Алгебра и анализ
Том 29 (2017), № 1

St. Petersburg Math. J.
Vol. 29 (2018), No. 1, Pages 81–106
http://dx.doi.org/10.1090/spmj/1483
Article electronically published on December 27, 2017

ENDOMORPHISM RINGS OF REDUCTIONS OF ELLIPTIC CURVES AND ABELIAN VARIETIES

YU. G. ZARHIN

Dedicated to Yu. D. Burago
on the occasion of his 80th birthday

Abstract. Let E be an elliptic curve without CM that is defined over a number field K. For all but finitely many non-Archimedean places v of K there is a reduction $E(v)$ of E at v that is an elliptic curve over the residue field $k(v)$ at v. The set of v's with ordinary $E(v)$ has density 1 (Serre). For such v the endomorphism ring $\mathrm{End}(E(v))$ of $E(v)$ is an order in an imaginary quadratic field.

We prove that for any pair of relatively prime positive integers N and M there are infinitely many non-Archimedean places v of K such that the *discriminant* $\mathbf{\Delta(v)}$ of $\mathrm{End}(E(v))$ is divisible by N and the ratio $\frac{\mathbf{\Delta(v)}}{N}$ is relatively prime to NM. We also discuss similar questions for reductions of Abelian varieties.

The subject of this paper was inspired by an exercise in Serre's "Abelian ℓ-adic representations and elliptic curves" and questions of Mihran Papikian and Alina Cojocaru.

§1. Introduction

Let K be a field, $\overline{K}$ its algebraic closure, $\mathrm{Gal}(K) = \mathrm{Aut}(\overline{K}/K)$ the absolute Galois group of K. Let A be an Abelian variety of positive dimension over K. We write $\mathrm{End}(A)$ for its endomorphism ring and $\mathrm{End}^0(A)$ for the corresponding finite-dimensional semisimple $\mathbb{Q}$-algebra $\mathrm{End}(A) \otimes \mathbb{Q}$. One may view $\mathrm{End}(A)$ as an *order* in $\mathrm{End}^0(A)$.

Let n be a positive integer that is *not* divisible by $\mathrm{char}(K)$. We write $A[n]$ for the kernel of multiplication by n in $A(\overline{K})$. It is well known that $A[n]$ is a finite Galois submodule of $A(\overline{K})$; if we forget about the Galois action then the commutative group $A[n]$ is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank $2\dim(A)$. If ℓ is a prime different from $\mathrm{char}(K)$ then we write $T_\ell(A)$ for the $\mathbb{Z}_\ell$-Tate module of A that is defined as a projective limit of commutative groups (Galois modules) A_{ℓ^i} where the transition map $A[\ell^{i+1}] \to A[\ell^i]$ is multiplication by ℓ. It is well known that $T_\ell(A)$ is a free $\mathbb{Z}_\ell$-module of rank $2\dim(A)$ provided with continuous Galois action

$$\rho_{\ell,A} \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)).$$

In particular, $T_\ell(A)$ carries the natural structure of $\mathrm{Gal}(K)$-module. On the other hand, the natural action of $\mathrm{End}(A)$ on A_n gives rise to the embedding

$$\mathrm{End}(A) \otimes \mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathrm{End}_{\mathrm{Gal}(K)}(A[n]).$$

2010 *Mathematics Subject Classification.* Primary 11G10, 14G25.

Key words and phrases. Absolute Galois group, Abelian variety, general linear group, Tate module, Frobenius element.

This work was partially supported by a grant from the Simons Foundation (#246625 to Yuri Zarkhin).

If (as above) we put $n = \ell^i$ then these embedding are glueing together to the embedding of $\mathbb{Z}_\ell$-algebras

$$(*) \qquad \mathrm{End}(A) \otimes \mathbb{Z}_\ell \hookrightarrow \mathrm{End}_{\mathrm{Gal}(K)}(T_\ell)(A)).$$

Tate [19, 20] conjectured that if K is finitely generated then the embedding $(*)$ is actually a bijection and proved it when K is a finite field. The case when $\mathrm{char}(K) > 2$ was done by the author [21, 22], the case when $\mathrm{char}(K) = 0$ by Faltings [4, 5] and the case when $\mathrm{char}(K) = 2$ by Mori [10] (see also [29, 26, 27]).

Now let us consider the $2\dim(A)$-dimensional $\mathbb{Q}_\ell$-vector space

$$V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

and identify $T_\ell(A)$ with the $\mathbb{Z}_\ell$-lattice

$$T_\ell(A) \otimes 1 \subset T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = V_\ell(A).$$

This allows us to identify $\mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A))$ with the (compact) subgroup of $\mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A))$ that consists of all automorphisms that leave invariant $T_\ell(A)$ and consider $\rho_{\ell,A}$ as the ℓ-adic representation

$$\rho_{\ell,A} \colon \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A)).$$

(By definition, $T_\ell(A)$ is a Galois-stable $\mathbb{Z}_\ell$-lattice in $V_\ell(A)$.) We write $G_{\ell,A}$ for the image

$$G_{\ell,A} := \rho_{\ell,A}(\mathrm{Gal}(K)) \subset \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A)).$$

It is known [15] that $G_{\ell,A}$ is a compact ℓ-adic subgroup of $\mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A))$. Extending the embedding $(*)$ by $\mathbb{Q}_\ell$-linearity, we get the embedding of $\mathbb{Q}_\ell$-algebras

$$(**) \qquad \mathrm{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \mathrm{End}(A) \otimes \mathbb{Q}_\ell \hookrightarrow \mathrm{End}_{\mathrm{Gal}(K)}(V_\ell)(A)) \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A)).$$

When K is finitely generated then the $\mathrm{Gal}(K)$-module $V_\ell(A)$ is semisimple: the case of finite fields was done by A. Weil [11], the case when $\mathrm{char}(K) > 2$ was done by the author [21, 22], the case when $\mathrm{char}(K) = 0$ by Faltings [4, 5] and the case when $\mathrm{char}(K) = 2$ by Mori [10] (see also [26]). The semisimplicity of the Galois module $V_\ell(A)$ means that the $G_{\ell,A}$-module $V_\ell(A)$ is semisimple.

Example 1.1 (see [20])**.** Let k be a finite field and

$$\sigma_k \colon \bar{k} \to \bar{k}, \quad x \mapsto x^{\#(k)}$$

the Frobenius automorphism of its algebraic closure. Then σ_k is a topological generator of $\mathrm{Gal}(k)$. If B is an Abelian variety over k of positive dimension then by Tate's *theorem on homomorphisms*

$$\mathrm{End}(B) \otimes \mathbb{Z}_\ell = \mathrm{End}_{\mathrm{Gal}(k)}(T_\ell(B))$$

coincides with the centralizer $\mathrm{End}_{\sigma_k}(T_\ell(B))$ of σ_k in $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(B)$. In addition, σ_k induces a semisimple (diagonalizable over $\overline{\mathbb{Q}_\ell}$) linear operator Fr_B in $V_\ell(B)$. The ring $\mathrm{End}(B)$ is commutative if and only if the characteristic polynomial

$$P_{\mathrm{Fr}_B}(t) = \det(t\mathrm{Id} - \sigma_k, V_\ell(B)) \in \mathbb{Q}_\ell[t]$$

has no multiple roots. (Actually this polynomial has integral coefficients and does not depend on a choice of $\ell \neq \mathrm{char}(k)$.)

Let $\mathfrak{G}_{\ell,A} \subset \mathrm{GL}(V_\ell(A))$ be the Zariski closure of

$$G_{\ell,A} \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A)) = \mathrm{GL}(V_\ell(A))(\mathbb{Q}_\ell)$$

in the general linear group $\mathrm{GL}(V_\ell(A))$ over $\mathbb{Q}_\ell$. By definition, $\mathfrak{G}_{\ell,A}$ is a linear $\mathbb{Q}_\ell$-algebraic subgroup of $\mathrm{GL}(V_\ell(A))$. When K is finitely generated, the semisimplicity of the $G_{\ell,A}$-module $V_\ell(A)$ means that (the identity component of) $\mathfrak{G}_{\ell,A}$ is a reductive algebraic group over $\mathbb{Q}_\ell$. If, in addition, $\mathrm{char}(K) = 0$ then by a theorem of Bogomolov [1, 2, 16], $G_{\ell,A}$ is an *open* subgroup in $\mathfrak{G}_{\ell,A}(\mathbb{Q}_\ell)$. It is known [16] that if the group $\mathfrak{G}_{\ell,A}$ is connected for one prime ℓ then it is connected for all primes.

1.2. Let K be a number field. For all but finitely many non-Archimedean places v of K one may define the *reduction* $A(v)$, which is an Abelian variety of the same dimension as A over the (finite) residue field $k(v)$ of A at v; see [18]. If ℓ does *not* coincide with the residual characteristic of v then each extension $\overline{v}$ of v to $\overline{K}$ gives rise to an isomorphism of Tate modules $T_\ell(A(v)) \cong T_\ell(A)$ that, in turn, gives rise to the natural isomorphisms

$$\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A(v))) \cong \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A)),\ \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A(v))) \cong \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)).$$

Under this isomorphism

$$\mathrm{Fr}_{A(v)} \in \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A(v))) \subset \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A(v)))$$

corresponds to a certain element

$$\mathrm{Frob}_{\overline{v},A,\ell} \in G_{\ell,A} \subset \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)) \subset \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A)) \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A)),$$

which is called the *Frobenius element* attached to $\overline{v}$ in $G_{\ell,A}$. (All $\mathrm{Frob}_{\overline{v},A,\ell}$'s for a given v constitute a conjugacy class in $G_{\ell,A}$.) This implies that the polynomial $P_{\mathrm{Fr}_{A(v)}}(t)$ coincides with the characteristic polynomial

$$P_{v,A}(t) := \det(t\,\mathrm{Id} - \mathrm{Frob}_{\overline{v},A,\ell}, V_\ell(A))$$

of $\mathrm{Frob}_{\overline{v},A,\ell}$. In particular, $\mathrm{End}(A(v))$ is commutative if and only if $P_{v,A}(t)$ has *no* multiple roots.

In the general case, if we denote by

$$\mathfrak{Z}(\mathrm{Frob}_{\overline{v},A,\ell})_0 \subset \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A))$$

the centralizer of $\mathrm{Frob}_{\overline{v},A,\ell}$ in $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A))$ then from Tate's theorem on homomorphisms (Example 1.1) it follows that $\mathfrak{Z}(\mathrm{Frob}_{\overline{v},A,\ell})_0$ is isomorphic as a $\mathbb{Z}_\ell$-algebra to $\mathrm{End}(A(v)) \otimes \mathbb{Z}_\ell$.

By the Chebotarev density theorem, the set of all $\mathrm{Frob}_{\overline{v},A,\ell}$'s (for all v) is everywhere dense in $G_{\ell,A}$ [15, Chapter I].

Our main result is the following statement.

Theorem 1.3. *Let A be an Abelian variety of positive dimension over a number field K. Suppose that the groups $\mathfrak{G}_{\ell,A}$ are connected. Let $\mathbf{P}$ be a finite nonempty set of primes and suppose that for each $\ell \in \mathbf{P}$ we are given an element*

$$f_\ell \in \mathfrak{G}_{\ell,A}(\mathbb{Q}_\ell) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A))$$

such that its characteristic polynomial

$$P_{f_\ell}(t) = \det(t\,\mathrm{Id} - f_\ell, V_\ell(A)) \in \mathbb{Q}_\ell[t]$$

has no multiple roots. Let

$$\mathfrak{Z}(f_\ell)_0 \subset \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A))$$

be the centralizer of f_ℓ in

$$\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A)) \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A)).$$

Then the set of non-Archimedean places v of K such that the residual characteristic $\mathrm{char}(k(v))$ *does not belong to $\mathbf{P}$, the Abelian variety A has good reduction at v, and*

$$\mathrm{End}(A(v)) \otimes \mathbb{Z}_\ell \cong \mathfrak{Z}(f_\ell)_0 \quad \forall \ell \in \mathbf{P}$$

has positive density. (*In addition, for all such v the ring* $\mathrm{End}(A(v))$ *is commutative.*)

Example 1.4. Let A be an Abelian variety of positive dimension over a number field K and suppose that the groups $\mathfrak{G}_{\ell,A}$ are connected. Let r be a positive integer and let $\ell_1, \dots, \ell_r$ be r *distinct primes*. Suppose that for each ℓ_i we are given a non-Archimedean place $\mathbf{v}_i$ of K such that its residual characteristic $\mathrm{char}(k(\mathbf{v}_i)) \ne \ell_i$, the Abelian variety A has good reduction $A(\mathbf{v}_i)$ at $\mathbf{v}_i$ and the endomorphism ring $\mathrm{End}(A(\mathbf{v}_i))$ is *commutative*. This implies that the characteristic polynomial of each Frobenius element $\mathrm{Frob}_{\overline{\mathbf{v}_i},A,\ell} \in G_{\ell,A}$ has *no multiple roots*. Recall that the centralizer $\mathfrak{Z}(\mathrm{Frob}_{\overline{\mathbf{v}_i},A,\ell})_0$ is isomorphic as $\mathbb{Z}_\ell$-algebra to $\mathrm{End}(A(\mathbf{v}_i)) \otimes \mathbb{Z}_\ell$. Let us put $\mathbf{P} = \{\ell_1, \dots, \ell_r\}$. From Theorem 1.3 it follows that the set of non-Archimedean places v of K such that the residual characteristic $\mathrm{char}(k(v))$ does not belong to $\mathbf{P}$, the abelian variety A has good reduction $A(v)$ at v, and

$$\mathrm{End}(A(v)) \otimes \mathbb{Z}_{\ell_i} \cong \mathrm{End}(A(\mathbf{v}_i)) \otimes \mathbb{Z}_{\ell_i} \quad \forall i = 1, \dots, r$$

has positive density.

Example 1.5. Let E be an elliptic curve without complex multiplication that is defined over a number field K. By a theorem of Serre [15, Chapter IV, Section 2.2],

$$\mathfrak{G}_{\ell,E} = \mathrm{GL}(V_\ell(E)).$$

In particular, $\mathfrak{G}_{\ell,E}$ is connected and isomorphic to the general linear group $\mathrm{GL}(2)$ over $\mathbb{Q}_\ell$ while

$$\mathfrak{G}_{\ell,E}(\mathbb{Q}_\ell) = \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(E)).$$

Let $\mathbf{P}$ be a finite nonempty set of primes. For each $\ell \in \mathbf{P}$ we fix a commutative *semisimple* 2-dimensional $\mathbb{Q}_\ell$-algebra C_ℓ. Let us choose an *order* $\mathcal{O}_\ell$ in C_ℓ, i.e., a $\mathbb{Z}_\ell$-subalgebra of C_ℓ (with the same 1) that is a free $\mathbb{Z}_\ell$-submodule of rank 2. Let us fix an isomorphism of free $\mathbb{Z}_\ell$-modules

$$\mathcal{O}_\ell \cong T_\ell(E),$$

which extends by $\mathbb{Q}_\ell$-linearity to the isomorphism of $\mathbb{Q}_\ell$-vector spaces

$$C_\ell = \mathcal{O}_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = V_\ell(E).$$

Multiplication in C_ℓ gives rise to an embedding

$$C_\ell \hookrightarrow \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(E));$$

further we will identify C_ℓ with its image in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(E))$. Clearly, C_ℓ coincides with its own centralizer in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(E))$. On the other hand, one may easily check (using the inclusion $1 \in \mathcal{O}_\ell$) that

$$\mathcal{O}_\ell = \{u \in C_\ell \mid u(T_\ell(E)) \subset T_\ell(E)\}.$$

This implies that $\mathcal{O}_\ell$ coincides with the centralizer of C_ℓ in

$$\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(E)) \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(E)).$$

Since C_ℓ is 2-dimensional, there exists $f_\ell \in C_\ell$ such that the pair $\{1, f_\ell\}$ is a basis of the $\mathbb{Q}_\ell$-vector space C_ℓ. Replacing f_ℓ by $1 + \ell^M f_\ell$ for sufficiently big positive integer M, we may and will assume that

$$f_\ell \in C_\ell^* \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(E)).$$

Clearly, the centralizer $\mathfrak{Z}(f_\ell)_0$ of f_ℓ in $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(E))$ coincides with the centralizer of C_ℓ in $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(E))$. This implies that

$$\mathfrak{Z}(f_\ell)_0 = \mathcal{O}_\ell \quad \forall \ell \in \mathbf{P}.$$

Applying Theorem 1.3, we conclude that the set of non-Archimedean places v of K such that the residual characteristic $\mathrm{char}(k(v))$ does *not* belong to $\mathbf{P}$, the elliptic curve E has good reduction at v, and

$$\mathrm{End}(E(v)) \otimes \mathbb{Z}_\ell \cong \mathcal{O}_\ell \quad \forall \ell \in \mathbf{P}$$

has positive density.

For example, if F is an imaginary quadratic field with the ring of integers O_F and N is a positive integer, then we consider the order $\Lambda = \mathbb{Z} + N \cdot O_F$ of conductor N in F and the collection of $\mathbb{Z}_\ell$-algebras

$$\mathcal{O}_\ell := \Lambda \otimes \mathbb{Z}_\ell \quad \forall \ell \in \mathbf{P}.$$

We see that the set $\Sigma(E, F, N)$ of all non-Archimedean places v of K such that the residual characteristic $\mathrm{char}(k(v))$ does *not* belong to $\mathbf{P}$, the elliptic curve E has good ordinary reduction at v, and

$$\mathrm{End}(E(v)) \otimes \mathbb{Z}_\ell \cong \Lambda \otimes \mathbb{Z}_\ell \quad \forall \ell \in \mathbf{P}$$

has positive density. In particular, this set is infinite.

Corollary 1.6. *Let E be an elliptic curve without CM that is defined over a number field K. Let N and M be relatively prime positive integers. Consider the set $\widetilde{\Sigma}(E, M, N)$ of non-Archimedean places v of K such E has good ordinary reduction at v, the residual characteristic* $\mathrm{char}(k(v))$ *does not divide NM, the discriminant $\mathbf{\Delta}(v)$ of the order* $\mathrm{End}(E(v))$ *is divisible by N and the ratio $\mathbf{\Delta}(v)/N$ is relatively prime to MN. Then $\widetilde{\Sigma}(E, M, N)$ contains a set of positive density. In particular, $\widetilde{\Sigma}(E, M, N)$ is infinite.*

Remark 1.7. Actually, one can prove that $\widetilde{\Sigma}(E, M, N)$ has density, which is, of course, positive.

Remark 1.8. The discriminant $\mathbf{\Delta}(v)$ is *not* divisible by a prime ℓ if and only if either

$$\mathrm{End}(E(v)) \otimes \mathbb{Q}_\ell = \mathbb{Q}_\ell \oplus \mathbb{Q}_\ell \supset \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell = \mathrm{End}(E(v)) \otimes \mathbb{Z}_\ell$$

or $\mathrm{End}(E(v)) \otimes \mathbb{Q}_\ell$ is a *field* that is an *unramified* quadratic extension of $\mathbb{Q}_\ell$ and $\mathrm{End}(E(v)) \otimes \mathbb{Z}_\ell$ is the ring of integers in this quadratic field.

Proof of Corollary 1.6. Let $\mathbf{P}$ be the set of prime divisors of MN. Choose an imaginary quadratic field F, whose discriminant is prime to NM and put $\Lambda = \mathbb{Z} + N \cdot O_F$. Then $\widetilde{\Sigma}(E, M, N)$ contains all the places of $\Sigma(E, F, N)$ except the finite set of places with residual characteristic dividing M. The set $\Sigma(E, F, N)$ has positive density (see Example 1.5), which would not change if we remove finitely many places from it. $\square$

Remark 1.9. Serre [15, Chapter IV, Section 2.2, Exercises on pp. IV–13] sketched a proof of the following assertion.

The set of non-Archimedean places v of K such that $\mathrm{char}(k(v))$ *does not belong to $\mathbf{P}$, the elliptic curve E has good ordinary reduction at v and*

$$\mathrm{End}(E(v)) \otimes \mathbb{Q}_\ell \cong C_\ell \quad \forall \ell \in \mathbf{P}$$

has positive density. In particular, if one defines the set $\Sigma_{\mathbf{P}}(E)$ of all places v such that E has good ordinary reduction at v, the residual characteristic $\mathrm{char}(k(v))$ does not belong to $\mathbf{P}$, and the discriminant of the quadratic field $\mathrm{End}(E(v)) \otimes \mathbb{Q}$ is divisible by all $\ell \in P$ then $\Sigma_{\mathbf{P}}(E)$ is infinite. (See also [13, Corollary 2.4 on p. 329].)

Theorem 1.10. *Let $g \geq 2$ be an integer, $n = 2g+1$ or $2g+2$. Let $\mathbf{P}$ be a nonempty finite set of primes and suppose that for each $\ell \in \mathbf{P}$ we a given a field $\mathcal{K}^{(\ell)}$ of characteristic different from ℓ, a g-dimensional simple Abelian variety $B^{(\ell)}$ over $\mathcal{K}^{(\ell)}$ that admits a polarization of degree prime to ℓ and such that* $\mathrm{End}^0(B^{(\ell)})$ *is a number field of degree $2g$. (For example, if B is a principally polarized g-dimensional simple complex Abelian variety of CM type then we may take $B^{(\ell)} = B$ for all $\ell \in \mathbf{P}$.)*

Let K be a number field and $f(x) \in K[x]$ a degree n irreducible polynomial whose Galois group over K is either the full symmetric group $\mathbf{S}_n$ or the alternating group $\mathbf{A}_n$.

Consider the genus g hyperelliptic curve $C_f : y^2 = f(x)$ and its Jacobian A, which is a g-dimensional Abelian variety over K.

Let Σ be the set of all non-Archimedean places v of K such that A has good reduction at v, the residual characteristic $\mathrm{char}(k(v))$ does not belong to $\mathbf{P}$ and the $\mathbb{Z}_\ell$-rings $\mathrm{End}(A)\otimes\mathbb{Z}_\ell$ and $\mathrm{End}((B^{\ell)}) \otimes \mathbb{Z}_\ell$ are isomorphic for all $\ell \in \mathbf{P}$. Then Σ has density > 0.

The paper is organized as follows. In §2 we discuss ℓ-adic symplectic groups that arise from polarizations on Abelian varieties. §3 deals with trace forms and realated symplectic structures. §4 deals with centralizers of certain *generic* elements of linear reductive groups over $\mathbb{Q}_\ell$. §5 deals with applications of the Chebotarev density theorem for infinite Galois extensions of number fields with ℓ-adic Galois groups. In §6 we prove Theorems 1.3 and 1.10.

§2. Polarizations and symplectic groups

Let B be an Abelian variety of positive dimension g over a field K and let ℓ be a prime that is different from $\mathrm{char}(K)$. We write

$$\chi_\ell \colon \mathrm{Gal}(K) \to \mathbb{Z}_\ell^*,$$

the *cyclotomic character* that defines the Galois action on all ℓ-power roots of unity. Let λ be a polarization on B. Then λ gives rise to the altermating nondegenerate $\mathbb{Z}_\ell$-bilinear form

$$e_{\lambda,\ell} \colon T_\ell(B) \times T_\ell(B) \to \mathbb{Z}_\ell$$

such that

$$e_{\lambda,\ell}(\rho_{\ell,B}(\sigma)x, \rho_{\ell,B}(\sigma)y) = \chi_\ell(\sigma)e_{\lambda,\ell}(x, y)$$

for all $\sigma \in \mathrm{Gal}(K)$ and $x, y \in T_\ell(B)$; in addition, $e_{\lambda,\ell}$ is perfect/unimodular if and only if $\deg(\lambda)$ is *not* divisible by ℓ (see [7]). Let us consider the (compact) group of symplectic similitudes

$$\mathrm{Gp}(T_\ell(B), e_{\lambda,\ell}) = \{u \in \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(B)) \mid \exists c \in \mathbb{Z}_\ell^* \text{ such that } e_{\lambda,\ell}(ux, uy) = c \cdot e_{\lambda,\ell}(x, y)$$

for all $x, y \in T_\ell(B)\}$. Clearly,

$$G_{\ell,B} = \rho_{\ell,A}(\mathrm{Gal}(K)) \subset \mathrm{Gp}(T_\ell(B), e_{\lambda,\ell}) \subset \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(B)) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(B)).$$

Extending $e_{\lambda,\ell}$ by $\mathbb{Q}_\ell$-linearity to $V_\ell(B) = T_\ell(B) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, we obtain the altermating nondegenerate $\mathbb{Z}_\ell$-bilinear form

$$V_\ell(B) \times V_\ell(B) \to \mathbb{Q}_\ell,$$

which we continue to denote $e_{\lambda,\ell}$. Clearly,

$$e_{\lambda,\ell}(\rho_{\ell,B}(\sigma)x, \rho_{\ell,B}(\sigma)y) = \chi_\ell(\sigma)e_{\lambda,\ell}(x, y)$$

for all $\sigma \in \mathrm{Gal}(K)$ and $x, y \in V_\ell(B)$. Let us consider the group of symplectic similitudes

$$\mathrm{Gp}(V_\ell(B), e_{\lambda,\ell}) = \{u \in \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(B)) \mid \exists c \in \mathbb{Q}_\ell^* \text{ such that } e_{\lambda,\ell}(ux, uy) = c \cdot e_{\lambda,\ell}(x, y)$$

for all $x, y \in V_\ell(B)\}$. Clearly, $\mathrm{Gp}(T_\ell(B), e_{\lambda,\ell})$ is the open compact subgroup of the (locally compact) group $\mathrm{Gp}(V_\ell(B), e_{\lambda,\ell})$ that coincides with the intersection

$$\mathrm{Gp}(V_\ell(B), e_{\lambda,\ell}) \cap \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(B)).$$

We have

$$G_{\ell,A} \subset \mathrm{Gp}(T_\ell(B), e_{\lambda,\ell}) \subset \mathrm{Gp}(V_\ell(B), e_{\lambda,\ell}) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(B)).$$

We write $\mathfrak{Gp}(V_\ell(B), e_{\lambda,\ell}) \subset \mathrm{GL}(V_\ell(B))$ for the connected linear reductive algebraic group of *symplectic similitudes* over $\mathbb{Q}_\ell$ attached to $e_{\lambda,\ell}$. Its group of $\mathbb{Q}_\ell$-points

$$\mathfrak{Gp}(V_\ell(B), e_{\lambda,\ell})(\mathbb{Q}_\ell) = \mathrm{Gp}(V_\ell(B), e_{\lambda,\ell}) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(B)) = \mathrm{GL}(V_\ell(B))(\mathbb{Q}_\ell).$$

Let us consider the finite-dimensional semisimple $\mathbb{Q}$-algebra

$$\mathrm{End}^0(B) = \mathrm{End}(B) \otimes \mathbb{Q}.$$

We have the natural isomorphisms of $\mathbb{Q}$-algebras

$$[\mathrm{End}(B) \otimes \mathbb{Z}_\ell] \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = \mathrm{End}(B) \otimes \mathbb{Q}_\ell = [\mathrm{End}(B) \otimes \mathbb{Q}] \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \mathrm{End}^0(B) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.$$

By $(**)$, there is a natural embedding

$$\mathrm{End}^0(B) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \mathrm{End}(B) \otimes \mathbb{Q}_\ell \hookrightarrow \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(B)).$$

We may view $\mathrm{End}^0(B)$ as a certain $\mathbb{Q}$-subalgebra of $\mathrm{End}^0(B) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, identify the latter with its image in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(B))$, and get

$$\mathrm{End}^0(B) \subset \mathrm{End}^0(B) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(B)).$$

The polarization λ gives rise to the *Rosati involution* [7, 11]

$$\mathrm{End}^0(B) \to \mathrm{End}^0(B), u \mapsto u'$$

such that

$$e_{\lambda,\ell}(ux, y) = e_{\lambda,\ell}(x, u'y) \quad \forall x, y \in V_\ell(B).$$

This involution extends by $\mathbb{Q}_\ell$-linearity to the involution of the semisimple finite-dimensional $\mathbb{Q}_\ell$-algebra $\mathrm{End}^0(B) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$,

$$\mathrm{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \to \mathrm{End}^0(B) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell, u \mapsto u',$$

such that

$$e_{\lambda,\ell}(ux, y) = e_{\lambda,\ell}(x, u'y) \quad \forall x, y \in V_\ell(B).$$

This implies that

$$u \in [\mathrm{End}^0(B) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell]^* \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(B))$$

lies in $\mathrm{Gp}(V_\ell(B), e_{\lambda,\ell})$ if and only if

$$u'u \in \mathbb{Q}_\ell^* \mathrm{Id}.$$

The following statement will be used in the proof of Theorem 1.10.

Theorem 2.1. *Suppose that* $\mathrm{End}^0(B)$ *is a number field of degree* $2g$*. Then there exists an element* $u \in \mathrm{End}(B)$ *and a positive integer* $q \in \mathbb{Z}$ *such that*

$$\mathrm{End}^0(B) = \mathbb{Q}[u], \quad u'u = q, \quad u \in \mathrm{Gp}(V_\ell(B), e_{\lambda,\ell})$$

and the characteristic polynomial $P_u(t) = \det(t\,\mathrm{Id} - u, V_\ell(B))$ *of* u *has no multiple roots.*

In addition, the centralizer $\mathfrak{Z}(u)_0$ *of* u *in* $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(B)) \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(B))$ *coincides with* $\mathrm{End}(B) \otimes \mathbb{Z}_\ell$*.*

In the course of the proof of Theorem 2.1 we will use the following statement that will be proven at the end of this section. (See also [23, Section 4].)

Lemma 2.2. *Let* Q *be a field of characteristic zero,* F_0/Q *a finite algebraic field extension, and* F/F_0 *a quadratic field extension. Let* $\tau \in \mathrm{Gal}(F/F_0)$ *be the only nontrivial element (involution) of the Galois group of* F/F_0*. Then there exists* $u \in F$ *such that* $F = Q[u]$ *and* $u \cdot \tau u = 1$*.*

Proof of Theorem 2.1. From Albert's classification [11] (see also [12]) it follows that the field $F := \mathrm{End}^0(B)$ is a CM field and the Rosati involution coincides with the complex conjugation $z \mapsto \bar{z}$ on F and $R := \mathrm{End}(B)$ is an order in F. Recall that F is a purely imaginary quadratic extension of its totally real number subfield F_0 and the complex conjugation is the only nontrivial element of the Galois group of F/F_0.

We have

$$F_\ell := F \otimes \mathbb{Q}_\ell = \mathrm{End}^0(B) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(B)).$$

Clearly, all elements of the commutative semisimple $\mathbb{Q}_\ell$-algebra F_ℓ act as semisimple linear operators in $V_\ell(B)$. The F_ℓ-module $V_\ell(B)$ is *free of rank* 1 [18, Section 4, Theorem 5(1)]. This implies that F_ℓ coincides with its own centralizer $\mathrm{End}_{F_\ell}(V_\ell(B))$ in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(B))$. On the other hand, the intersection

$$F_\ell \cap \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(B))$$

coincides with

$$R_\ell := R \otimes \mathbb{Z}_\ell = \mathrm{End}(B) \otimes \mathbb{Z}_\ell$$

[18, Section 4, Theorem 5(1)].

Suppose that we have constructed an element $u \in R = \mathrm{End}(B)$ such that $F = \mathrm{End}^0(B) = \mathbb{Q}[u]$ and $u'u = q$ for some positive integer q. This implies that the centralizer $\mathfrak{Z}(u)$ of u in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(B))$ coincides with the centralizer $\mathrm{End}_{F_\ell}(V_\ell(B))$ of F_ℓ, i.e., equals F_ℓ. It follows that the centralizer $\mathfrak{Z}(u)_0$ of u in $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(B))$ coincides with the the intersection $F_\ell \cap \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(B))$, i.e., equals R_ℓ. In addition, since F_ℓ is the centralizer of u in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(B))$ and

$$\dim_{\mathbb{Q}_\ell}(F_\ell) = 2g = \dim_{\mathbb{Q}_\ell}(V_\ell(B)),$$

the characteristic polynomial $P_u(t)$ of u has *no* multiple roots. We have

$$e_{\lambda,\ell}(ux, uy) = e_{\lambda,\ell}(x, u'uy) = e_{\lambda,\ell}(x, q \cdot y) = q \cdot e_{\lambda,\ell}(x, y)$$

for all $x, y \in V_\ell(B)$. This implies that

$$u \in \mathrm{Gp}(V_\ell(B), e_{\lambda,\ell}).$$

Now let us construct such an u. Applying Lemma 2.2 (to $Q = \mathbb{Q}$), we obtain the existence of $u_1 \in F$ with $\mathbb{Q}[u_1] = F$ and $u_1' \cdot u_1 = 1$. Then there is a positive integer m such that $u := mu_1$ lies in R. Clearly,

$$\mathbb{Q}[b] = \mathbb{Q}[u_1] = F, \quad u' = mu_1', \quad u' \cdot u = m^2 u_1' \cdot u_1 = m^2 \cdot 1 = m^2.$$

Now one has only to put $q = m^2$. □

Proof of Lemma 2.2. Recall that for each $u \in F$ the Q-subalgebra $Q[u]$ of F generated by u is actually a subfield, i.e., coincides with the (sub)field $Q(u)$.

Since F/F_0 is quadratic, $F = F_0(\sqrt{\delta})$ for some *nonzero* $\delta \in F_0$. We have

$$F = F_0 + F_0 \cdot \sqrt{\delta}, \quad \tau(\sqrt{\delta}) = -\sqrt{\delta}$$

and F_0 coincides with the subfield of τ-invariants in F.

Suppose that there is a nonzero $\beta_0 \in F_0$ such that $F_0 = Q(\delta\beta_0^2)$. Replacing if necessary β_0 by $2\beta_0$, we may and will assume that

$$\delta\beta_0^2 + 1 \neq 0.$$

Let us put

$$\beta = \frac{\delta\beta_0^2 - 1}{\delta\beta_0^2 + 1} + \frac{2\beta_0}{\delta\beta_0^2 + 1} \cdot \sqrt{\delta}.$$

Clearly,

$$\beta \notin F_0, \quad \tau(\beta) = \frac{\delta\beta_0^2 - 1}{\delta\beta_0^2 + 1} - \frac{2\beta_0}{\delta\beta_0^2 + 1} \cdot \sqrt{\delta}, \quad \tau(\beta) \cdot \beta = 1$$

and therefore $Q(\beta)$ contains $\tau(\beta) = 1/\beta$, which implies that it contains both $\frac{\delta\beta_0^2-1}{\delta\beta_0^2+1}$ and $\frac{2\beta_0}{\delta\beta_0^2+1} \cdot \sqrt{\delta}$. This implies that $Q(\beta)$ contains $\delta\beta_0^2$ and therefore contains $Q(\delta\beta_0^2)$. Since $Q(\delta\beta_0^2) = F_0$, the subfield $Q(\beta)$ contains F_0 and we have

$$F_0 \subset Q(\beta) \subset F.$$

Since F_0 does not contain β, $F_0 \neq Q(\beta)$ and therefore $Q(\beta) = F$. We have

$$Q[\beta] = Q(\beta) = F.$$

This ends the proof if we find $\beta_0 \in F_0$ with

$$F_0 = Q(\delta\beta_0^2).$$

Now let us construct such a β_0. If $F_0 = Q$ we may take any

$$\beta_0 \in Q = F, \quad \beta_0 \neq 0, \quad \beta_0^2 \neq -\frac{1}{\delta}.$$

Now suppose that $F_0 \neq Q$. Since F_0/Q is separable, there is $\gamma \in F_0$ with $F_0 = Q(\gamma)$. Clearly, $\gamma \notin \mathbb{Q} \subset Q$; in particular, $\gamma \neq 0$. Since separable F_0/Q contains only finitely many field subextensions of Q, there are two *distinct* positive integers $i, j \in \mathbb{Z} \subset Q$ such that the subfields $Q(\delta(\gamma+i)^2)$ and $Q(\delta(\gamma+j)^2)$ do coincide. (Notice that $i^2 \neq j^2$.) This implies that $2\delta(j-i)\gamma$ lies in $Q(\delta(\gamma+i)^2)$, i.e.,

$$\delta \cdot \gamma \in Q(\delta(\gamma+i)^2) = Q(\delta(\gamma+j)^2).$$

This implies that both

$$\frac{(\gamma+i)^2}{\gamma} = \frac{\delta \cdot (\gamma+i)^2}{\delta \cdot \gamma} \text{ and } \frac{(\gamma+j)^2}{\gamma} = \frac{\delta \cdot (\gamma+j)^2}{\delta \cdot \gamma}$$

lie in $Q(\delta(\gamma+i)^2)$. This implies that

$$(2i-2j) + \frac{i^2-j^2}{\gamma} = \frac{(\gamma+i)^2}{\gamma} - \frac{(\gamma+j)^2}{\gamma} \in Q(\delta(\gamma+i)^2).$$

Since $i^2 \neq j^2$, we conclude that $1/\gamma$ lies in $Q(\delta(\gamma+i)^2)$ and therefore

$$Q(\gamma) = F_0 \supset Q(\delta(\gamma+i)^2) \supset Q(1/\gamma) = Q(\gamma) = F_0.$$

This implies that $Q(\delta(\gamma+i)^2) = F_0$ and we may put $\beta_0 = \gamma + i$. □

We finish this section with the following elementary (and probably well-known) statement that will be used later in Example 4.6.

Lemma 2.3. *Let Q be a field of characteristic zero and C a finite-dimensional commutative semisimple Q-algebra. Then there exists an invertible element u of C such that $C = Q[u]$.*

Proof. It is well known that commutative semisimple C splits into a finite direct sum

$$C = \bigoplus_{i=1}^{r} C_i$$

where each C_i is an overfield of Q. It is also clear that C_i/Q is a finite algebraic field extension. Since we live in characteristic zero, each C_i/Q is separable and therefore there exists nonzero $z_i \in C_i$ such that $C_i = Q[z_i]$. Let $\mathcal{P}_i(t) \in Q[t]$ be the minimal polynomial of z_i over Q. By definition, $\mathcal{P}_i(t)$ is an irreducible monic polynomial of degree $[C_i : Q]$. We have

$$\mathbb{Z} \subset \mathbb{Q} \subset Q \subset C_i.$$

We may choose integers $n_i \in \mathbb{Z}$ in such a way that all $\mathcal{P}_i(t+n_i)$ are distinct and do *not* vanish at zero; in particular, they all are monic irreducible and therefore relatively prime to each other. Clearly, $\mathcal{P}_i(t+n_i)$ is the minimal polynomial of $z_i - n_i$ over K. Clearly, $Q_j = Q[z_i] = Q[z_i - n_i]$. This implies that the field C_i is isomorphic as Q-algebra to the quotient $Q[t]/\mathcal{P}_i(t+n_i)Q[t]$. This implies that the Q-algebra $Q[t]/\{\prod_{i=1}^r \mathcal{P}_i(t+n_i)\}Q[t]$ is isomorphic to the direct sum $\oplus_{i=1}^r C_i = C$. Now one may take as u the image of t in C. □

§3. Trace forms

3.1. Let ℓ be a prime. Let $F_0/\mathbb{Q}_\ell$ be a field extension of finite degree g. Let $\mathcal{O}_0 = \mathcal{O}_{0,\ell}$ be the ring of integers of the ℓ-adic field $F_{0,\ell} := F_0$, which carries the natural structure of a free $\mathbb{Z}_\ell$-module of rank g. We fix a uniformizer $\pi \in \mathcal{O}_0$ that generates the maximal ideal in $\mathcal{O}_0$. We write

$$\mathrm{Tr}_0 := \mathrm{Tr}_{F_0/\mathbb{Q}_\ell}\colon F_0 \to \mathbb{Q}_\ell$$

for the ($\mathbb{Q}_\ell$-linear) trace map from F_0 to $\mathbb{Q}_\ell$. It is well known that the symmetric $\mathbb{Q}_\ell$-bilinear *trace form*

$$B_{\mathrm{Tr}}\colon F_0 \times F_0 \to \mathbb{Q}_\ell,\ x, y \mapsto \mathrm{Tr}_0(xy)$$

is nondegenerate. This means that the homomorphism of $\mathbb{Q}_\ell$-vector spaces

$$\phi_{\mathrm{Tr}}\colon F_0 \to \mathrm{Hom}_{\mathbb{Q}_\ell}(F_0, \mathbb{Q}_\ell)$$

that assigns to each $a \in F_0$ the $\mathbb{Q}_\ell$-linear map

$$B_{\mathrm{Tr}}(a, ?)\colon F_0 \to \mathbb{Q}_\ell,\ x \mapsto B_{\mathrm{Tr}}(a, x) = \mathrm{Tr}_0(ax)$$

is an isomorphism. Recall that the natural homomorphism of $\mathbb{Z}_\ell$-algebras

$$\mathcal{O}_0 \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \to F_0,\ x \otimes c \mapsto c \cdot x$$

is an isomorphism. This implies that the restriction map

$$\mathrm{Hom}_{\mathbb{Q}_\ell}(F_0, \mathbb{Q}_\ell) \to \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{O}_0, \mathbb{Q}_\ell)$$

is an isomorphism of $\mathbb{Z}_\ell$-modules. (Further we will identify these modules, using this isomorphism.) We have

$$\mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{O}_0, \mathbb{Z}_\ell) \subset \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{O}_0, \mathbb{Q}_\ell) = \mathrm{Hom}_{\mathbb{Q}_\ell}(F_0, \mathbb{Q}_\ell).$$

The preimage

$$\mathcal{D}^{-1} := \phi_{\mathrm{Tr}}^{-1}(\mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{O}_0, \mathbb{Z}_\ell)) \subset F_0$$

is the *inverse different*, which is a fractional ideal in F_0 that contains $\mathcal{O}_0$ [14, Chapter III, Section 3]. Since the obvious $\mathbb{Z}_\ell$-bilinear pairing of free $\mathbb{Z}_\ell$-modules of rank g

$$\mathcal{O}_0 \times \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{O}_0, \mathbb{Z}_\ell) \to \mathbb{Z}_\ell$$

is unimodular, the $\mathbb{Z}_\ell$-bilinear pairing of free $\mathbb{Z}_\ell$-modules of rank g

$$\mathcal{O}_0 \times \mathcal{D}^{-1} \to \mathbb{Z}_\ell, \quad (x, y) \mapsto \mathrm{Tr}_0(xy)$$

is also unimodular. Notice that there is a nonnegative integer d such that

$$\mathcal{D}^{-1} = \pi^{-d}\mathcal{O}_0 \subset F_0.$$

This implies that the symmetric $\mathbb{Z}_\ell$-bilinear pairing

$$\widetilde{B}_{\mathrm{Tr}}\colon \mathcal{O}_0 \times \mathcal{O}_0 \to \mathbb{Z}_\ell, \quad x, y \mapsto \mathrm{Tr}_0(\pi^{-d}xy)$$

is unimodular.

Let $T = T_\ell$ be a free $\mathcal{O}_0$-module of rank 2 provided with an alternating $\mathcal{O}_0$-bilinear unimodular form

$$e_0\colon T \times T \to \mathcal{O}_0.$$

Since T has rank 2, such a form exists and is unique, up to multiplication by an element of $\mathcal{O}_0^*$. This implies that if u is an automorphism of T then

$$e_0(ux, uy) = \det(u) \cdot e_0(x, y) \quad \forall x, y \in T.$$

Consider the 2-dimensional $\mathcal{O}_0 \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = F_0$-vector space

$$V = V_\ell := T \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

and extend e_0 by F_0-linearity to the alternating nondegenerate F_0-bilinear form

$$V \times V \to F_0,$$

which we continue to denote e_0. Clearly, if $u \in \mathrm{Aut}_{F_0}(V)$, then

$$e_0(ux, uy) = \det(u) \cdot e_0(ux, uy) \quad \forall x, y \in V.$$

Here and above

$$\det\colon \mathrm{Aut}_{F_0}(V) \cong \mathrm{GL}(2, F_0) \to F_0^*$$

is the determinant homomorphism.

Lemma 3.2. *The alternating $\mathbb{Z}_\ell$-bilinear form*

$$e = e_\ell\colon T \times T \to \mathbb{Z}_\ell,\ x, y \mapsto \mathrm{Tr}_0(\pi^{-d} e_0(x, y))$$

is unimodular.

Proof. Let $l\colon T \to \mathbb{Z}_\ell$ be a $\mathbb{Z}_\ell$-linear map. We need to prove that there is exactly one $z \in T$ such that

$$l(x) = \mathrm{Tr}_0(\pi^{-d} e_0(x, z)) \quad \forall x \in T.$$

In order to do that, we choose a basis $\{f_1, f_2\}$ of the free $\mathcal{O}_0$-module T. Then l gives rise (and is uniquely determined by) two $\mathbb{Z}_\ell$-linear maps

$$l_i\colon R \to \mathbb{Z}_\ell, \quad a \mapsto l(a \cdot e_i)$$

for $i = 1, 2$. We have

$$l(a_1 f_1 + a_2 f_2) = l_1(a_1) + l_2(a_2) \quad \forall a_1, a_2 \in \mathcal{O}_0.$$

Since $\widetilde{B}_{\mathrm{Tr}}$ is unimodular, there exists exactly one $c_i \in \mathcal{O}_0$ with

$$l_i(a) = \widetilde{B}_{\mathrm{Tr}}(a, c_i) \quad \forall a \in \mathcal{O}$$

for $i = 1, 2$. This implies that

$$\begin{aligned} l(a_1 f_1 + a_2 f_2) &= \widetilde{B}_{\mathrm{Tr}}(a_1, c_1) + \widetilde{B}_{\mathrm{Tr}}(a_2, c_2) \\ &= \mathrm{Tr}_0(\pi^{-d} \cdot a_1 c_1) + \mathrm{Tr}_0(\pi^{-d} \cdot a_2 c_2) = \mathrm{Tr}_0(\pi^{-d} \cdot [a_1 c_1 + a_2 c_2]). \end{aligned}$$

Since e_0 is unimodular, there is exactly one $z \in T$ with

$$e_0(f_1, z) = c_1, \quad e_0(f_2, z) = c_2.$$

This implies that

$$e_0(a_1 f_1 + a_2 f_2, z) = a_1 c_1 + a_2 c_2$$

and therefore

$$l(a_1 f_1 + a_2 f_2, z) = \mathrm{Tr}_0[\pi^{-d} \cdot e_0(a_1 f_1 + a_2 f_2, z)] = e(a_1 f_1 + a_2 f_2, z). \qquad \square$$

3.3. Let $C = C_\ell$ be a 2-dimensional commutative semisimple F_0-algebra. Then C is either a quadratic field extension F of F_0 or is isomorphic (as an F_0-algebra) to the direct sum $F_0 \oplus F_0$. Suppose that $R = R_\ell \subset C$ is an $\mathcal{O}_0$-subalgebra of C that is a free $\mathcal{O}_0$-module of rank 2. Clearly, the natural homomorphism of $\mathcal{O}_0$-algebras

$$R \otimes_{\mathcal{O}_0} F \to C, \quad x \otimes a \mapsto ax$$

is an isomorphism.

Suppose that $C = F$ is a field (that is a quadratic extension of F_0). Then $\mathcal{O}_0 \subset R \subset \mathcal{O}$ where $\mathcal{O}$ is the ring of integers in the ℓ-adic field F. This implies that there is a nonnegative integer i such that

$$R = R_i := \mathcal{O}_0 + \pi^i \mathcal{O} \subset \mathcal{O} = R_0.$$

Conversely, for any nonnegative integer i the $\mathcal{O}_0$-(sub)algebra $\mathcal{O}_0+\pi^i\mathcal{O}\subset C$ is a free $\mathcal{O}_0$-module of rank 2.

Suppose that $C:=F_0\oplus F_0$ and let us put

$$\mathcal{O}:=\mathcal{O}_0\oplus\mathcal{O}_0\subset F_0\oplus F_0=C.$$

We view $\mathcal{O}_0$ as a $\mathcal{O}_0$-subalgebra of $\mathcal{O}$ via the diagonal embedding. Then

$$\mathcal{O}_0\subset R\subset\mathcal{O}.$$

This implies that there is a nonnegative integer such that

$$R=R_i:=\mathcal{O}_0+\pi^i\mathcal{O}\subset\mathcal{O}=R_0.$$

Conversely, for any nonnegative integer i the $\mathcal{O}$-(sub)algebra $\mathcal{O}_0+\pi^i\mathcal{O}\subset C$ is a free $\mathcal{O}_0$-module of rank 2.

We fix an isomorphism $T\cong R$ of free $\mathcal{O}_0$-modules of rank 2. This provides T with the natural structure of free R-module of rank 1 and gives rise to the embedding of R-algebras

$$R\hookrightarrow \mathrm{End}_{\mathcal{O}_0}(T),$$

which extends by F_0-linearity the embedding of F_0-algebras

$$C=R\otimes_{\mathcal{O}_0}F_0\hookrightarrow \mathrm{End}_{\mathcal{O}_0}(T)\otimes_{\mathcal{O}_0}F=\mathrm{End}_{F_0}(T\otimes_{\mathcal{O}_0}F)=\mathrm{End}_{F_0}(V).$$

Further we will identify C with its image in $\mathrm{End}_{F_0}(V)$. Clearly, V becomes a free C-module of rank 1. In particular, the centralizer of C in $\mathrm{End}_{F_0}(V)$ coincides with C. Since T is a free R-module of rank 1, the centralizer of C in $\mathrm{End}_{\mathcal{O}_0}(T)\subset\mathrm{End}_{F_0}(V)$ coincides with

$$R\subset C\subset\mathrm{End}_{F_0}(V).$$

Actually, we can do better and view V as the $2g$-dimensional $\mathbb{Q}_\ell$-vector space and T as the $\mathbb{Z}_\ell$-lattice of rank $2g$ in V. Indeed, C is a finite-dimensional semisimple $\mathbb{Q}_\ell$-algebra of $\mathbb{Q}_\ell$-dimension $2g$ that acts faithfully on the $2g$-dimensional $\mathbb{Q}_\ell$-vector space V. This implies that the centralizer of C even in $\mathrm{End}_{\mathbb{Q}_\ell}(V)$ coincides with C and the centralizer of C in $\mathrm{End}_{\mathbb{Z}_\ell}(T)\subset\mathrm{End}_{\mathbb{Q}_\ell}(V)$ coincides with

$$R\subset C\subset\mathrm{End}_{\mathbb{Q}_\ell}(V)$$

(recall that T is a free R-module of rank 1 and therefore the centralizer of R in $\mathrm{End}_{\mathbb{Z}_\ell}(T)$ coincides with R). If

$$u\in C^*\subset\mathrm{Aut}_{F_0}(V)$$

and $c=\det(u)\in F_0^*$ actually lies in $\mathbb{Q}_\ell^*$ then

$$\begin{aligned}e(ux,uy)&=\mathrm{Tr}_0(\pi^{-d}e_0(ux,uy))\\&=\mathrm{Tr}_0(\pi^{-d}c\cdot e_0(x,y))=c\cdot\mathrm{Tr}_0(\pi^{-d}\cdot e_0(x,y))=c\cdot e(x,y)\end{aligned}$$

for all $x,y\in V$. This implies that u lies in the group $\mathrm{Gp}(V,e)$ of symplectic similitudes.

Lemma 3.4. *There exists*

$$\mathbf{u}=\mathbf{u}_\ell\in C^*=C_\ell^*$$

that lies in $\mathrm{Gp}(V,e)=Gp(V_\ell,e_\ell)$ *and such that*

$$\mathbb{Q}_\ell[\mathbf{u}_\ell]=\mathbb{Q}_\ell[\mathbf{u}]=C=C_\ell.$$

In particular, the centralizer of $\mathbf{u}_\ell$ *in* $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell)\subset\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell)$ *coincides with*

$$R=R_\ell\subset C\subset\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell).$$

Proof. Suppose that C is a quadratic overfield F of F_0. Let τ be the only nontrivial element (involution of $\mathrm{Gal}(F/F_0)$. Then V becomes a one-dimensional vector space over F but we view V as a 2-dimensional F_0-vector space and each $u \in F$ acts on V as an F_0-linear operator that is multiplication by u. Then the determinant $\det(u)$ of this operator is the *norm* of u with respect to F/F_0, i.e,,

$$\det(u) = u \cdot \tau(u).$$

This implies that if $u \cdot \tau(u) = 1$ then u lies in the symplectic group $\mathrm{Sp}(V, e) \subset \mathrm{Gp}(V, e)$. So, we need to find $\mathbf{u} \in F^*$ with

$$\mathbf{u} \cdot \tau\mathbf{u} = 1, \quad \mathbb{Q}_\ell[\mathbf{u}] = F.$$

But the existence of such $\mathbf{u}$ is guaranteed by Lemma 2.2 and we are done.

Suppose that $C = F_0 \oplus F_0$. Let

$$u = (u_1, u_2) \in F_0^* \times F_0^* = C^*.$$

Clearly $\det(u) = u_1 u_2 \in F_0^*$. This implies that if $u_2 = u_1^{-1}$ then

$$\det(u) = u_1 u_2 = u_1 u_1^{-1} = 1$$

and u lies in the symplectic group $\mathrm{Sp}(V, e) \subset \mathrm{Gp}(V, e)$. By Lemma 2.3, there exists a nonzero $u_1 \in F_0$ with $\mathbb{Q}_\ell[u_1] = F_0$. Replacing u_1 by $\ell^N u_1$ for sufficiently large positive integer N, we may and will assume that

$$0 \neq u_1 \in \ell\mathcal{O}_0 \subset \pi\mathcal{O}_0$$

and therefore $u_1^{-1} \notin \mathcal{O}_0$. This implies that the degree g *minimal polynomial* $P_1(t) \in \mathbb{Q}_\ell[t]$ of u_1 over $\mathbb{Q}_\ell$ has coefficients in $\mathbb{Z}_\ell$, which is not the case for the degree g (monic) *minimal polynomial* $P_2(t) \in \mathbb{Q}_\ell[t]$ of $u_2 = u_1^{-1}$ over $\mathbb{Q}_\ell$. Since both P_1 and P_2 are monic irreducible over $\mathbb{Q}_\ell$, they are relatively prime. This implies that if we put $\mathbf{u} = (u_1, u_1^{-1}) \in F_0 \oplus F_0$ then the $\mathbb{Q}_\ell$-(sub)algebra $\mathbb{Q}_\ell[\mathbf{u}]$ of $F_0 \oplus F_0$ is isomorphic to the quotient $\mathbb{Q}_\ell[t]/P_1(t)P_2(t)\mathbb{Q}_\ell[t]$ and therefore has $\mathbb{Q}_\ell$-dimension

$$\deg(P_1 P_2) = g + g = 2g = \dim_{\mathbb{Q}_\ell}(F_0 \oplus F_0)$$

and therefore

$$\mathbb{Q}_\ell[\mathbf{u}] = F_0 \oplus F_0 = C. \qquad \square$$

§4. Linear algebraic groups over $\mathbb{Q}_\ell$

The content of this section was inspired by exercises in Serre's book [15, Chapter IV, Section 2.2].

4.1. Let V be a vector space of finite positive dimension d over $\mathbb{Q}_\ell$. We write Id for the identity automorphism of V. Let T be a $\mathbb{Z}_\ell$-lattice in V of (maximal) rank d. For every $u \in \mathrm{End}_{\mathbb{Q}_\ell}(V)$ we write $\mathfrak{Z}(u)$ for its centralizer in $\mathrm{End}_{\mathbb{Q}_\ell}(V)$ and $\mathbb{Q}_\ell[u]$ for the $\mathbb{Q}_\ell$-subalgebra in $\mathrm{End}_{\mathbb{Q}_\ell}(V)$ generated by u. We have

$$\mathrm{Id}, u \in \mathbb{Q}_\ell[u] \subset \mathfrak{Z}(u) \subset \mathrm{End}_{\mathbb{Q}_\ell}(V).$$

Consider the intersection

$$\mathfrak{Z}(u)_0 := \mathfrak{Z}(u) \cap \mathrm{End}_{\mathbb{Z}_\ell}(T) \subset \mathrm{End}_{\mathbb{Z}_\ell}(T) \subset \mathrm{End}_{\mathbb{Q}_\ell}(V).$$

Clearly, $\mathfrak{Z}(u)_0$ coincides with the centralizer of u in $\mathrm{End}_{\mathbb{Z}_\ell}(T) \subset \mathrm{End}_{\mathbb{Q}_\ell}(V)$. It is also clear that $\mathfrak{Z}(u)_0$ is a $\mathbb{Z}_\ell$-subalgebra (order) in $\mathfrak{Z}(u)$ and the natural map

$$\mathfrak{Z}(u)_0 \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \to \mathfrak{Z}(u), \quad u \otimes c \mapsto cu$$

is an isomorphism of $\mathbb{Q}_\ell$-algebras.

If $u \in \mathrm{End}_{\mathbb{Q}_\ell}(V)$ then we consider its characteristic polynomial

$$P_u(t) = \det(t\,\mathrm{Id} - u, V) \in \mathbb{Q}_\ell[t]$$

and define $\Delta(u) \in \mathbb{Q}_\ell$ as the *discriminant* of $P_u(t)$. For each $g \in \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$

$$P_{gug^{-1}}(t) = P_u(t), \quad \Delta(gug^{-1}) = \Delta(u).$$

The polynomial $P_u(t)$ has *no* multiple roots if and only if $\Delta(u) \neq 0$. If this is the case then u is a semisimple (diagonalizable over $\overline{\mathbb{Q}}_\ell$) linear operator in V, the subalgebra

$$\mathbb{Q}_\ell[u] \subset \mathrm{End}_{\mathbb{Q}_\ell}(V)$$

is a commutive semisimple $\mathbb{Q}_\ell$-(sub)algebra of $\mathbb{Q}_\ell$-dimension d, which coincides with $\mathfrak{Z}(u)$.

Let $\mathfrak{G} \subset \mathrm{GL}(V)$ be a connected reductive linear (sub)group of positive dimension. Clearly $\mathfrak{G}(\mathbb{Q}_\ell)$ is a closed subgroup of $\mathrm{Aut}_{\mathbb{Q}_\ell}(V)$ with respect to the ℓ-adic topology. One may view

$$\Delta \colon u \mapsto \Delta(u)$$

as a regular function on the affine algebraic variety $\mathfrak{G}$. We assume that Δ is *not* identically zero on $\mathfrak{G}$.

Lemma 4.2. *Let G be an open compact subgroup in $\mathfrak{G}(\mathbb{Q}_\ell)$. Then the subset*

$$G_\Delta := G \cap \{\Delta = 0\} \subset G$$

has measure zero with respect to the Haar measure on G.

Proof. The group G carries the natural structure of an open compact ℓ-adic subgroup of $\mathfrak{G}(\mathbb{Q}_\ell)$; in addition, if N is the dimension of G then N coincides with the dimension of $\mathfrak{G}$. Clearly, every nonempty open (with respect to the ℓ-adic topology) subset of G is dense in $\mathfrak{G}$ with respect to the Zariski topology. This implies that the *interior* of G_Δ with respect to the ℓ-adic topology is *empty*. Notice that G_Δ is a closed *analytical subspace* of G that is stable under conjugation. It is known [17, Section 4.2] that there is a positive integer a such that for each positive integer n there is an open subgroup $G(n)$ in G with index

$$(G : G(n)) = a\ell^{nN}.$$

In addition, there is a positive integer b such that the image C_n of G_Δ in the finite group $G/G(n)$ consists of at most $b\ell^{n(N-1)}$ elements ([17, Example at the end of Section 4.1 and formula (73) of Section 4.2]). Since the (normalized) Haar measure of each coset of the subgroup $G(n)$ in G is $1/(G : G(n))$, we conclude that the Haar measure of G_Δ does not exceed

$$m(n) = \frac{b\ell^{n(N-1)}}{a\ell^{nN}}.$$

Since $m(n)$ tends to 0 while n tends to ∞, the Haar measure of G_Δ is zero. $\square$

4.3. Let $\mathbf{u}$ be an element of $\mathfrak{G}(\mathbb{Q}_\ell)$ with $\Delta(\mathbf{u}) \neq 0$, i,e., $P_{\mathbf{u}}(t)$ has *no* multiple roots. Then $\mathbf{u}$ is semisimple and regular in $\mathrm{GL}(V)$ and therefore is a semisimple regular element of $\mathfrak{G}$. Recall that the subalgebra

$$\mathbb{Q}_\ell[\mathbf{u}] \subset \mathrm{End}_{\mathbb{Q}_\ell}(V)$$

is a commutative semisimple d-dimensional $\mathbb{Q}_\ell$-(sub)algebra that coincides with $\mathfrak{Z}(\mathbf{u})$.

Let $\mathfrak{T}$ be the *maximal torus* in $\mathfrak{G}$ that contains (regular) $\mathbf{u}$. Since such a $\mathfrak{T}$ is unique [3, Chapter IV, Section 12.2], it is defined over $\mathbb{Q}_\ell$ and we have

$$\mathbf{u} \in \mathfrak{T}(\mathbb{Q}_\ell) \subset \mathfrak{G}(\mathbb{Q}_\ell) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V).$$

Consider the subset $\mathfrak{T}'(\mathbf{u}) \subset \mathfrak{T}(\mathbb{Q}_\ell)$ that consists of all

$$u \in \mathfrak{T}(\mathbb{Q}_\ell) \subset \mathfrak{G}(\mathbb{Q}_\ell) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$$

such that $\Delta(u) \neq 0$. Clearly, $\mathfrak{T}'(\mathbf{u})$ is open everywhere dense in $\mathfrak{T}(\mathbb{Q}_\ell)$ with respect to the ℓ-adic topology, it contains $\mathbf{u}$ and all its elements are semisimple regular in $\mathfrak{G}$ and commute with $\mathbf{u}$. Then for each $u \in \mathfrak{T}'(\mathbf{u})$

$$\mathfrak{Z}(u) \subset \mathrm{End}_{\mathbb{Q}_\ell}(V)$$

is also a commutative semisimple $\mathbb{Q}_\ell$-(sub)algebra of $\mathbb{Q}_\ell$-dimension d that coincides with $\mathbb{Q}_\ell[u]$; it also contains $\mathbf{u}$ and therefore contains $\mathbb{Q}_\ell[\mathbf{u}]$, which is also d-dimensional. This implies that

$$\mathbb{Q}_\ell[u] = \mathfrak{Z}(u) = \mathfrak{Z}(\mathbf{u}) = \mathbb{Q}_\ell[\mathbf{u}] \subset \mathrm{End}_{\mathbb{Q}_\ell}(V)$$

and therefore

$$\mathfrak{Z}(u)_0 = \mathfrak{Z}(\mathbf{u})_0 \subset \mathrm{End}_{\mathbb{Z}_\ell}(T)$$

for all $u \in \mathfrak{T}'(\mathbf{u})$.

Let us consider the map of ℓ-adic manifolds

$$\Psi_{\mathbf{u}} \colon \mathfrak{G}(\mathbb{Q}_\ell) \times \mathfrak{T}'(\mathbf{u}) \to \mathfrak{G}(\mathbb{Q}_\ell), \quad (g, u) \mapsto gug^{-1}.$$

Clearly, Δ does *not* vanish on the image of Ψ.

It is known ([6, p. 469, Proof of Theorem 2.1], see also [8, Proof of Proposition 7.3]) that the *tangent map* to $\Psi_{\mathbf{u}}$ is everywhere *surjective* (recall that every $u \in \mathfrak{T}'(\mathbf{u})$ is regular in $\mathfrak{G}$). This implies that $\Psi_{\mathbf{u}}$ is an *open map*, i.e., the image under $\Psi_{\mathbf{u}}$ of any open subset of $\mathfrak{G}(\mathbb{Q}_\ell) \times \mathfrak{T}'(\mathbf{u})$ is open in $\mathfrak{G}(\mathbb{Q}_\ell)$. In particular, if G is an open compact subgroup in $\mathfrak{G}(\mathbb{Q}_\ell)$ then $\mathfrak{T}'(\mathbf{u})_G = \mathfrak{T}'(\mathbf{u}) \cap G$ is a (nonempty) open subset in G whose closure contains Id and therefore the image $\Psi_{\mathbf{u}}(\mathfrak{T}'(\mathbf{u})_G \times G)$ is an open subset in G whose closure contains Id. Notice that

$$\mathfrak{Z}(gug^{-1}) = g\mathfrak{Z}(u)g^{-1} \quad \forall g \in G.$$

If, moreover,

$$G \subset \mathrm{Aut}_{\mathbb{Z}_\ell}(T) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$$

then

$$\mathfrak{Z}(gug^{-1})_0 = g\mathfrak{Z}(u)_0 g^{-1} = g\mathfrak{Z}(\mathbf{u})_0 g^{-1} \quad \forall g \in G.$$

In particular, the $\mathbb{Z}_\ell$-algebras $\mathfrak{Z}(gug^{-1}))_0$ and $\mathfrak{Z}(\mathbf{u})_0$ are isomorphic. In addition, if $\mathbf{u} \in G$ then

$$\mathbf{u} \in \Psi_{\mathbf{u}}(\mathfrak{T}'(\mathbf{u})_G \times G).$$

Theorem 4.4. *Let G be an open compact subgroup in $\mathfrak{G}(\mathbb{Q}_\ell)$ that lies in*

$$\mathrm{Aut}_{\mathbb{Z}_\ell}(T) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V).$$

Let $\mathbf{u}$ be an element of $\mathfrak{G}(\mathbb{Q}_\ell)$ such that its characteristic polynomial

$$P_{\mathbf{u}}(t) = \det(t\,\mathrm{Id} - \mathbf{u}, V) \in \mathbb{Q}_\ell[t]$$

has no multiple roots. Let us consider the set $X(\mathbf{u}, T, G)$ of all elements $u \in G$ such that the $\mathbb{Z}_\ell$-algebra $\mathfrak{Z}(u)_0$ is isomorphic to $\mathfrak{Z}(\mathbf{u})_0$. Then $X(\mathbf{u}, T, G)$ is a nonempty open subset in G that is stable under conjugation. Its boundary lies in G_Δ and contains Id.

Remark 4.5. Suppose that $\mathbf{u}_1$ and $\mathbf{u}_2$ are elements of $\mathfrak{G}(\mathbb{Q}_\ell)$ with

$$\Delta(\mathbf{u}_1) \neq 0, \quad \Delta(\mathbf{u}_2) \neq 0.$$

Consider elements

$$u_1 \in X(\mathbf{u}_1, T, G), \quad u_2 \in X(\mathbf{u}_2, T, G).$$

We have isomorphisms of $\mathbb{Z}_\ell$-algebras

$$\mathfrak{Z}(\mathbf{u}_1)_0 \cong \mathfrak{Z}(u_1)_0, \quad \mathfrak{Z}(\mathbf{u}_2)_0 \cong \mathfrak{Z}(u_2)_0.$$

This implies that either $\mathfrak{Z}(\mathbf{u}_1)_0$ and $\mathfrak{Z}(\mathbf{u}_2)_0$ are *isomorphic* and

$$u_1 \in X(\mathbf{u}_2, T, G), \quad u_2 \in X(\mathbf{u}_1, T, G)$$

or they are *not* isomorphic and

$$u_1 \notin X(\mathbf{u}_2, T, G), \quad u_2 \notin X(\mathbf{u}_1, T, G).$$

It follows that the subsets $X(\mathbf{u}_1, T, G)$, and $X(\mathbf{u}_2, T, G)$ either *coincide* or do *not* meet each other.

Proof of Theorem 4.4. It is clear that $X(\mathbf{u}, T, G)$ is stable under conjugation, $\mathbf{u}$ lies in $X(\mathbf{u}, T, G)$ while Id does *not* belong to $X(\mathbf{u}, T, G)$. In the notation above, $\Psi_{\mathbf{u}}(\mathfrak{T}'(\mathbf{u})_G \times G)$ is an open subset in G whose closure contains Id (and therefore Id lies on the boundary) and such that for each $u \in \Psi_{\mathbf{u}}(\mathfrak{T}'_G \times G)$ the $\mathbb{Z}_\ell$-algebra $\mathfrak{Z}(u)_0$ is isomorphic to $\mathfrak{Z}(\mathbf{u})_0$. This implies that $X(\mathbf{u}, T, G)$ contains open $\Psi_{\mathbf{u}}(\mathfrak{T}'(\mathbf{u})_G \times G) \subset G$. In particular, $X(\mathbf{u}, T, G)$ is nonempty and its closure in G contains Id. It remains to prove that $X(\mathbf{u}, T, G)$ is open. Let u_1 be an element of $X(\mathbf{u}, T, G)$. Clearly,

$$X(\mathbf{u}, T, G) = X(u_1, T, G).$$

On the other hand, the centralizer $\mathfrak{Z}(u_1)$ of u_1 in $\mathrm{End}_{\mathbb{Q}_\ell}(V)$ is isomorphic to $\mathfrak{Z}(\mathbf{u})$, i.e., is a semisimple commutative $\mathbb{Q}_\ell$-algebra of $\mathbb{Q}_\ell$-dimension d where $d = \dim_{\mathbb{Q}_\ell}(V)$. This means that the characteristic polynomial of u_1 has no multiple roots and therefore (replacing $\mathbf{u}$ by u_1) we may define $\mathfrak{T}'(u_1)$, Ψ_{u_1}, and $\mathfrak{T}'(u_1)_G$. Since u_1 is an element of G, it lies in the open subset $\Psi_{u_1}(\mathfrak{T}'(\mathbf{u})_G \times G)$ of G. On the other hand,

$$\Psi_{u_1}(\mathfrak{T}'(\mathbf{u})_G \times G) \subset X(u_1, T, G) = X(\mathbf{u}, T, G)$$

which proves the openness of $X(\mathbf{u}, T, G)$.

We still have to check that Δ vanishes identically on the boundary of $X(\mathbf{u}, T, G)$. In order to do that, recall (Remark 4.5) that if

$$u \in G, \quad \Delta(u) \neq 0$$

then either $X(\mathbf{u}, T, G) = X(u, T, G)$ or these two open subsets of G do *not* meet each other. Taking into account that $u \in X(u, T, G)$, we obtain that

$$\{G \setminus G_\Delta\} \setminus X(\mathbf{u}, T, G)$$

coincides with the union of all (open) $X(u, T, G)$ where u runs through the (same!) set $\{G \setminus G_\Delta\} \setminus X(\mathbf{u}, T, G)$. This implies that $G \setminus \{G_\Delta \cup X(\mathbf{u}, T, G)\}$ is an *open* subset in G that obviously does *not* meet $X(\mathbf{u}, T, G)$. This implies that the closure of $X(\mathbf{u}, T, G)$ lies in

$$X(\mathbf{u}, T, G) \cup G_\Delta.$$

Since $X(\mathbf{u}, T, G)$ is open, its boundary lies in G_Δ. On the other hand, we saw in Subsection 4.3 that Id lies in the closure of $X(\mathbf{u}, T, G)$ but not in $X(\mathbf{u}, T, G)$. This implies that Id lies on the boundary of $X(\mathbf{u}, T, G)$. □

Example 4.6. Suppose that $\mathfrak{G} = \mathrm{GL}(V)$. Let C be a d-dimensional semisimple commutative $\mathbb{Q}_\ell$-algebra and $R \subset C$ an order in C, i.e., a $\mathbb{Z}_\ell$-subalgebra of C (with the same 1) that is a free $\mathbb{Z}_\ell$-module of rank d. By Lemma 2.3, there exists $\mathbf{u} \in C^*$ such that $C = \mathbb{Q}_\ell[\mathbf{u}]$. We fix an isomorphism of free $\mathbb{Z}_\ell$-modules $R \cong T$ and use it in order to provide T with the structure of a free R-module of rank 1. Tensoring by $\mathbb{Q}_\ell$, we obtain the natural structure of a $R \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = C$-module on $T \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = V$. This gives us the $\mathbb{Q}_\ell$-algebra embedding $C \hookrightarrow \mathrm{End}_{\mathbb{Q}_\ell}(V)$ in such a way that $R \subset C$ lands in $\mathrm{End}_{\mathbb{Z}_\ell}(T) \subset \mathrm{End}_{\mathbb{Q}_\ell}(V)$. Further we will identify C and R with their images in $\mathrm{End}_{\mathbb{Q}_\ell}(V)$ and $\mathrm{End}_{\mathbb{Z}_\ell}(T)$ respectively. (In particular, we may view $\mathbf{u}$ as an element of $C^* \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$.) Since $\mathbf{u}$ lies in semisimple commutative $C \subset \mathrm{End}_{\mathbb{Q}_\ell}(V)$, it is a semisimple linear operator in V.

This provides V with the natural structure of a free C-module of rank 1; in particular, the centralizer $\mathrm{End}_C(V)$ of C in $\mathrm{End}_{\mathbb{Q}_\ell}(V)$ coincides with C. Similarly, T becomes a free R-module of rank 1 and the centralizer $\mathrm{End}_R(T)$ of R in $\mathrm{End}_{\mathbb{Z}_\ell}(T)$ coincides with R. It follows that the centralizer of $\mathbf{u}$ in $\mathrm{End}_{\mathbb{Q}_\ell}(V)$ coincides with C and therefore the centralizer $\mathfrak{Z}(\mathbf{u})_0$ of $\mathbf{u}$ in $\mathrm{End}_{\mathbb{Z}_\ell}(T) \subset \mathrm{End}_{\mathbb{Q}_\ell}(V)$ coincides with R. In particular, the $\mathbb{Q}_\ell$-dimension of the centralizer of semisimple $\mathbf{u}$ in $\mathrm{End}_{\mathbb{Q}_\ell}(V)$ coincides with $\dim_{\mathbb{Q}_\ell}(V)$ and therefore the characteristic polynomial of $\mathbf{u}$ has *no* multiple roots.

Let $\mathbf{X}(R,T,G)$ be the set of all $u \in G$ such that $\mathfrak{Z}(u)_0$ is isomorphic as a $\mathbb{Z}_\ell$-algebra to R. Then

$$\mathbf{X}(R,T,G) = X(\mathbf{u},T,G).$$

From Theorem 4.4 it follows that $\mathbf{X}(R,T,G)$ is an open nonempty subset of G, whose closure contains the identity element and the boundary has measure zero with respect to the Haar measure on G.

Example 4.7. Suppose $d = 2g$ is even, $\mathcal{C}$ is a g-dimensional semisimple commutative $\mathbb{Q}_\ell$-algebra and $\mathcal{R} \subset \mathcal{C}$ is an order in $\mathcal{C}$. Let $\mathcal{T}$ be a a free $\mathcal{R}$-module of rank 1. Then $\mathcal{V} = \mathcal{T} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is a free $\mathcal{R} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = \mathcal{C}$-module of rank 1. We may view $\mathcal{T}$ as a rank g $\mathbb{Z}_\ell$-lattice (and a $\mathcal{R}$-submodule) in $\mathcal{V}$. Consider the free $\mathcal{R}$-module $\mathbf{T} = \mathcal{T} \oplus \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{T}, \mathbb{Z}_\ell)$ of rank 2, which is a rank $2g$ $\mathbb{Z}_\ell$-lattice in the $2g$-dimensional vector space $\mathbf{V} = \mathcal{V} \oplus \mathrm{Hom}_{\mathbb{Q}_\ell}(\mathcal{V}, \mathbb{Q}_\ell)$. Notice that $\mathbf{V}$ carries the natural structure of a free $\mathcal{C}$-module of rank 2 and we have a natural embedding

$$\begin{aligned} \mathcal{C} \oplus \mathcal{C} &\hookrightarrow \mathrm{End}_{\mathbb{Q}_\ell}(\mathcal{V}) \oplus \mathrm{End}_{\mathbb{Q}_\ell}(\mathrm{Hom}_{\mathbb{Q}_\ell}(\mathcal{V}, \mathbb{Q}_\ell)) \\ &\subset \mathrm{End}_{\mathbb{Q}_\ell}[\mathcal{V} \oplus \mathrm{Hom}_{\mathbb{Q}_\ell}(\mathcal{V}, \mathbb{Q}_\ell)] = \mathrm{End}_{\mathbb{Q}_\ell}(\mathbf{V}) \end{aligned}$$

such that each $(u_1, u_2) \in \mathcal{C} \oplus \mathcal{C}$ sends $(x, l) \in \mathcal{V} \oplus \mathrm{Hom}_{\mathbb{Q}_\ell}(\mathcal{V}, \mathbb{Q}_\ell)$ to $(u_1 x, l u_2)$. Further we will identify $\mathcal{C} \oplus \mathcal{C}$ with its image in $\mathrm{End}_{\mathbb{Q}_\ell}(\mathbf{V})$. Under this identification the subring $\mathcal{R} \oplus \mathcal{R} \subset \mathcal{C} \oplus \mathcal{C}$ lands in

$$\mathrm{End}_{\mathbb{Z}_\ell}(\mathcal{T}) \oplus \mathrm{End}_{\mathbb{Z}_\ell}(\mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{T}, \mathbb{Z}_\ell)) \subset \mathrm{End}_{\mathbb{Z}_\ell}(\mathcal{T} \oplus \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{T}, \mathbb{Z}_\ell)) = \mathrm{End}_{\mathbb{Z}_\ell}(\mathbf{T}).$$

Clearly, $\mathcal{C} \oplus \mathcal{C}$ coincides with its own centralizer in $\mathrm{End}_{\mathbb{Q}_\ell}(\mathbf{V})$ and $\mathcal{R} \oplus \mathcal{R}$ coincides with its own centralizer in $\mathrm{End}_{\mathbb{Z}_\ell}(\mathbf{T})$. Notice that the $\mathbb{Q}_\ell$-dimensions of $\mathcal{C} \oplus \mathcal{C}$ and $\mathbf{V}$ do coincide.

There is a perfect alternating $\mathbb{Z}_\ell$-bilinear form

$$e \colon \mathbf{T} \times \mathbf{T} \to \mathbb{Z}_\ell, \quad (x_1, l_1), (x_2, l_2) \mapsto l_1(x_2) - l_2(x_1)$$

for all

$$x_1, x_2 \in \mathcal{T}, \quad l_1, l_2 \in \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{T}, \mathbb{Z}_\ell).$$

This form extends by $\mathbb{Q}_\ell$-linearity to the nondegenerate alternating $\mathbb{Q}_\ell$-bilinear form

$$\mathbf{V} \times \mathbf{V} \to \mathbb{Q}_\ell, \quad (x_1, l_1), (x_2, l_2) \mapsto l_1(x_2) - l_2(x_1)$$

$$\forall x_1, x_2 \in \mathcal{V}, \quad l_1, l_2 \in \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{V}, \mathbb{Q}_\ell),$$

which we also denote by e.

Let $\mathfrak{G} = \mathfrak{Gp}(\mathbf{V}, e) \subset \mathrm{GL}(\mathbf{V})$ be the (connected) reductive algebraic $\mathbb{Q}_\ell$-group of symplectic similitudes of $\mathbf{V}$ attached to e. We have

$$\mathfrak{G}(\mathbb{Q}_\ell) = \mathfrak{Gp}(\mathbf{V}, e)(\mathbb{Q}_\ell) = \mathrm{Gp}(\mathbf{V}, e).$$

If $u_1 \in \mathcal{C}^*$ and $q \in \mathbb{Q}_\ell^*$ then the element $(u_1, q u_1^{-1}) \in (\mathcal{C} \oplus \mathcal{C})^* \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(\mathbf{V})$ lies in $\mathrm{Gp}(\mathbf{V}, e)$. When $q = 1$ this element lies in $\mathrm{Sp}(\mathbf{V}, e)$.

Using Example 4.6, choose $u_1 \in \mathcal{C}^* \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(\mathcal{V})$ such that the characteristic polynomial $P_{u_1}(t)$ has no multiple roots, $\mathbb{Q}_\ell[u_1] = \mathcal{C}$ and the centralizer $\mathfrak{Z}[u_1]_0$ of u_1 in $\mathrm{End}_{\mathbb{Z}_\ell}(\mathcal{T}) \subset \mathrm{End}_{\mathbb{Q}_\ell}(\mathcal{V})$ coincides with $\mathcal{R}$. We may choose q in such a way that the characteristic polynomial $P_{q u_1^{-1}}(t) = (t/q)^g P_{u_1}(q/t)$ of $q u_1^{-1}$ has no common roots with $P_u(t)$.

(For example, pick an integer N such that none of the roots of $P_u(t)$ is of the form $\pm\ell^N$ and put $q = \ell^{2N}$.) Then the characteristic polynomial of

$$\mathbf{u} = (u_1, qu_1^{-1}) \in (\mathcal{C} \oplus \mathcal{C})^* \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(\mathbf{V})$$

coincides with the product $(t/q)^g P_{u_1}(q/t) \cdot P_{u_1}(t)$ and therefore has no multiple roots. It follows that $\mathbb{Q}_\ell[\mathbf{u}] = \mathcal{C} \oplus \mathcal{C}$ and therefore the centralizer of $\mathbf{u}$ in $\mathrm{End}_{\mathbb{Q}_\ell}(\mathbf{V})$ coincides with $\mathcal{C} \oplus \mathcal{C}$ and therefore the centralizer $\mathfrak{Z}(\mathbf{u})_0$ of $\mathbf{u}$ in $\mathrm{End}_{\mathbb{Z}_\ell}(\mathbf{T}) \subset \mathrm{End}_{\mathbb{Q}_\ell}(\mathbf{V})$ coincides with $\mathcal{R} \oplus \mathcal{R}$.

Let $G \subset \mathrm{Aut}_{\mathbb{Z}_\ell}(\mathbf{T})$ be an open compact subgroup in $\mathrm{Gp}(\mathbf{V}, e)$. Let $\mathbf{X}(\mathcal{R} \oplus \mathcal{R}, \mathbf{T}, G)$ be the set of all $u \in G$ such that $\mathfrak{Z}(u)_0$ is isomorphic as a $\mathbb{Z}_\ell$-algebra to $\mathcal{R} \oplus \mathcal{R}$. Then

$$\mathbf{X}(\mathcal{R} \oplus \mathcal{R}, T, G) = X(\mathbf{u}, \mathbf{T}, G).$$

From Theorem 4.4 it follows that $\mathbf{X}(\mathcal{R} \oplus \mathcal{R}, \mathbf{T}, G)$ is an open nonempty subset of G whose closure contains the identity element and the boundary has measure zero with respect to the Haar measure on G.

Corollary 4.8. *Let $\mathcal{G}$ be a compact profinite topological group. Let $\mathbf{P}$ be a nonempty finite set of primes.*

Suppose that for each $\ell \in \mathbf{P}$ we are given the following data.

- *A $\mathbb{Q}_\ell$-vector space V_ℓ of finite positive dimension d_ℓ provided with a $\mathbb{Z}_\ell$-lattice $T_\ell \subset V_\ell$ of rank d_ℓ.*
- *A connected reductive linear algebraic subgroup $\mathfrak{G}_\ell \subset \mathrm{GL}(V_\ell)$ of positive dimension.*
- *An element*

$$\mathbf{u}_\ell \in \mathfrak{G}_\ell(\mathbb{Q}_\ell) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell)$$

such that its characteristic polynomial

$$P_{\mathbf{u}_\ell}(t) = \det(t\,\mathrm{Id} - \mathbf{u}_\ell, V) \in \mathbb{Q}_\ell[t]$$

has no multiple roots. We write $\mathfrak{Z}(\mathbf{u}_\ell)_0$ for the centralizer of $\mathbf{u}_\ell$ in $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell) \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell)$.

- *A continuous homomorphism of topological groups*

$$\rho_\ell \colon \mathcal{G} \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell),$$

whose image

$$G_\ell := \rho_\ell(\mathcal{G}) \subset \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell),$$

is an open subgroup in $\mathfrak{G}_\ell(\mathbb{Q}_\ell)$.

Consider the subset $Y_\ell \subset \mathcal{G}$ that consists of all $\sigma \in \mathcal{G}$ such that the centralizer $\mathfrak{Z}(\rho_\ell(\sigma))_0$ of $\rho_\ell(\sigma)$ in $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell) \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell)$ is isomorphic (as a $\mathbb{Z}_\ell$-algebra) to $\mathfrak{Z}(\mathbf{u}_\ell)_0$.

Consider the product-homomorphism

$$\rho := \prod_{\ell \in \mathbf{P}} \rho_\ell \colon \mathcal{G} \to \prod_{\ell \in \mathbf{P}} G_\ell, \quad \sigma \mapsto \{\rho_\ell(\sigma)\}_{\ell \in \mathbf{P}}.$$

Then the image $\rho(\mathcal{G})$ is an open subgroup of finite index in $\prod_{\ell \in \mathbf{P}} G_\ell$ and the intersection

$$Y := \bigcap_{\ell \in \mathbf{P}} Y_\ell \subset \mathcal{G}$$

of all Y_ℓ is an open nonempty subset in $\mathcal{G}$ that is stable under conjugation and its closure contains the identity element of $\mathcal{G}$.

Proof. Clearly, (every Y_ℓ and therefore) Y is stable under conjugation. From Theorem 4.4 it follows that every

$$X(\mathbf{u}_\ell, T_\ell, G_\ell) \subset G_\ell$$

is an open nonempty subset of G_ℓ and its closure contains the identity element of G_ℓ. Clearly,

$$Y_\ell = \rho_\ell^{-1}(X(\mathbf{u}_\ell, T_\ell, G_\ell)) \subset \mathcal{G}.$$

This implies that every Y_ℓ is an open nonempty subset in $\mathcal{G}$ and its closure contains the identity element of $\mathcal{G}$. This implies that Y is also open. It remains to check that Y is nonempty and its closure contains the identity element. In order to do that, notice that each G_ℓ contains an open subgroup of finite index that is a pro-ℓ-group. So, there is an open subgroup $\mathcal{G}_1$ of finite index in $\mathcal{G}$ such that $G_{\ell,1} := \rho_\ell(\mathcal{G}_1)$ is a pro-ℓ-group. Clearly, $G_{\ell,1}$ is a closed subgroup of finite index in G_ℓ and therefore is open in G_ℓ and therefore is open in $\mathfrak{G}_\ell(\mathbb{Q}_\ell)$ as well.

Let us consider the product-homomorphism

$$\rho_1 \colon \mathcal{G}_1 \to \prod_{\ell \in \mathbf{P}} G_{\ell,1}, \quad \sigma \mapsto \{\rho_\ell(\sigma)\}_{\ell \in \mathbf{P}}.$$

The image $\rho_1(\mathcal{G}_1) \subset \prod_{\ell \in \mathbf{P}} G_{\ell,1}$ is a compact subgroup that maps surjectively on each factor $G_{\ell,1}$. Since the $G_{\ell,1}$'s are pro-ℓ-groups for pairwise ℓ, we have

$$\rho_1(\mathcal{G}_1) = \prod_{\ell \in \mathbf{P}} G_{\ell,1},$$

i.e., ρ_1 is *surjective*. (Compare with [8, Proof of Proposition 7.1]. Actually, this argument goes back to Serre [15, Chapter IV, Section 2.2, Exercise 3c on pp. IV–14].) Since ρ_1 is *surjective*,

$$Y \cap \mathcal{G}_1 = \rho_1^{-1}(\prod_{\ell \in \mathbf{P}} X(\mathbf{u}_\ell, T_\ell, G_{\ell,1})) \subset \mathcal{G}_1$$

is nonempty (as the preimage of a nonempty subset) and its closure contains the identity element of $\mathcal{G}_1$. $\square$

Corollary 4.9. *We keep the notation and assumptions of Corollary* 4.8. *Assume additionally that $\mathcal{G}$ is a closed subgroup of $\prod_{\ell \in \mathbf{P}} G_\ell$ and $\rho_\ell \colon \mathcal{G} \to G_\ell$ coincides with the corresponding projection map* (*for all $\ell \in \mathbf{P}$*). *Then $\mathcal{G}$ is an open subgroup of finite index in $\prod_{\ell \in \mathbf{P}} G_\ell$,*

$$Y = \mathcal{G} \cap \prod_{\ell \in \mathbf{P}} X(\mathbf{u}_\ell, T_\ell, G_\ell) \subset \mathcal{G}$$

is on open nonempty subset of $\mathcal{G}$ while the boundary of Y in $\mathcal{G}$ contains the identity element of $\mathcal{G}$ and has measure zero with respect to the Haar measure on $\mathcal{G}$.

Proof. Clearly, $\mathcal{G}$ is compact. From Corollary 4.8 it follows that $\mathcal{G}$ is an open subgroup of finite index in $\prod_{\ell \in \mathbf{P}} G_\ell$. By the definition of Y,

$$Y = \mathcal{G} \cap \prod_{\ell \in \mathbf{P}} X(\mathbf{u}_\ell, T_\ell, G_\ell) \subset \prod_{\ell \in \mathbf{P}} G_\ell.$$

It follows that the closure $\overline{Y}$ of Y lies in

$$\prod_{\ell \in \mathbf{P}} [X(\mathbf{u}_\ell, T_\ell, G_\ell) \sqcup (G_\ell)_\Delta] \subset \prod_{\ell \in \mathbf{P}} G_\ell.$$

Recall (Corollary 4.8) that Y is open in $\mathcal{G}$. This implies that the boundary ∂Y of Y lies in the (finite) union Z of products

$$Z_p := (G_p)_\Delta \times \prod_{\ell \in \mathbf{P}, \ell \neq p} G_\ell$$

for all $p \in P$. By Lemma 4.2, $(G_p)_\Delta$ has measure zero with respect to the Haar measure on G_p. This implies that each product-set Z_p has measure zero with respect to the Haar measure on $\prod_{\ell\in\mathbf{P}} G_\ell$. It follows that their union Z and therefore its subset ∂Y have measure zero with respect to the Haar measure on $\prod_{\ell\in\mathbf{P}} G_\ell$. Since ∂Y lies in $\mathcal{G}$, which is an open subgroup of finite index in $\prod_{\ell\in\mathbf{P}} G_\ell$, the boundary ∂Y has measure zero with respect to the Haar measure on $\mathcal{G}$ as well. □

Remark 4.10. Since Y is open nonempty in $\mathcal{G}$, its measure (with respect to the Haar measure) is positive.

§5. Frobenius elements

Let $\mathbf{P}$ be a finite nonempty set of primes. Let K be a number field and $L \subset \overline{K}$ a Galois extension of K that is unramified outside a finite set of places of K. Let $\mathcal{G} := \mathrm{Gal}(L/K)$ be the Galois group of L/K.

Let v be a non-Archimedean place of K. Let us choose an extension $\overline{v}$ of v to $\overline{K}$. Let $D(\overline{v}) \subset \mathrm{Gal}(K)$ be the decomposition group of $\overline{v}$ and $I(\overline{v}) \subset D(\overline{v})$ the (normal) inertia (sub)group of $\overline{v}$. It is known that the quotient $D(\overline{v})/I(\overline{v})$ is canonically isomorphic to the absolute Galois group $\mathrm{Gal}(k(v))$ of the finite *residue field* $k(v)$ at v. In particular, this quotient has a canonical generator $\phi_{\overline{v}}$ that corresponds to the *Frobenius automorphism* in $\mathrm{Gal}(k(v))$.

There is a natural continuous surjective homomorphism (restriction map)

$$\mathrm{res}_L\colon \mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(L/K)$$

that kills $I(\overline{v})$ if and only if v is unramified in L. If this is the case then the restriction res_L induces a continuous homomorphism $D(\overline{v})/I(\overline{v}) \to \mathrm{Gal}(L/K)$ and we call the image of $\phi_{\overline{v}}$ the Frobenius element at $\overline{v}$ in $\mathrm{Gal}(L/K)$ and denote it

$$\mathrm{Frob}_{\overline{v},L} \in \mathrm{Gal}(L/K).$$

All the $\mathrm{Frob}_{\overline{v},L}$'s (for a given v) constitute a *conjugacy class* in $\mathrm{Gal}(L/K)$.

If L'/K is a Galois subextension of L/K, then the corresponding Frobenius element

$$\mathrm{Frob}_{\overline{v},L'} \in \mathrm{Gal}(L'/K)$$

coincides with the image of $\mathrm{Frob}_{\overline{v},L}$ under the natural surjective homomorphism (restriction map)

$$\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(L'/K).$$

We will need the following variant of Chebotarev's density theorem that is due to Serre [15, Chapter I, Section 2.2, Corollary 2].

Lemma 5.1. *Let $\mathcal{X}$ be a subset of the Galois group $\mathcal{G} = \mathrm{Gal}(L/K)$ that is stable under conjugation. Assume that the boundary of $\mathcal{X}$ has measure 0 with respect to the Haar measure on $\mathcal{G}$. Then the set of non-Archimedean places v of K such that the corresponding Frobenius elements $\mathrm{Frob}_{\overline{v}}$ lie in $\mathcal{X}$ has positive density.*

We will apply Lemma 5.1 in the following situation.

The field L is a compositum of infinite Galois extensions $K(\ell/K)$ for all $\ell \in \mathbf{P}$. The inclusions $K \subset K(\ell) \subset L$ induces a continuous surjective homomorphism

$$\rho_\ell\colon \mathcal{G} = \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(K(\ell)/K),$$

which we denote by

$$\rho_\ell\colon \mathcal{G} \twoheadrightarrow \mathrm{Gal}(K(\ell)/K).$$

The product-homomorphism

$$\rho\colon \mathcal{G} \to \prod_{\ell\in\mathbf{P}} \mathrm{Gal}(K(\ell)/K), \quad \sigma \mapsto \{\rho_\ell(\sigma)\}_{\ell\in\mathbf{P}}$$

is an embedding, whose (homeomorphic) image is a certain closed subgroup of the product $\prod_{\ell\in\mathbf{P}} \mathrm{Gal}(K(\ell)/K)$ that maps surjectively on each factor. Further we will identify $\mathcal{G}$ with this closed subgroup in $\prod_{\ell\in\mathbf{P}} \mathrm{Gal}(K(\ell)/K)$.

Lemma 5.2. *Suppose that for each $\ell \in \mathbf{P}$ we are given the following data.*

- *A $\mathbb{Q}_\ell$-vector space V_ℓ of finite positive dimension d_ℓ provided with a $\mathbb{Z}_\ell$-lattice $T_\ell \subset V_\ell$ of rank d_ℓ.*
- *A connected reductive linear algebraic subgroup $\mathfrak{G}_\ell \subset \mathrm{GL}(V_\ell)$ of positive dimension.*
- *An element*
$$\mathbf{u}_\ell \in \mathfrak{G}_\ell(\mathbb{Q}_\ell) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell)$$
such that its characteristic polynomial $P_{\mathbf{u}_\ell}(t) = \det(t\,\mathrm{Id} - \mathbf{u}_\ell, V) \in \mathbb{Q}_\ell[t]$ has no multiple roots.
- *A compact subgroup*
$$G_\ell \subset \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell)$$
that is an open subgroup in $\mathfrak{G}_\ell(\mathbb{Q}_\ell)$.
- *An isomorphism of compact groups*
$$\mathrm{Gal}(K(\ell)/K) \cong G_\ell.$$
Further we will identify these two groups via this isomorphism and $\mathcal{G}$ with a certain closed subgroup of $\prod_{\ell\in\mathbf{P}} G_\ell$ that maps surjectively on each factor. We keep the notation ρ_ℓ for the projection map
$$\mathcal{G} \twoheadrightarrow G_\ell.$$
For each $\ell \in \mathbf{P}$ and $\sigma \in \mathcal{G}$, we have
$$\rho_\ell(\sigma) \in G_\ell \subset \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell).$$
- *For each $\ell \in \mathbf{P}$, consider the subset $Y_\ell \subset \mathcal{G}$ that consists of all $\sigma \in \mathcal{G}$ such that the centralizer $\mathfrak{Z}(\rho_\ell(\sigma))_0$ of $\rho_\ell(\sigma)$ in $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell) \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell)$ is isomorphic (as a $\mathbb{Z}_\ell$-algebra) to $\mathfrak{Z}(\mathbf{u}_\ell)_0$.*

Also consider the intersection

$$Y = \bigcap_{\ell\in\mathbf{P}} Y_\ell \subset \mathcal{G} \subset \prod_{\ell\in\mathbf{P}} G_\ell.$$

Then the set of non-Archimedean places v of K such that the corresponding Frobenius *elements* $\mathrm{Frob}_{\bar{v}}$ *lie in Y has density > 0.*

Proof. We put $\mathcal{X} := Y \subset \mathcal{G}$. We know that Y is stable under conjugation, has positive measure, and its boundary has measure 0 with respect to the Haar measure on $\mathcal{G}$ (Remark 4.10 and Corollary 4.8). Now the result follows from Lemma 5.1. □

Remark 5.3. Suppose that for each $\ell \in \mathbf{P}$ we are given an open *normal* subgroup G'_ℓ in G_ℓ of finite index. Put

$$\mathcal{G}' = \mathcal{G} \cap \prod_{\ell\in\mathbf{P}} G'_\ell \subset \mathcal{G}, \quad Y' = Y \cap \mathcal{G}' \subset \mathcal{G}'.$$

Then $\mathcal{G}'$ is an open subgroup of finite index in $\mathcal{G}$ and therefore is closed in $\mathcal{G}$. We know that Y is open in $\mathcal{G}$ and its boundary contains the identity element. This implies that Y' is an open nonempty subset of $\mathcal{G}$; in particular, it has positive measure with respect to the Haar measure on $\mathcal{G}$. Since each G'_ℓ is normal in G_ℓ, the subgroup $\prod_{\ell\in\mathbf{P}} G'_\ell$ is normal in $\prod_{\ell\in\mathbf{P}} G_\ell$ and therefore $\mathcal{G}'$ is normal in $\mathcal{G}$, which implies that Y' is a subset of $\mathcal{G}$ that is stable under conjugation. On the other hand, the boundary of Y' lies in the boundary of Y and therefore also has measure zero with respect to the Haar measure on $\mathcal{G}$. Now Lemma 5.1 implies that the set of non-Archimedean places v of K such that the corresponding *Frobenius elements* $\mathrm{Frob}_{\overline{v}}$ lie in Y' has density > 0.

5.4. Let $\mathbf{P}$ be a nonempty finite set of primes, A an Abelian variety of positive dimension g over a number field K. We put

$$d = 2g, \quad V_\ell = V_\ell(A), \quad T_\ell = T_\ell(A), \quad \rho_\ell = \rho_{\ell,A},$$
$$\mathcal{G} = \mathrm{Gal}(K), \quad G_\ell = \rho_{\ell,A}(\mathrm{Gal}(K)) = G_{\ell,A}.$$

We define $K(\ell) \subset \overline{K}$ as the field $\bigcup_{i=1}^\infty K(A[\ell^i])$ of definition of all ℓ-power torsion points on A. From the definition of Tate modules it follows that $K(\ell)$ coincides with the subfield of $\ker(\rho_{\ell,A})$-invariants in $\overline{K}$ and $\mathrm{Gal}(K(\ell)/K) = G_{\ell,A}$. Let v be a non-Archimedean place of K and $\overline{v}$ an extension of v to $\overline{K}$. Assume that A has good reduction at v and the residual chacacteristic of v is different from ℓ. Then

$$\mathrm{Frob}_{\overline{v},K(\ell)} = \mathrm{Frob}_{\overline{v},A,\ell} \in G_{\ell,A} = \mathrm{Gal}(K(\ell)/K)$$

([18, Section 2], [15, Chapter I]). On the other hand, recall (Section 1.2) that there is an isomorphism of $\mathbb{Z}_\ell$-algebras

$$(***) \qquad \mathfrak{Z}(\mathrm{Frob}_{\overline{v},A,\ell})_0 \cong \mathrm{End}(A(v)) \otimes \mathbb{Z}_\ell.$$

Theorem 5.5. *Let g be a positive integer. Let $\mathbf{P}$ be a nonempty finite set of primes. Suppose that for every $\ell \in \mathbf{P}$ we are given the following data.*

- *A $2g$-dimensional $\mathbb{Q}_\ell$-vector space V_ℓ provided with alternating nondegenerate $\mathbb{Z}_\ell$-bilinear form*
$$e_\ell \colon V_\ell \times V_\ell \to \mathbb{Q}_\ell.$$
We write $\mathrm{Gp}(V_\ell, e_\ell) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell)$ for the corresponding group of symplectic similitudes.
- *An element*
$$\mathbf{u}_\ell \in \mathrm{Gp}(V_\ell, e_\ell) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell)$$
such that the characteristic polynomial
$$P_{\mathbf{u}_\ell}(t) = \det(t\,\mathrm{Id} - \mathbf{u}_\ell, V_\ell) \in \mathbb{Q}_\ell[t]$$
has no multiple roots. Let $\mathfrak{Z}(\mathbf{u}_\ell)$ be the centralizer of $\mathbf{u}_\ell$ in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell)$, which is a commutative semisimple $\mathbb{Q}_\ell$-algebra of dimension $2g$.
- *A $\mathbb{Z}_\ell$-lattice T_ℓ of rank $2g$ in V_ℓ such that the restriction of e_ℓ to $T_\ell \times T_\ell$ takes values in $\mathbb{Z}_\ell$ and the corresponding alternating $\mathbb{Z}_\ell$-bilinear form*
$$T_\ell \times T_\ell \to \mathbb{Z}_\ell, \quad x, y \mapsto e_\ell(x, y)$$
is perfect. Let $\mathfrak{Z}(\mathbf{u}_\ell)_0$ for the centralizer of $\mathbf{u}_\ell$ in
$$\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell) \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell),$$
which is an order in $\mathfrak{Z}(\mathbf{u}_\ell)$ and coincides with the intersection
$$\mathfrak{Z}(\mathbf{u}_\ell) \cap \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell).$$

Let A be a g-dimensional Abelian variety over a number field K that admits a polarization λ such that its degree $\deg(\lambda)$ is not divisible by ℓ for all $\ell \in \mathbf{P}$. Suppose that $\mathfrak{G}_{\ell,A} = \mathfrak{Gp}(V_\ell(A), e_{\lambda,\ell}$ for all primes ℓ.

Let Σ be the set of non-Archimedean places of K such that A has good reduction at v, the residual characteristic of v does not belong to $\mathbf{P}$ and the $\mathbb{Z}_\ell$-algebras $\mathrm{End}(A(v)) \otimes \mathbb{Z}_\ell$ *and $\mathfrak{Z}(\mathbf{u}_\ell)_0$ are isomorphic for all $\ell \in \mathbf{P}$.*

Then Σ has positive density.

Remark 5.6. If $\mathfrak{G}_{\ell,A} = \mathfrak{Gp}(V_\ell(A), e_{\lambda,\ell})$ for one prime ℓ then it is true for all primes [24]. Such A are sometimes called Abelian varieties of GSp type. If A is an abelian variety of GSp type then the set of non-Archimedean places v of K such that $\mathrm{End}^0(A(v))$ is a degree $2g$ CM field has density 1 [30].

Proof. For each $\ell \in \mathbf{P}$, let us fix a symplectic isomorphism

$$\phi_\ell \,:\, (T_\ell(A), e_{\lambda,\ell}) \cong (T_\ell, e_\ell).$$

Extending ϕ_ℓ by $\mathbb{Q}_\ell$-linearity, we obtain a symplectic isomorphism

$$(V_\ell(A), e_{\lambda,\ell}) \cong (V_\ell, e_\ell),$$

which we continue to denote by ϕ_ℓ. Clearly,

$$\mathrm{Gp}(V_\ell(A), e_{\lambda,\ell}) = \phi_\ell^{-1}\mathrm{Gp}(V_\ell), e_\ell)\phi_\ell.$$

Let us put

$$\mathbf{u}'_\ell = \phi_\ell^{-1}\mathbf{u}_\ell\phi \in \phi_\ell^{-1}\mathrm{Gp}(V_\ell), e_\ell)\phi_\ell = Gp(V_\ell(A), e_{\lambda,\ell}) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A).$$

Clearly, the characteristic polynomial of $\mathbf{u}'_\ell$ has no multiple roots (since it coincides with the characteristic polynomial of $\mathbf{u}_\ell$) and the centralizer $\mathfrak{Z}(\mathbf{u}'_\ell)_0$ is isomorphic as $\mathbb{Z}_\ell$-algebra to $\mathfrak{Z}(\mathbf{u}_\ell)_0$.

Now Theorem 5.5 follows from Lemma 5.2 combined with ($\ast\ast\ast$). $\square$

§6. Proof of main results

Proof of Theorem 1.3. In light of Subsection 5.4, the result follows from Lemma 5.2 combined with ($\ast\ast\ast$). $\square$

Proof of Theorem 1.10. Recall that A is a *Jacobian* and therefore admits a canonical principal polarization λ. This implies that the corresponding alternating $\mathbb{Z}_\ell$-bilinear form

$$e_{\lambda,\ell} \colon T_\ell(A) \times T_\ell(A) \to \mathbb{Z}_\ell$$

is unimodular. It is also known [24] that our assuptions on the Galois group of $f(x)$ imply that

$$\mathfrak{G}_{A,\ell} = \mathfrak{Gp}(V_\ell(A), e_{\lambda,\ell})$$

for all primes ℓ.

For each $\ell \in P$ the Abelian variety$B^{(\ell)}$ admits a polarization say, μ_ℓ of degree prime to ℓ. This implies that the corresponding alternating $\mathbb{Z}_\ell$-bilinear form

$$e_{\mu_\ell,\ell} \colon T_\ell(B^{(\ell)}) \times T_\ell(B^{(\ell)}) \to \mathbb{Z}_\ell$$

is unimodular. We put

$$V_\ell = V_\ell(B^{(\ell)}), \quad T_\ell = T_\ell(B^{(\ell)}), \quad e_\ell = e_{\mu_\ell,\ell}.$$

Since both alternating forms $e_{\lambda,\ell}$ and $e_{\mu,\ell}$ are unimodular and the ranks of free $\mathbb{Z}_\ell$-modules $T_\ell(A)$ and $T_\ell(B^{(\ell)})$ do coincide, there is a symplectic isomorphism of free $\mathbb{Z}_\ell$-modules

$$\phi_\ell i \,:\, T_\ell(A) \cong T_\ell(B^{(\ell)}),$$

which extends by $\mathbb{Q}_\ell$-linearity to the symplectic isomorphism of $\mathbb{Q}_\ell$-vector spaces

$$V_\ell(A) \cong V_\ell(B^{(\ell)}),$$

which we continue to denote ϕ. Clearly,

$$\mathrm{Gp}(V_\ell(A), e_{\lambda,\ell}) = \phi^{-1}\mathrm{Gp}(V_\ell(B^{(\ell)}), e_{\mu,\ell})\phi.$$

Using Theorem 2.1, pick

$$\mathbf{u}_\ell \in \mathrm{End}((B^{(\ell)})) \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(B^{(\ell)}) = \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell)$$

such that its characteristic polynomial has no multiple roots, $\mathbf{u}_\ell$ lies in

$$\mathrm{Gp}(V_\ell(B^{(\ell)}), e_{\mu,\ell}) = \mathrm{Gp}(V_\ell, e_\ell),$$

and the centralizer $\mathfrak{Z}(\mathbf{u}_\ell)_0$ of $\mathbf{u}_\ell$ in $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(B^{(\ell)})) = \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell)$ coincides with the set $\mathrm{End}((B^{(\ell)})) \otimes \mathbb{Z}_\ell$. Now the result follows from Theorem 5.5. □

§7. Complements

Theorem 7.1. *Let $g \geq 2$ be an integer, $n = 2g+1$ or $2g+2$. Let $\mathbf{P}$ be a nonempty finite set of primes and suppose that for each $\ell \in \mathbf{P}$ we are given a g-dimensional semisimple commutative $\mathbb{Q}_\ell$-algebra $\mathcal{C}_\ell$ and an order $\mathcal{R}_\ell$ in $\mathcal{C}_\ell$.*

Let K be a number field and $f(x) \in K[x]$ a degree n irreducible polynomial whose Galois group over K is either the full symmetric group $\mathbf{S}_n$ or the alternating group $\mathbf{A}_n$. Let us consider the genus g hyperelliptic curve $C_f : y^2 = f(x)$ and its Jacobian A, which is a g-dimensional Abelian variety over K.

Let Σ be the set of all non-Archimedean places v of K such that A has good reduction at v, the residual characteristic $\mathrm{char}(k(v))$ does not belong to $\mathbf{P}$ and the $\mathbb{Z}_\ell$-rings $\mathrm{End}(A)\otimes\mathbb{Z}_\ell$ and $\mathcal{R}_\ell \oplus \mathcal{R}_\ell$ are isomorphic for all $\ell \in \mathbf{P}$. Then Σ has density > 0.

Proof. Recall that A admits a principal polarization λ and for each prime ℓ

$$e_{\lambda,\ell} \colon T_\ell(A) \times T_\ell(A) \to \mathbb{Z}_\ell$$

is the corresponding alternating perfect $\mathbb{Z}_\ell$-bilinear pairing. Let ℓ be a prime that lies in $\mathbf{P}$. We put

$$\mathcal{R} = \mathcal{R}_\ell, \quad \mathcal{C} = \mathcal{C}_\ell$$

and fix a free $\mathcal{R} = \mathcal{R}_\ell$-module $\mathcal{T} = \mathcal{T}_\ell$ of rank 1 (e.g., $\mathcal{T}_\ell = \mathcal{R}_\ell$). Let

$$\mathcal{V} = \mathcal{V}_\ell, \quad \mathbf{T} = \mathbf{T}_\ell, \quad \mathbf{V} = \mathbf{V}_\ell$$

be as in Example 4.7. In particular, $\mathbf{T}_\ell$ is a free $\mathbb{Z}_\ell$-module of rank $2g$ that is a lattice in the $2g$-dimensional $\mathbb{Q}_\ell$-vector space $\mathbf{V}$.

In addition, using Example 4.7, we obtain an alternating perfect $\mathbb{Z}_\ell$-bilinear form

$$e_\ell \colon \mathbf{T}_\ell \times \mathbf{T}_\ell \to \mathbb{Z}_\ell$$

and an element

$$\mathbf{u}_\ell \in \mathrm{Gp}(\mathbf{V}_\ell, e_\ell) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(\mathbf{V}_\ell)$$

such that the centralizer $\mathfrak{Z}(\mathbf{u}_\ell)_0$ in $\mathrm{End}_{\mathbb{Z}_\ell}(\mathbf{T}_\ell) \subset \mathrm{End}_{\mathbb{Q}_\ell}(\mathbf{V}_\ell)$ is isomorphic to $\mathcal{R}_\ell \oplus \mathcal{R}_\ell$.

Now the result follows from Theorem 5.4. □

Theorem 7.2. *Let $g \geq 2$ be an integer, $n = 2g+1$ or $2g+2$. Let $\mathbf{P}$ be a nonempty finite set of primes and suppose that for each $\ell \in \mathbf{P}$ we are given the following data.*

- *A degree g field extension $F_{0,\ell}/\mathbb{Q}_\ell$. We write $\mathcal{O}_{0,\ell}$ for the ring of integers in the ℓ-adic field $F_{0,\ell}$.*
- *A 2-dimensional semisimple commutative $\mathbb{F}_{0,\ell}$-algebra $\mathcal{C}_\ell$.*
- *An $\mathcal{O}_{0,\ell}$-subalgebra R_ℓ of $\mathcal{C}_\ell$ that is a free $\mathcal{O}_{0,\ell}$-module of rank 2.*

Let K be a number field and $f(x) \in K[x]$ a degree n irreducible polynomial whose Galois group over K is either the full symmetric group $\mathbf{S}_n$ or the alternating group $\mathbf{A}_n$. Consider the genus g hyperelliptic curve $C_f : y^2 = f(x)$ and its Jacobian A, which is a g-dimensional Abelian variety over K.

Let Σ be the set of all non-Archimedean places v of K such that A has good reduction at v, the residual characteristic $\mathrm{char}(k(v))$ *does not belong to* $\mathbf{P}$ *and the $\mathbb{Z}_\ell$-rings* $\mathrm{End}(A) \otimes \mathbb{Z}_\ell$ *and R_ℓ are isomorphic for all $\ell \in \mathbf{P}$. Then Σ has density > 0.*

Proof. The proof is literally the same as the proof of Theorem 7.1 with the only modification: we need to use Lemma 3.4 instead of Example 4.7. $\square$

Remark 7.3. Let $\mathbf{N}$ be a positive integer. The assertions of Theorems 1.3, 1.10, 5.5, 7.1, 7.2 (respectively, of Example 1.5 and Corollary 1.6) remain true if we impose an additional condition on the places v that the residual characteristic of v does not divide $\mathbf{N}$ and $A(v)[\mathbf{N}]$ lies in $A(v)(k(v))$ (respectively, $E(v)[\mathbf{N}]$ lies in $E(v)(k(v))$). Indeed, let $\mathbf{P}'$ be the set of prime divisors of $\mathbf{N}$. Then the proofs remain the same with the only modification: we should deal with the finite set of primes $\widetilde{\mathbf{P}} = \mathbf{P} \cup \mathbf{P}'$ (instead of $\mathbf{P}$) and apply Remark 5.3 (instead of Lemma 5.2) to $G_\ell = G_{\ell,A}$ for all $\ell \in \widetilde{\mathbf{P}}$,

$$G'_\ell = G_{\ell,A} \cap [\mathrm{Id} + \mathbf{N} \cdot \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A))] \subset G_{\ell,A} = G_\ell$$

if $\ell \mid \mathbf{N}$ and

$$G'_{\ell,A} = G_{\ell,A} = G_\ell$$

if ℓ does *not* divide $\mathbf{N}$. It would be interesting to compute explicitly the corresponding densities (at least, in the case of elliptic curves) or just to study their asymptotic behavior.

Remark 7.4. In Theorems 1.3, 1.10, 5.5, 7.1, 7.2 we assume that $\mathrm{Gal}(f) = \mathbf{S}_n$ or $\mathbf{A}_n$ only in order to make sure that the Jacobian is of GSp type. See [24, 25, 28] where we discuss the cases of smaller $\mathrm{Gal}(f)$'s when the Jacobian is still of GSp type and therefore Theorems 1.3, 1.10, 5.5, 7.1, 7.2 remain true.

Acknowledgments

I thank Mihran Papikian and Alina Cojocaru for stimulating questions and their interest in this paper.

References

[1] F. A. Bogomolov, *Sur l'algébricité des représentations ℓ-adiques*, C. R. Acad. Sci. Paris Sér. A-B **290** (1980), no. 15, 701–703. MR574307

[2] ______, *Holomorphic tensors and vector bundles on projective manifolds*, Izv. Akad. Nauk Ser. Mat. **42** (1978), no. 6, 1227–1287; English transl., Math. USSR-Izv. **13** (1979), no. 3, 499–555. MR522939

[3] A. Borel, *Linear algebraic groups*, W. A. Benjamin, Inc., New York–Amsterdam, 1969. MR0251042

[4] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zählkorpern*, Invent. Math. **73** (1983), 349–366; Erratum **75** (1984), 381. MR0718935 (85g:110261) MR0732534 (85g:11026b)

[5] ______, *Complements to Mordell*, Rational Points (Bonn, 1983/1984) Aspects, Math. E6, Vieweg & Sohn, Braunschweig, 1984, pp.203–227. MR766574

[6] G. Harder, *Eine Bemerkung zum schwachen Approximationssatz*, Arc. Math. **19** (1968), 465–471. MR0241427

[7] S. Lang, *Abelian varieties*, 2nd ed., Springer-Verlag, Berlin, 1983. MR713430

[8] M. Larsen and R. Pink, *On ℓ-independence of algebraic monodromy groups in compatible systems of representations*, Invent. Math. **107** (1992), no. 3, 603–636. MR1150604

[9] J. S. Milne, *Étale cohomology*, Princeton Univ. Press, vol. 33, Princeton Math. Ser., Princeton, NJ, 1980. MR559531

[10] L. Moret-Bailly, *Pinceaux de variétés abéliennes*, Astérisque **129** (1985). MR797982

[11] D. Mumford, *Abelian varieties*, 2nd ed., Oxford Univ. Press, London, 1974. MR2514037 (2010e:14040)

[12] F. Oort, *Endomorphism algebras of abelian varieties*, Algebraic Geometry and Commutative Algebra. Vol. II, Kinokuniya, Tokyo, 1988, pp. 469–502. MR977774

[13] R. Schoof, *The exponents of the groups of points on the reductions of an elliptic curve*, Arithmetic Algebraic Geometry, Progr. Math., vol. 89, Birkhäuser, Boston Basel, 1991, pp. 325–336. MR1085266

[14] J. -P. Serre, *Corps locaux*, Publ. Univ. Nancago, vol. 8, Hermann, Paris, 1968. MR0354618

[15] ———, *Abelian ℓ-adic representations and elliptic curves*, 2nd ed., Addison–Wesley Publ., Redwood City, CA, 1989. MR1043865

[16] ———, *Lettres à Ken Ribet du* 1/1/1981 *et* 29/1/1981, Euvres, Collected Papers, vol. IV, Springer-Verlag, Berlin, 2000, pp. 1–20. MR1730973

[17] ———, *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. IHES **54** (1981), 123–201. MR644559

[18] J. -P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. MR0236190

[19] J. Tate, *Algebraic cycles and poles of zeta functions*, Arithmetical Algebraic Geometry, Harper and Row, New York, 1965, pp. 93–110. MR0225778

[20] ———, *Endomorphisms of Abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR0206004

[21] Yu. G. Zarhin, *Endomorphisms of Abelian varietes over fields of finite characteristics*, Izv. Akad. Nauk SSSR Ser. Mat. **39** (1975), no. 2, 272–277; English transl., Math. USSR-Izv. **9** (1975), no. 2, 255–260. MR0371897

[22] ———, *Abelian varieties in characteristics P*, Mat. Zametki **19** (1976), no. 3, 393–400; English transl., Math. Notes **19** (1976), no. 3, 240–244. MR0422287

[23] ———, *The equations defining the moduli of abelian varieties with endomorphisms from a totally real field*, Tr. Moskov. Mat. Obshch. **42** (1981), 3–49; English transl., Translations of the Moscow Mathm Soc. 1982, issue 2, pp. 1–46. MR621993

[24] ———, *Very simple* 2*-adic representations and hyperelliptic Jacobians*, Moscow Math. J. **2** (2002), no. 2, 403–431. MR1944511

[25] ———, *Families of absolutely simple hyperelliptic jacobians*, Proc. London Math. Soc. **100** (2010), no. 1, 24–54. MR2578467

[26] ———, *Abelian varieties over fields of finite characteristic*, Cent. Eur. J. Math. **12** (2014), no. 5, 659–674. MR3165576

[27] ———, *Galois groups of Mori trinomials and hyperelliptic curves with big monodromy*, Eur. J. Math. **2** (2016), no. 1, 360–381. MR3454107

[28] ———, *Two-dimensional families of hyperelliptic jacobians with big monodromy*, Trans. Amer. Math. Soc. **368** (2016), no. 5, 3651–3672. MR3451889

[29] Yu. G. Zarhin and A. N. Parshin, *Finiteness problems in Diophantine geometry*, Amer. Math. Soc. Transl. (2) **143** (1989), 35–102; `arXiv:0912.4325 [math.NT]`.

[30] D. Zywina, *The splitting of reductions of an abelian variety*, Int. Math. Res. Not. IMRN, **2014**, no. 18, 5042–5083. MR3264675

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

Email address: `zarhin@math.psu.edu`

Received 10/FEB/2016

Originally published in English