},$$

which consists of 27 elements of the form $v_i + v_j$, where $v_i \in V_i, v_j \in V_j, 1 \leq i, j \leq 3, i \neq j, v_i, v_j$ non-zero.

In view of (3.1), (6), we need to enumerate up to conjugation the solvable subgroups of $O(q)$ that are transitive on $X$.

For instance, every 3-Sylow subgroup of $O(q)$ is transitive on $X$.

Note that each $V_i, i = 1, 2, 3$, is an elliptic plane. Thus, $O(q|V_i) = \text{GL}(V_i)$ is generated by $\gamma_i, \tau_i$, where

$$\gamma_i: \begin{cases} e_i \mapsto f_i \\ f_i \mapsto e_i + f_i \end{cases}, \quad \tau_i: \begin{cases} e_i \mapsto f_i \\ f_i \mapsto e_i \end{cases}$$

The planes $V_1, V_2, V_3$ are permuted transitively by $\langle \gamma, \tau \rangle \simeq S_3$, a subgroup of $O(q)$, where

$$\gamma: \begin{cases} e_1 \mapsto e_2, \ e_2 \mapsto e_3, \ e_3 \mapsto e_1 \\ f_1 \mapsto f_2, \ f_2 \mapsto f_3, \ f_3 \mapsto f_1 \end{cases}, \quad \tau: \begin{cases} e_1 \mapsto e_1, \ e_2 \mapsto e_3, \ e_3 \mapsto e_2 \\ f_1 \mapsto f_1, \ f_2 \mapsto f_3, \ f_3 \mapsto f_2 \end{cases}$$

Put $\gamma_0 := \gamma_1 \gamma_2 \gamma_3$, $\tau_0 := \tau_1 \tau_2 \tau_3$, and put

$$\Psi := \langle \gamma, \gamma_1, \gamma_2, \gamma_3 \rangle,$$

which is a 3-Sylow subgroup of $O(q)$.

The group $\Psi$ has center

$$\mathfrak{Z} = \langle \gamma_0 \rangle,$$

derived group

$$\mathfrak{D} = \langle \gamma_1 \gamma_2^{-1}, \gamma_2 \gamma_3^{-1} \rangle,$$

and maximal subgroups

$$\mathfrak{M} = \langle \gamma_1, \gamma_2, \gamma_3 \rangle, \quad \mathfrak{M}_i = \langle \mathfrak{D}, \gamma \gamma_1^i \rangle, \quad i \in \mathbb{Z}/3\mathbb{Z}.$$

For any $i \in \mathbb{Z}/3\mathbb{Z}$, one has

$$\mathfrak{Z} = [\mathfrak{M}_i, \mathfrak{M}_i].$$
And
\[ \tau \mathcal{M}_1 \tau^{-1} = \mathcal{M}_2. \]

The subgroups of \( \mathcal{P} \) that are transitive on \( X \), besides \( \mathcal{P} \), are the maximal subgroups \( \mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3 \).

Let \( \mathcal{Q} \) denote the subgroup of \( O(q) \cap GL_3(E) \) consisting of those elements \( g \) such that \( g(e_2 + e_3) = e_2 + e_3 \), and

\[ g(e_1) = e_1 + b(e_2 + e_3), \quad b \in F_2[3]. \]

One finds by calculation that \( \mathcal{Q} = \{1, \tau, \gamma_1^j \tau_0^j \beta \tau_0^{-j} \gamma_1^{-i}, i \in \mathbb{Z}/3\mathbb{Z}, j \in \mathbb{Z}/2\mathbb{Z}\} \), where

\[ \beta : \begin{cases} 
  e_1 &\mapsto e_1 + e_2 + e_3 \\
  e_2 &\mapsto e_1 + \gamma_0 e_2 + \gamma_0^{-1} e_3 \\
  e_3 &\mapsto e_1 + \gamma_0^{-1} e_2 + \gamma_0 e_3 
\end{cases} \]

**Lemma 11.1.** For any subgroup \( \mathcal{G} \) of \( O(q) \), let its normalizer in \( O(q) \) be denoted by \( N(\mathcal{G}) \). Then

1) \( N(\mathcal{M}) = \langle \mathcal{P}, \tau, \tau_1, \tau_2, \tau_3 \rangle \).

2) \( N(\mathcal{D}) = N(\mathcal{P}) = \mathcal{P}(\tau, \tau_0) \).

3) \( N(\mathcal{M}_1) = N(\mathcal{M}_2) = \mathcal{P}(\tau \tau_0) \).

4) \( N(\mathcal{Z}) = N(\mathcal{M}_0) = \mathcal{P}\mathcal{Q}(\tau_0) \).

**Proof.** The planes \( V_1, V_2, V_3 \) are all the irreducible sub-\( \mathcal{M} \)-modules of \( E \), whence, are permuted by the normalizer \( N(\mathcal{M}) \).

Every \( V_i, i = 1, 2, 3 \), has
\[ GL(V_1) \times GL(V_2) \times GL(V_3) = \langle \mathcal{M}, \tau_1, \tau_2, \tau_3 \rangle \]
as its normalizer in \( O(q) \). Thus, evidently,
\[ N(\mathcal{M}) = \langle \mathcal{M}, \tau_1, \tau_2, \tau_3, \gamma, \tau \rangle = \langle \mathcal{P}, \tau, \tau_1, \tau_2, \tau_3 \rangle. \]

This is 1).

The planes \( V_1, V_2, V_3 \) are also irreducible \( \mathcal{D} \)-modules. From the identities,
\[ V_1 = \text{Ker}(\gamma_2 \gamma_3^{-1} - 1), \quad V_2 = \text{Ker}(\gamma_1 \gamma_3^{-1} - 1), \quad V_3 = \text{Ker}(\gamma_1 \gamma_2^{-1} - 1), \]
it follows that
\[ GL_{\mathcal{D}}(E) = \langle \gamma_1, \gamma_2, \gamma_3 \rangle = \mathcal{M}. \]

As \( \mathcal{M} = GL_{\mathcal{D}}(E) \) is normalized by \( N(\mathcal{D}) \), \( N(\mathcal{D}) \) is a subgroup of \( N(\mathcal{M}) = \langle \mathcal{P}, \tau, \tau_1, \tau_2, \tau_3 \rangle \). By inspection, \( N(\mathcal{D}) = \langle \mathcal{P}, \tau, \tau_0 \rangle \), which normalizes \( \mathcal{P} \), so \( N(\mathcal{P}) = N(\mathcal{D}) \). This proves 2).
In either $\mathcal{M}_1$ or $\mathcal{M}_2$, $\mathfrak{D}$ is the only non-cyclic subgroup of order 9. Therefore, $N(\mathcal{M}_i) \leq N(\mathfrak{D}) = \langle \mathfrak{P}, \tau, \tau_0 \rangle$, and both $N(\mathcal{M}_1)$ and $N(\mathcal{M}_2)$ are equal to $\mathfrak{P} \langle \tau \tau_0 \rangle$, as one verifies easily. This shows 3).

Finally, $N(\mathfrak{Z})$ is generated by $\tau_0$ and $\mathfrak{O}(\mathfrak{q}) \cap \text{GL}_Z(E)$. Show that $\mathfrak{O}(\mathfrak{q}) \cap \text{GL}_Z(E) = PQ$: $\forall g \in \mathfrak{O}(\mathfrak{q}) \cap \text{GL}_Z(E)$, as $P$ is transitive on $X$, there exists $p \in P$ such that

$$p^{-1}g(e_2 + e_3) = e_2 + e_3.$$  

The vector $p^{-1}g(e_1)$, being orthogonal to $p^{-1}g(e_2 + e_3)$ and $p^{-1}g(f_2 + f_3)$, is of the following form:

$$p^{-1}g(e_1) = ae_1 + b(e_2 + e_3), \quad a \in \mathbb{Z}, \quad b \in \mathbb{F}_2[3],$$

where $a = \gamma_i^1$, some $i \in \mathbb{Z}/3\mathbb{Z}$. Then

$$\gamma_i^1 p^{-1}g: \begin{cases} e_2 + e_3 \mapsto e_2 + e_3, \\ e_1 \mapsto e_1 + b(e_2 + e_3) \end{cases}$$

By definition, $\gamma_i^1 p^{-1}g \in \Omega$, and $g \in \mathfrak{P} \langle \Omega \rangle \subset \mathfrak{P} \Omega$.

Now, $\mathfrak{P}, \tau_0, \beta$ do normalize $\mathcal{M}_0$. Hence, $N(\mathcal{M}_0) = N(\mathfrak{Z}) = \mathfrak{P} \Omega \langle \tau_0 \rangle$, which is 4).

Suppose given a solvable subgroup $\mathfrak{G}$ of $O(q)$ acting transitively on $X$. By conjugation in $O(q)$, we arrange that $\mathfrak{G} \cap \mathfrak{D}$ is a 3-Sylow subgroup of $\mathfrak{G}$, thus, $\mathfrak{G} \cap \mathfrak{P} = \mathfrak{P}$, or $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3$.

**Lemma 11.2.** $5 \nmid \text{Card}(\mathfrak{G})$.

*Proof.* Let $\mathcal{L}$ be a $(3,5)$-Hall subgroup of $\mathfrak{G}$ containing $\mathfrak{G} \cap \mathfrak{P}$.

We need to show that $\mathcal{L} = \mathfrak{G} \cap \mathfrak{P}$.

The group $\mathfrak{G} \cap \mathfrak{P}$ is normal in $\mathcal{L}$, since 5 is not congruent to 1 modulo 3, and when $\text{Card}(\mathfrak{G} \cap \mathfrak{P}) = 27$, $\mathfrak{G} \cap \mathfrak{P}$ lies even in the center of $\mathcal{L}$, for 1 is only divisor of 27 that is congruent to 1 modulo 5.

To prove the lemma, it suffices to note that the normalizer of $\mathfrak{P}$ and the centralizers of $\mathcal{M}_i$, $i = 1, 2, 3$, all normalizing $\mathfrak{D}$, have order dividing $3^42^2$, (11.1), 2).

**Lemma 11.3.** Any abelian normal subgroup of $\mathfrak{G}$ is of odd order.

*Proof.* Let $\mathfrak{a}$ be the 2-Sylow subgroup of an abelian normal subgroup of $\mathfrak{G}$.

The space $E^a$ of $\mathfrak{a}$-invariants is a non-zero $\mathfrak{G}$-module, in particular, a non-zero $\mathfrak{D}$-module, thus, the quadratic form $q|E^a$ is non-degenerate.

The group $\mathfrak{a}$ normalizes $(E^a)^\perp$, and

$$(E^a)^\perp a \subset E^a \cap (E^a)^\perp = 0.$$
It follows that a maximal abelian normal subgroup $\mathfrak{A}$ of $\mathfrak{G}$ is a 3-group, of order 27, 9, or 3.

If $\text{Card}(\mathfrak{A}) = 27$, $\mathfrak{A} = \mathfrak{M}$.

Then $\mathfrak{G}$ is contained in $N(\mathfrak{M}) = \langle \mathfrak{P}, \tau, \tau_1, \tau_2, \tau_3 \rangle$, and has the form $\langle \gamma \rangle \mathfrak{H}$, where $\mathfrak{H}$ is any subgroup of $\langle \gamma, \tau, \tau_1, \tau_2, \tau_3 \rangle$ containing $\gamma$. Explicitly, if $\mathfrak{T}$ denotes any of the groups $1$, $\langle \tau \rangle$, $\langle \tau_0 \rangle$, $\langle \tau, \tau_0 \rangle$, then $\mathfrak{H} = \langle \gamma \rangle \mathfrak{T}$, or $\langle \gamma, \tau_1 \tau_2, \tau_2 \tau_3 \rangle \mathfrak{T}$.

Next, suppose $\mathfrak{A}$ cyclic of order 9.

Then, $\mathfrak{A}$ is irreducible on $E$, and is its own centralizer in $O(q)$. Since the quotient $N(\mathfrak{A})/\mathfrak{A}$ acts faithfully by conjugation on $\mathfrak{A}$, and since $\text{Aut}(\mathfrak{A}) \simeq (\mathbb{Z}/9\mathbb{Z})^\times = \mathbb{Z}/6\mathbb{Z}$, the normalizer $N(\mathfrak{A})$ has order dividing $3^3.2$. So $(N(\mathfrak{A}) : \mathfrak{G} \cap \mathfrak{P}) \leq 2$, and $\mathfrak{G} \cap \mathfrak{P}$ is normal in $N(\mathfrak{A})$. It can only be that $\mathfrak{G} \cap \mathfrak{P} = \mathfrak{M}_1$ or $\mathfrak{M}_2 = \tau \mathfrak{M}_1 \tau^{-1}$. Therefore, $\mathfrak{G}$ is conjugate to either $\mathfrak{M}_1$ or $\mathfrak{M}_1 (\tau \tau_0)$.

Now, suppose $\mathfrak{A} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Then, $\mathfrak{A}$ is conjugate to $\mathfrak{D}$, and $\mathfrak{G}$ is conjugate to a subgroup of $N(\mathfrak{D})$. Using that $N(\mathfrak{D})/\mathfrak{D} \simeq \mathfrak{S}_3 \times \mathfrak{S}_3$, the two factors being $\langle \gamma, \tau \rangle$ and $\langle \gamma_1, \tau_0 \rangle$ ($\langle \gamma, \gamma_1 \rangle \in \mathfrak{D}$), one finds that $\mathfrak{G}$ is conjugate to $\mathfrak{M}_1$, or $\langle \mathfrak{M}_1, \tau \tau_0 \rangle$, or $\mathfrak{M}_0 \mathfrak{T}$, where $\mathfrak{T} = 1, \langle \tau \rangle, \langle \tau_0 \rangle, \langle \tau, \tau_0 \rangle$.

Finally, suppose $\text{Card}(\mathfrak{A}) = 3$.

Then, $\mathfrak{A} = 3$, and $\mathfrak{G} \leq N(3) = N(\mathfrak{M}_0)$. In this situation, one checks that $\mathfrak{G}$ is conjugate in $O(q)$ to $\mathfrak{M}_0 \langle \beta \rangle$, $\mathfrak{M}_0 \langle \beta, \tau_0 \rangle$, $\mathfrak{M}_0 \mathfrak{Q}$, $\mathfrak{M}_0 \mathfrak{N} \langle \tau_0 \rangle$, $\mathfrak{P} \mathfrak{Q}$, or $\mathfrak{P} \mathfrak{N} \langle \tau_0 \rangle$.

We have obtained the following classification.

**Proposition 11.4.** Let $\mathfrak{T}$ be any of the groups $1$, $\langle \tau \rangle$, $\langle \tau_0 \rangle$, $\langle \tau \tau_0 \rangle$, $\langle \tau, \tau_0 \rangle$. Then the solvable subgroups of $O(q)$ that act transitively on $X$ are the conjugates of $\mathfrak{P} \mathfrak{T}$, $\mathfrak{P} \langle \tau_1 \tau_2, \tau_2 \tau_3 \rangle \mathfrak{T}$, $\mathfrak{P} \mathfrak{N}$, $\mathfrak{P} \mathfrak{N} \langle \tau_0 \rangle$, $\mathfrak{M} \mathfrak{T}$, $\mathfrak{M} \langle \beta \rangle$, $\mathfrak{M} \langle \beta, \tau_0 \rangle$, $\mathfrak{M} \mathfrak{N}$, $\mathfrak{M} \mathfrak{N} \langle \tau_0 \rangle$, $\mathfrak{M} \mathfrak{N} \langle \tau_0 \rangle$, $\mathfrak{M} \mathfrak{N} \langle \tau_0 \rangle$, $\mathfrak{M}_1$, and $\mathfrak{M}_1 (\tau \tau_0)$.

**Proposition 11.5.** Let $S$, $\eta$, $s$ be as in §4. The pairs $(E_6, \alpha_1)$, $(E_6, \alpha_6)$ are elliptic over $\eta$ if and only if either $s$ is of characteristic 3 or $\text{Card}(k(s)) \equiv \pm 4 \bmod 9$.

**Proof.** By (3.1), (6), $(E_6, \alpha_1)$, $(E_6, \alpha_6)$ are elliptic over $\eta$ if and only if some group in the previous proposition is a quotient of $\pi_1(\eta, \eta)$.

If $s$ is of characteristic 3, either $\mathfrak{M}_0$ or $\mathfrak{M}_1$ is a quotient of $\pi_1(\eta, \eta)$ : Indeed, let $F$ denote the maximal pro-3 quotient of $\pi_1(\eta, \eta)$.
When $\mu_3(\eta) = 1$, $F$ is a free pro-3-group of rank $\geq 2$, thus has a quotient isomorphic to $\mathcal{M}_1$.

When $\mu_3(\eta) > 1$, $F$ has the presentation
\[
\langle x_1, \cdots, x_{d+2} \mid x_1^q [x_1, x_2] [x_3, x_4] \cdots [x_{d+1}, x_{d+2}] = 1 \rangle
\]
where $d = [\eta : Q_3]$, $q$ is the maximal power of 3 such that $\mu_q(\eta) = \mu_q(\eta)$, and $[x, y] := x^{-1}y^{-1}xy$ is the commutator of $x, y$.

The homomorphism $F \to \mathcal{M}_0$, defined as
\[
\begin{align*}
x_1 &\mapsto \gamma \\
x_2 &\mapsto \gamma_0 \\
x_3 &\mapsto \gamma_1 \gamma_2^{-1} \\
x_i &\mapsto 1, \ i > 3
\end{align*}
\]
is clearly surjective.

Next, suppose $s$ is of characteristic different from 3. Then $\mathcal{M}_0$ is not a sub-quotient of $\pi_1(\eta, \eta)$. This excludes all but $\mathcal{M}_1, \mathcal{M}_1\langle \tau\tau_0 \rangle$ in the list of (11.4).

Any surjection $\rho : \pi_1(\eta, \eta) \to \mathcal{M}_1$ or $\rho : \pi_1(\eta, \eta) \to \mathcal{M}_1\langle \tau\tau_0 \rangle$ is necessarily tame, with cyclic inertia group $\rho(I)$ of order 9, where $I$ denotes the kernel of the epimorphism $\pi_1(\eta, \eta) \to \pi_1(S, \eta)$. From the structure of $\pi_1(\eta, \eta)$, it follows immediately that such a surjection $\rho$ exists with image $\mathcal{M}_1$ (resp. $\mathcal{M}_1\langle \tau\tau_0 \rangle$) if and only if $\text{Card}(k(s)) \equiv 4 \pmod{9}$ (resp. $\text{Card}(k(s)) \equiv -4 \pmod{9}$).

\[\Box\]

12. Type $E_7$

Let $E, (, )$ be a 6-dimensional symplectic $F_2$-vector space, $e_i, f_j, 1 \leq i, j \leq 3$, a sympletic base.

Let $q$ be the quadratic form on $E$ such that
\[
q(e_i) = q(f_j) = 1, \ q(e_i + e_j) = q(f_i + f_j) = 0, \ q(e_i + f_j) = \delta_{ij}
\]
where $\delta_{ij} = 1$, if $i = j$, and 0, if $i \neq j$, $\forall \ i, j = 1, 2, 3$.

Clearly, the orthogonal group $O(q)$ is a subgroup of the symplectic group $\text{Sp}(E)$.

The group $\text{Sp}(E)$ is of order $2^9.3^4.5.7$, $O(q)$ is of order $2^7.3^4.5$, and the homogenous space
\[
X = \text{Sp}(E)/O(q)
\]
consists of 28 elements.

We shall determine up to conjugation those solvable subgroups of $\text{Sp}(E)$ that are transitive on $X$, cf. (3.1), 7).
Any such subgroup contains a 7-Sylow subgroup of $\text{Sp}(E)$. By conjugation in $\text{Sp}(E)$, we arrange that it contains $\zeta$, where

$$\zeta : \begin{cases} e_1 \mapsto e_2, & e_2 \mapsto e_3, & e_3 \mapsto e_1 + e_2 \\ f_1 \mapsto f_1 + f_2, & f_2 \mapsto f_3, & f_3 \mapsto f_1 \end{cases}$$

Indeed, $\zeta$ is of order 7, because letting $V = F_2e_1 + F_2e_2 + F_2e_3$, $V^\vee = F_2f_1 + F_2f_2 + F_2f_3$, then

$$\det(T - \zeta, V) = T^3 + T + 1, \quad \det(T - \zeta, V^\vee) = T^3 + T^2 + 1$$

and

$$\det(T - \zeta, E) = (T^3 + T + 1)(T^3 + T^2 + 1) = (T^7 - 1)/(T - 1).$$

As $\zeta$-modules, $V, V^\vee$ are irreducible, mutually non-isomorphic. The subspaces $0, V, V^\vee, E$ are the only sub-$\zeta$-modules of $E$.

The commutant $\text{End}_\zeta(E)$ is equal to $F_2[\zeta][V] \times F_2[\zeta][V^\vee]$.

And

$$\text{GL}_\zeta(E) \cap \text{Sp}(E) = F_2[\zeta]^\times = \langle \zeta \rangle.$$

that is to say, $\langle \zeta \rangle$ is its own centralizer in $\text{Sp}(E)$.

The normalizer of $\langle \zeta \rangle$ in $\text{Sp}(E)$ admits $\zeta, \sigma$ as generators, where

$$\sigma : \begin{cases} e_1 \mapsto f_1, & e_2 \mapsto f_2, & e_3 \mapsto f_2 + f_3 \\ f_1 \mapsto e_1, & f_2 \mapsto e_2 + e_3, & f_3 \mapsto e_3 \end{cases}$$

for, this normalizer modulo $\langle \zeta \rangle$ acts faithfully by conjugation on $\langle \zeta \rangle$, and $\sigma, \zeta$ satisfy the equations

$$\sigma^6 = 1, \quad \sigma \zeta \sigma^{-1} = \zeta^{-2}.$$ 

Let $\mathcal{G}$ denote the centralizer of $V$ in $\text{Sp}(E)$.

Via $g \mapsto (g - 1)|V^\vee$, $\mathcal{G}$ can be identified with the $F_2$-vector space consisting of those linear transformations $A : V^\vee \to V$ such that the bilinear form

$$u', v' \mapsto (u', Av')$$

is symmetric in $u', v' \in V^\vee$.

For any $g \in \mathcal{G}$, the function $v' \mapsto (v', (g - 1)v')$ is linear on $V^\vee$, whence, there exists a unique vector $v_g \in V$ satisfying

$$(v', (g - 1)v') = (v_g, v'), \quad \forall v' \in V^\vee.$$ 

The function $\mathcal{G} \to V$, $g \mapsto v_g$, is linear; its kernel $\mathcal{G}^1$ consists of those elements $g \in \mathcal{G}$ such that the form $u', v' \mapsto (u', (g - 1)v')$ is alternating, that is, $(u', (g - 1)v') = (u' \land v', \omega_g)$, for a uniquely
determined 2-form \( \omega_g \in \wedge^2 V \). The map \( g \mapsto \omega_g \) establishes a canonical bijection from \( S^1 \) onto \( \wedge^2 V \).

The following sequence
\[
0 \to S^1 \to S^g \xrightarrow{g \mapsto \omega_g} V \to 0
\]
is exact. As \( \wedge^2 V = S^1 \) and \( V \) are non-isomorphic \( \zeta \)-modules, this exact sequence splits uniquely as \( \zeta \)-modules so that
\[
S = S^1 \oplus S^2,
\]
with \( S^2 \) \( \zeta \)-linearly isomorphic to \( V \).

**Proposition 12.1.** The solvable subgroups of \( \text{Sp}(E) \) that are transitive on \( X \) are the conjugates of \( \langle \zeta \rangle S, \langle \zeta, \sigma^2 \rangle S, \langle \zeta \rangle S_i, \langle \zeta, \sigma^2 \rangle S_i \), \( i = 1, 2 \).

**Proof.** Suppose \( G \leq \text{Sp}(E) \) solvable, transitive on \( X \), and \( \zeta \in G \).

Recall that \( \text{Card}(\text{Sp}(E)) = 2^9.3^4.5.7 \), \( \text{Card}(O(q)) = 2^7.3^4.5 \).

Show \( 5 \nmid \text{Card}(G) \): for otherwise \( G \) would have a Hall subgroup of order 35, necessarily cyclic. But \( \mathbb{Z}/35\mathbb{Z} \) allows no faithful 6-dimensional representations over \( \mathbb{F}_2 \).

Write \( \text{Card}(G) = 2^a.3^b.7 \), \( a \geq 2, b \geq 0 \).

Let \( \mathcal{L} \) be a Hall subgroup of \( G \), of order \( 3^b.7 \), containing \( \zeta \). Since \( b \leq 4 \), \( \langle \zeta \rangle \) is normal in \( \mathcal{L} \). So \( \mathcal{L} \leq \langle \zeta, \sigma \rangle \). Either \( \mathcal{L} = \langle \zeta \rangle \), or \( \langle \zeta, \sigma^2 \rangle \), and \( b = 0 \) or 1.

Let \( \mathcal{H} \) be a Hall subgroup of \( G \), of order \( 2^a.7 \), containing \( \zeta \).

As \( a \geq 2 \), \( \mathcal{H} \) is not contained in \( \langle \zeta, \sigma \rangle \), that is, \( \langle \zeta \rangle \) is not normal in \( \mathcal{H} \).

Let \( \mathfrak{A} \) be a maximal abelian normal subgroup of \( \mathcal{H} \).

Show \( 7 \nmid \text{Card}(\mathfrak{A}) \): otherwise, the unique 7-Sylow subgroup of \( \mathfrak{A} \) would be normal in \( \mathcal{H} \).

Therefore, \( \mathfrak{A} \) is a 2-group. Then \( E^\mathfrak{A} \), the subspace of \( E \) centralized by \( \mathfrak{A} \), is a non-zero \( \mathcal{H} \)-module, and being normalized by \( \zeta \), it must be \( V \) or \( V^\vee \). Replacing \( \mathfrak{S} \) by \( \sigma \mathfrak{S} \sigma^{-1} \) if necessary, we suppose \( E^\mathfrak{A} = V \).

Now, \( \mathfrak{A} \leq \mathfrak{S} \), and as \( \sigma^3 \) does not normalize \( V \), it follows that \( \sigma^3 \notin \mathcal{H} \), and \( \mathcal{H} \cap \langle \zeta, \sigma \rangle = \langle \zeta \rangle \). The group \( \mathcal{H} \) has \( 2^a = \text{Card}(\mathcal{H}/\langle \zeta \rangle) \) 7-Sylow subgroups, and only one 2-Sylow subgroup, because \( 2^a.7 - 2^a(7-1) = 2^a \). If \( a \leq \mathcal{H} \) is this 2-Sylow subgroup, then \( E^a \) is a non-zero sub-\( \mathcal{H} \)-module of \( E^\mathfrak{A} = V \). So \( E^a = V, a \leq \mathfrak{S} \), and \( a \) is abelian. Therefore, \( \mathfrak{A} = a \) is 2-Sylow in \( \mathcal{H} \), by the choice of \( \mathfrak{A} \).

One finds that \( \mathcal{H} \leq \langle \zeta \rangle \mathfrak{S} \), and \( \mathfrak{S} = \mathcal{L}\mathcal{H} \leq \langle \zeta, \sigma^2 \rangle \mathfrak{S} \).
To conclude the proof, it needs only to show that $\langle \zeta \rangle \mathcal{G}^i, i = 1, 2,$ are both transitive on $X$.

Any $g \in \mathcal{G}$ has the form

$$g : \begin{cases} e_i \mapsto e_i, & i = 1, 2, 3 \\ f_i \mapsto f_i + \sum_{j=1,2,3} A_{ij} e_j \end{cases}$$

where $A_{ij}$ is a symmetric matrix with coefficients in $\mathbb{F}_2$; and $g$ preserves the quadratic form $q$ if and only if $A_{12} = A_{23} = A_{13}$.

The elements of $\mathcal{G}^1$ correspond to those matrices $A_{ij}$ having zero diagonal entries.

The intersection $O(q) \cap \langle \zeta \rangle \mathcal{G}^1 = O(q) \cap \mathcal{G}^1$ equals $\{1, g_1\}$, where

$$g_1 : \begin{cases} e_i \mapsto e_i, & i = 1, 2, 3 \\ f_1 \mapsto f_1 + e_2 + e_3, & f_2 \mapsto f_2 + e_1 + e_3, & f_3 \mapsto f_3 + e_1 + e_2 \end{cases}$$

And a simple calculation shows that $\mathcal{G}^2$ is spanned as a $\zeta$-module by $\tau$, where

$$\tau : \begin{cases} e_i \mapsto e_i, & i = 1, 2, 3 \\ f_1 \mapsto f_1 + e_1, & f_2 \mapsto f_2 + e_3, & f_3 \mapsto f_3 + e_2 \end{cases}$$

The intersection $O(q) \cap \langle \zeta \rangle \mathcal{G}^2 = O(q) \cap \mathcal{G}^2$ consists of 1 and $g_2 := \zeta^2 \tau \zeta^{-2}$. Explicitly,

$$g_2 : \begin{cases} e_i \mapsto e_i, & i = 1, 2, 3 \\ f_1 \mapsto f_1 + e_2 + e_3, & f_2 \mapsto f_2 + e_1 + e_3, & f_3 \mapsto f_3 + e_1 + e_2 + e_3 \end{cases}$$

Since $\text{Card}(X) = 28$, $\text{Card}(\langle \zeta \rangle \mathcal{G}^i) = 56, i = 1, 2$, both groups $\langle \zeta \rangle \mathcal{G}^i$ are indeed transitive on $X$. □

**Proposition 12.2.** Let $S, \eta, s$ be as in §4. The pair $(E_7, \alpha_7)$ is elliptic over $\eta$ if and only if $s$ is of characteristic 2.

**Proof.** Any solvable subgroup $\mathcal{G}$ of $\{1, -1\} \times \text{Sp}(E)$ transitive on

$$\{1, -1\} \times (\text{Sp}(E) / O(q))$$

contains an $\mathbb{F}_2^4$ (12.1). Only if $s$ is of characteristic 2, $\mathcal{G}$ may be a quotient of $\pi_1(\eta, \overline{\eta})$. If $s$ is of characteristic 2, $\{1, -1\} \times \langle \zeta \rangle \mathcal{G}$ is a quotient of $\pi_1(\eta, \overline{\eta})$ because of (4.1) and because $\langle \zeta \rangle \mathcal{G}$ has no subgroup of index 2. One concludes that $(E_7, \alpha_7)$ is elliptic if and only if $\text{char}(s) = 2$, (3.1), 7). □
REFERENCES

1. J.D. Achter. Split reductions of simple abelian varieties. Math. Res. Lett. 16, no. 2 : 199–213, 2009.
2. J.D. Achter. Explicit bounds for split reductions of simple abelian varieties. J. Théor. Nombres Bordeaux, 24, no. 1 : 41–55, 2012.
3. N. Bourbaki. Groupes et algèbres de Lie. Chapitres IV–VI, VII–VIII, Hermann, 1975.
4. P. Deligne. Variétés de Shimura : Interprétation modulaire, et techniques de construction de modèles canoniques. Proceedings of Symposia in Pure Mathematics, vol. 33, part 2 : 247–290, 1979.
5. R. Howe. Perspectives on Invariant Theory. Israel Mathematical Conference Proceedings, vol 8 : 1–182, 1995.
6. D. Livingstone and A. Wagner. Transitivity of finite permutation groups on unordered sets. Math. Z, 90 : 393–403, 1965.
7. V. Kumar Murty and Vijay M. Patankar. Splitting of abelian varieties. Int. Math. Res. Not., 2008.
8. J.P. Serre. Cohomologie Galoisienne. LNM 5, cinquième edition, 1997.
9. J. Tate. Classes d’isogénie de variétés abéliennes sur un corps fini (d’après T.Honda). Séminaire Bourbaki, 1968/69, Exp. 352, LNM 179 : 95–110, 1971.
10. J. Tits. Classification of Algebraic Semisimple Groups. Algebraic Groups and Discontinuous Subgroups, Proc. Sympos. Pure Math : 33–62, 1966.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TORONTO
E-mail address: murty@math.toronto.edu, zongying@math.toronto.edu