Torsion of abelian varieties, Weil classes and cyclotomic extensions

BY YURI G. ZARHIN†
325 McAllister Building, Department of Mathematics, Pennsylvania State University,
University Park, PA 16802, USA
e-mail: zarhin@math.psu.edu

(Received 12 September 1997; revised 18 December 1997)

Let $K \subset \mathbb{C}$ be a field finitely generated over $\mathbb{Q}$, $K(a) \subset \mathbb{C}$ the algebraic closure of $K$ and $G(K) = \text{Gal}(K(a)/K)$ its Galois group. For each positive integer $m$ we write $K(\mu_m)$ for the subfield of $K(a)$ obtained by adjoining to $K$ all $m$th roots of unity. For each prime $\ell$ we write $K(\ell)$ for the subfield of $K(a)$ obtained by adjoining to $K$ all $\ell$-power roots of unity. We write $K(c)$ for the subfield of $K(a)$ obtained by adjoining to $K$ all roots of unity in $K(a)$. Let $K(ab) \subset K(a)$ be the maximal abelian extension of $K$. The field $K(ab)$ contains $K(c)$; if $K = \mathbb{Q}$ then $K(ab) = K(c)$ (the Kronecker-Weber theorem). We write $\chi: G(K) \to \mathbb{Z}^*_\ell$ for the cyclotomic character defining the Galois action on all $\ell$-power roots of unity. We write $\bar{\chi}_\ell = \chi_\ell \mod \ell: G(K) \to \mathbb{Z}^*_\ell \to (\mathbb{Z}/\ell\mathbb{Z})^*$ for the cyclotomic character characterizing the Galois action on the $\ell$th roots of unity.

The character $\chi_\ell$ identifies $\text{Gal}(K(\ell)/K)$ with a subgroup of $\mathbb{Z}^*_\ell = \text{Gal}(\mathbb{Q}(\ell)/\mathbb{Q})$. Let $\mu(\mathbb{Z}_\ell)$ be the finite cyclic group $\mu(\mathbb{Z}_\ell)$ of all roots of unity in $\mathbb{Z}^*_\ell$. Its order is equal to $\ell - 1$ if $\ell$ is odd and 2 if $\ell = 2$. Let $\mathbb{Q}(\ell)'$ be the subfield of $\mu(\mathbb{Z}_\ell)$-invariants in $\mathbb{Q}(\ell)$. Clearly, $\text{Gal}(\mathbb{Q}(\ell)/\mathbb{Q}(\ell)') = \mu(\mathbb{Z}_\ell)$ and $\text{Gal}(\mathbb{Q}(\ell)'/\mathbb{Q}) = \mathbb{Z}^*_\ell/\mu(\mathbb{Z}_\ell)$ is isomorphic to $\mathbb{Z}_\ell$.

Let $g$ be a positive integer and $X$ a $g$-dimensional abelian variety over $K$. We write $\text{End}_K(X)$ for the ring of all endomorphisms of $X$ defined over $K$ and $\text{End}^0(X)$ for the finite-dimensional semisimple $\mathbb{Q}$-algebra $\text{End}_K(X) \otimes \mathbb{Q}$. Its centre $F = F_X$ is a field if and only if $X$ is $K$-isogenous to a power of a $K$-simple abelian variety. If so, $F$ is either a totally real number field or a CM-field. We write $\text{Lie}(X)$ for the tangent space to $X$ at the origin. It is the $g$-dimensional $K$-vector space. By functoriality, $\text{End}^0(X)$ acts faithfully on $\text{Lie}(X)$. We write

\[ \text{Tr}_{\text{Lie}(X)}: \text{End}^0(X) \hookrightarrow \text{End}_K(\text{Lie}(X)) \to K \subset \mathbb{C} \]

for the corresponding trace map. The embedding $\text{End}^0(X) \hookrightarrow \text{End}_K(\text{Lie}(X))$ gives rise to a natural structure of (not necessarily faithful) $\text{End}^0(X) \otimes \mathbb{Q}$ $K$-module on $\text{Lie}(X)$.

The well-known Mordell–Weil–Néron–Lang theorem asserts that $X(K)$ is a finitely generated commutative group. In particular, its torsion subgroup $\text{TORS}(X(K))$ is finite. Hereafter we will write $\text{TORS}(A)$ for the torsion subgroup of a commutative group $A$. This implies that $\text{TORS}(X(L))$ is finite for any finite algebraic extension $L$ of $K$. Mazur [7] has raised the question of whether the groups $X(K(\ell))$ are finitely generated. In this connection, Serre (in letters to Mazur, of January 1974) and Imai [5] have proved independently that $\text{TORS}(X(K(\ell)))$ is finite for all $\ell$.

† Supported by the NSF.
Now assume that \( L \subset K(a) \subset \mathbb{C} \) is an infinite Galois extension of \( K \). When \( L = K(c) \) a theorem of Ribet [10] asserts that \( \text{TORS}(X(K(c))) \) is finite. The author [20] has proven that if the centre \( F \) of \( \text{End}^0(X) \) is a direct sum of totally real number fields and \( \text{TORS}(X(L)) \) is infinite then \( L \) contains infinitely many roots of unity. On the other hand, Bogomolov (Séminaire Delange-Pisot-Poitou, mai 1982, Paris) proved that \( \text{TORS}(X(L)) \) is finite if the intersection of \( L \) and \( K(ab) \) has finite degree over \( K \) [24]. For example, if \( K = \mathbb{Q} \), we obtain that if \( \text{TORS}(X(L)) \) is infinite then the intersection of \( L \) and \( \mathbb{Q}(c) \) has infinite degree over \( \mathbb{Q} \). The main result of the present paper is the following statement, which deals with essentially non-cyclotomic extensions and may be viewed as a partial improvement of the Bogomolov’s result.

**Definition 0.1.** We say that \( X \) and \( K \) satisfy hypothesis (H) if they enjoy one of the following properties:

1. there is a discrete valuation \( v \) on \( K \) such that \( X \) has potential purely multiplicative reduction at \( v \);
2. \( K \) does not contain a CM-field (e.g. \( K \subset \mathbb{R} \));
3. the Hodge group of \( X \) is semisimple;
4. the centre \( F \) of \( \text{End}^0(X) \) is a CM-field and the pair \( (X, F) \) is of Weil type, i.e. the \( F \otimes_{\mathbb{Q}} K \)-module \( \text{Lie}(X) \) is free.

**Remark 0.2.** It is proven in [14] that if an abelian variety has somewhere a (potential) purely multiplicative reduction then its Hodge group is semisimple.

**Theorem 0.3 (Main Theorem).** Let \( X \) be a \( g \)-dimensional abelian variety over \( K \). Assume that \( X \) and \( K \) satisfy hypothesis (H). If the intersection of \( L \) and \( K(c) \) has finite degree over \( K \) then \( \text{TORS}(X(L)) \) is finite.

**Remark 0.4.** If \( L \) is totally real then \( \text{TORS}(X(L)) \) is finite for an arbitrary \( X \) [23]. We refer to [10, 17, 18, 20–24] for other results concerning the torsion in infinite extensions.

The main theorem is an immediate corollary of the following statement.

**Theorem 0.5.** Let \( g \) be a positive integer. There exists a positive integer \( N = N(g) \) depending only on \( g \) and enjoying the following properties:

Let \( X \) be a \( g \)-dimensional abelian variety over \( K \) and assume that \( X \) and \( K \) satisfy hypothesis (H). Then assume that for some prime \( \ell \) the \( \ell \)-primary part of \( \text{TORS}(X(L)) \) is infinite. Then \( K(\ell) \) has finite degree over the intersection \( L \cap K(\ell) \) and this degree divides \( (N, \ell - 1) \) if \( \ell \) is odd and divides 2 if \( \ell = 2 \). In addition, \( L \) contains \( \mathbb{Q}(\ell) \). Let \( P = P(X, L) \) be the set of primes \( \ell \) such that \( X(L) \) contains a point of order \( \ell \). If \( P \) is infinite then for all but finitely many primes \( \ell \in P \) the degree \( [K(\mu_\ell) : L \cap K(\mu_\ell)] \) of the field extension \( K(\mu_\ell)/L \cap K(\mu_\ell) \) divides \( (N, \ell - 1) \).

We will prove Theorem 0.5 in Section 3.

1. **Main construction**

Let \( F \) be the centre of \( \text{End}_K(X) \otimes \mathbb{Q} \), \( R_F = F \cap \text{End}_K(X) \) the centre of \( \text{End}_K(X) \).

We put \( V_Z = V_Z(X) = H_1(X(\mathbb{C}), \mathbb{Z}) \), \( V = V(X) = H_1(X(\mathbb{C}), \mathbb{Q}) = V_Z \otimes \mathbb{Q} \).
For each nonnegative integer \( m \) one may naturally identify the \( m \)-th rational cohomology group \( H^m(X(\mathbb{C}), \mathbb{Q}) \) of \( X(\mathbb{C}) \) with \( \text{Hom}_Q(\Lambda^m_\mathbb{Q} V(X), \mathbb{Q}) \). For each prime \( \ell \) there are natural identifications

\[
X_\ell = V_\mathbb{Z}/\ell V_\mathbb{Z}, \quad T_\ell(X) = V_\mathbb{Z} \otimes \mathbb{Z}_\ell, \quad V_\ell(X) = V(X) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = V_\mathbb{Z} \otimes \mathbb{Q}_\ell.
\]

There is a natural Galois action

\[
\rho_\ell = \rho_{\ell,X} : G(K) \to \text{Aut}_{\mathbb{Z}_\ell}(T_\ell(X)) \subset \text{Aut}_{\mathbb{Q}_\ell}(V_\ell(X))
\]

induced by the Galois action on the torsion points of \( X \) [11]. One may naturally identify the \( m \)-th \( \ell \)-adic cohomology group \( H^m(X_a, \mathbb{Q}_\ell) \) of \( X_a = X \times K(a) \) with

\[
\text{Hom}_{\mathbb{Q}_\ell}(\Lambda^m_{\mathbb{Q}_\ell} V_\ell(X), \mathbb{Q}_\ell) = \text{Hom}_{\mathbb{Q}_\ell}(\Lambda^m_{\mathbb{Q}_\ell} V(X), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.
\]

This identification is an isomorphism of the Galois modules.

Assume now that \( F \) is a number field, i.e. \( X \) is either simple or isogenous over \( K \) to a self-product of a simple abelian variety. Let \( O_F \) be the ring of integers in \( F \). It is well known that \( R_F \) is a subgroup of finite index in \( O_F \). Recall that for each prime \( \ell \) there is a splitting \( F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \bigoplus \lambda F_\lambda \), where \( \lambda \) runs through the set of prime ideals dividing \( \ell \) in \( O_F \) and \( F_\lambda \) is the completion of \( F \) with respect to \( \lambda \)-adic topology. There is a natural splitting \( V_\ell(X) = \bigoplus V_\lambda(X) \), where

\[
V_\lambda(X) = F_\lambda V_\ell(X) = V(X) \otimes_{\mathbb{F}_\ell} F_\lambda.
\]

It is well known that all \( V_\lambda(X) \) are \( G(K) \)-invariant \( F_\lambda \)-vector spaces of dimension \( 2 \dim(X)/[F: \mathbb{Q}] \). We write \( \rho_{\lambda,X} \) for the corresponding \( \lambda \)-adic representation

\[
\rho_{\lambda,X} : G(K) \to \text{Aut}_{F_\lambda} V_\lambda(X)
\]

of \( G(K) \) [9, 11]. Similarly, for all but finitely many \( \ell \),

\[
R_F/\ell R_F = O_F/\ell O_F = \bigoplus_{\lambda | \ell} O_F/\lambda
\]

is a direct sum of finite fields \( O_F/\lambda \) of characteristic \( \ell \). Also, \( X_\ell = V_\mathbb{Z}/\ell V_\mathbb{Z} \) is a free \( R_F/\ell R_F = O_F/\ell O_F \)-module of rank \( 2 \dim(X)/[F: \mathbb{Q}] \) and there is a natural splitting

\[
X_\ell = V_\mathbb{Z}/\ell V_\mathbb{Z} = \bigoplus_{\lambda | \ell} X_\lambda
\]

where \( X_\lambda = (O_F/\lambda) \cdot X_\ell \). Clearly, each \( X_\lambda \) is a \( G(K) \)-invariant \( O_F/\lambda \)-vector space of dimension \( 2 \dim(X)/[F: \mathbb{Q}] \). We write \( \rho_{\lambda,X} \) for the corresponding modular representation

\[
\tilde{\rho}_{\lambda,X} : G(K) \to \text{Aut}_{O_F/\lambda} X_\lambda
\]

of \( G(K) \) [9]. Let \( d \) be a positive integer and assume that there exists a non-zero \( 2d \)-linear form \( \psi \in \text{Hom}_Q(\bigotimes_{\mathbb{Q}}^{2d} V(X), \mathbb{Q}) \), enjoying the following properties.

1. For all \( f \in F; v_1, \ldots, v_{2d} \in V(X) \)

\[
\psi(f v_1, v_2, \ldots, v_{2d}) = \psi(v_1, f v_2, \ldots, v_{2d}) = \cdots = \psi(v_1, v_2, \ldots, f v_{2d}).
\]
2. For any prime $\ell$ let us extend $\psi$ by $\mathbb{Q}_\ell$-linearity to the non-zero multilinear form $\psi_\ell \in \text{Hom}_{\mathbb{Q}_\ell}(\bigotimes_{i=1}^{2d} V_\ell(X), \mathbb{Q}_\ell)$. Then for all $\sigma \in G(K); v_1, \ldots, v_{2d} \in V_\ell(X)$

$$\psi_\ell(\sigma(v_1), \sigma(v_2), \ldots, \sigma(v_{2d})) = \chi^D_\ell(\sigma)\psi_\ell(v_1, v_2, \ldots, v_{2d}).$$

We call such a form admissible or $d$-admissible.

Example. Let us assume that $F$ is a totally real number field. If $\mathcal{L}$ is an invertible sheaf on $X$ defined over $K$ and algebraically non-equivalent to zero then one may associate to $\mathcal{L}$ its first Chern class

$$c_1(\mathcal{L}) \in H^2(X(\mathbb{C}), \mathbb{Q}) \simeq \text{Hom}_{\mathbb{Q}}(\Lambda^2_{\mathbb{Q}}(V(X), \mathbb{Q})).$$

The well-known properties of Rosati involutions and Weil pairings imply that $c_1(\mathcal{L})$ is 1-admissible (see p. 237 of [8], especially the last sentence, and section 2 of [15]).

There exists a unique $(F - 2d)$-linear form $\psi_F \in \text{Hom}_F(\bigotimes_{i=1}^{2d} V(X), F)$ such that

$$\psi = \text{Tr}_{F/Q}(\psi_F).$$

Multiplying $\psi$ by a sufficiently divisible positive integer, we may and will assume that the restriction of $\psi_F$ to $V_\mathbb{Z} \times \cdots \times V_\mathbb{Z}$ takes on values in $R_F$. Let $\text{Im}(\psi_F)$ be the additive subgroup of $R_F$ generated by values of $\psi_F$ on $V_\mathbb{Z} \times \cdots \times V_\mathbb{Z}$. Clearly, $\text{Im}(R_F)$ is a subgroup of finite index in $R_F$ that is an ideal. Notice that for all but finitely many primes $\ell$

$$O_F = R_F/\ell R_F, \quad \text{Im}(\psi_F) = R_F/\ell R_F.$$

Let us extend $\psi_F$ by $F_\lambda$-linearity to the non-zero multilinear form

$$\psi_{F,\lambda} \in \text{Hom}_{F_\lambda} \left( \bigotimes_{i=1}^{2d} V_\lambda(X), F_\lambda \right).$$

Then

$$\psi_{F,\lambda}(\sigma(v_1), \sigma(v_2), \ldots, \sigma(v_{2d})) = \chi^D_\ell(\sigma)\psi_{F,\lambda}(v_1, v_2, \ldots, v_{2d})$$

for all $\sigma \in G(K); v_1, \ldots, v_{2d} \in V_\lambda(X)$.

Similarly, for all but finitely many $\ell$, the form $\psi_F$ induces a non-zero multilinear form

$$\psi_F^{(\ell)} \in \text{Hom}_{R_F/\ell R_F} \left( \bigotimes_{i=1}^{2d} X_\ell, R_F/\ell R_F \right)$$

enjoying the following two properties.

The subgroup of $R_F/\ell R_F$ generated by all the values of $\psi_F^{(\ell)}$ coincides with $R_F/\ell R_F$.

For all $\sigma \in G(K); v_1, \ldots, v_{2d} \in X_\ell$

$$\psi_F^{(\ell)}(\sigma(v_1), \sigma(v_2), \ldots, \sigma(v_{2d})) = \check{\chi}^D_\ell(\sigma)\psi_F^{(\ell)}(v_1, v_2, \ldots, v_{2d}).$$

This implies that for all but finitely many $\ell$ the restriction of $\psi_F^{(\ell)}$ to $X_\lambda$ defines a non-zero multilinear form

$$\psi_F^{(\lambda)} \in \text{Hom}_{O_F/\lambda} \left( \bigotimes_{i=1}^{2d} X_\ell, O_F/\lambda \right)$$

YURI G. ZARHIN
such that
\[ \psi_F^{(\lambda)}(\sigma(v_1), \sigma(v_2), \ldots, \sigma(v_{2d})) = \chi^d(\sigma)\psi_F^{(\lambda)}(v_1, v_2, \ldots, v_{2d}) \]
for all \( \sigma \in G(K); v_1, \ldots, v_{2d} \in X_\lambda \).

**Remark 1.1.** Using the Künneth formula for \( X_\lambda^{2d} \), one may view \( \psi_\ell \) as a Tate cohomology class on \( X_\lambda^{2d} \). If \( \psi \) is skew-symmetric then \( \psi_\ell \) is a Tate cohomology class on \( X_\sigma \).

**Theorem 1.2.** Assume that the centre \( F \) of \( \text{End}^0 X \) is a field and there is a \( d \)-admissible form \( \psi \) on \( X \). Let \( \ell \) be a prime and assume that the \( \ell \)-torsion in \( X(L) \) is infinite. If \( L^{(1)} \) is the intersection of \( L \) and \( K(\ell) \) then the field extension \( K(\ell)/L^{(1)} \) has finite degree dividing \((d, \ell - 1)\) if \( \ell \) is odd and dividing \( 2 \) if \( \ell = 2 \). In addition, \( L \) contains \( Q(\ell)' \).

**Proof.** As explained in ([21], 0-8, 0-11) the assumption that the \( \ell \)-torsion in \( X(L) \) is infinite means that there exists a place \( \lambda \) of \( F \), dividing \( \ell \), such that the Galois group \( G(L) \) of \( L \) acts trivially on \( V_\lambda(X) \). Since \( \psi_F, \lambda \) is not identically zero, we conclude that
\[ \chi^d(\sigma) = 1, \quad \forall \sigma \in G(L) \subset G(K). \]
We write \( G' \) for the kernel of \( \chi^d \). We have \( G(L) \subset G' \subset G(K) \).

Recall that the kernel of \( \chi_\ell: G(K) \to \mathbb{Z}_\ell^* \) coincides with the Galois group \( G(K(\ell)) \) of \( K(\ell) \) and \( \chi_\ell \) identifies \( \text{Gal}(K(\ell)/K) \) with a subgroup of \( \mathbb{Z}_\ell^* = \text{Gal}(Q(\ell)/Q) \). Since the torsion subgroup of \( \mathbb{Z}_\ell^* \) is the cyclic group \( \mu(\mathbb{Z}_\ell) \) of order \( 1 \) if \( \ell \) is odd and of order \( 2 \) if \( \ell = 2 \), \( G' \) coincides with the kernel of \( (\chi_\ell)^d \) with \( d' = (d, \ell - 1) \) if \( \ell \) is odd and \( d' = (d, 2) \) if \( \ell = 2 \) respectively. This implies that the field \( K' = K(\alpha)^{G'} \) of \( G' \)-invariants is a subfield of \( K(\ell) \) and \([K(\ell): K'] \) divides \( d' \), since \( \chi_\ell \) establishes an isomorphism between \( \text{Gal}(K(\ell)/K') \) and
\[ \{ s \in \text{Im}(\chi_\ell) \subset \mathbb{Z}_\ell^* \mid s^{d'} = 1 \} \subset \{ s \in \mu(\mathbb{Z}_\ell) \mid s^{d'} = 1 \}. \]
Now it is clear that \( K' \subset L \), since \( G(L) \subset G' = G(K') \). It is also clear that \( K(\ell)/K' \) is a cyclic extension of degree dividing \( d' \).

In order to prove the last assertion of the theorem, notice that
\[ \text{Gal}(K(\ell)/K) \subset \text{Gal}(Q(\ell)/Q) = \mathbb{Z}_\ell^* \]
and the finite subgroup \( \text{Gal}(K(\ell)/K') \) of \( \text{Gal}(K(\ell)/K) \) sits in \( \mu(\mathbb{Z}_\ell) \subset \mathbb{Z}_\ell^* \). Since \( \mu(\mathbb{Z}_\ell) = \text{Gal}(Q(\ell)/Q(\ell)'), \ Q(\ell)' \subset K' \). Since \( K' \subset L, \ Q(\ell)' \subset L \).

**Theorem 1.3.** Assume that the centre \( F \) of \( \text{End}^0 X \) is a field and there is a \( d \)-admissible form \( \psi \) on \( X \). Let \( S \) be an infinite set of primes \( \ell \) such that for all but finitely many \( \ell \in S \) the \( \ell \)-torsion in \( X(L) \) is not zero. Then for all but finitely many \( \ell \in S \) the field extension \( K(\mu_\ell)/K(\mu_\ell) \cap L \) has degree dividing \((d, \ell - 1)\).

**Proof.** For all but finitely many \( \ell \) the \( G(K) \)-module \( X_\ell \) is semisimple and the centralizer of \( G(K) \) in \( \text{End}(X_\ell) \) coincides with \( \text{End}_K(X) \otimes \mathbb{Z}/\mathbb{Z} \). This assertion was proved in [19] for number fields \( K \); the proof is based on results of Faltings [2]. (See [6] for an effective version.) However, the same proof works for arbitrary finitely generated fields \( K \), if one uses results of [3], generalizing the results of [2]. Clearly, for all but finitely many \( \ell \) the centre of \( \text{End}_K(X) \otimes \mathbb{Z}/\mathbb{Z} \) coincides with \( R_F/\ell R_F = O_F/\ell O_F \). Applying theorem 5f of [20] to \( G = G(K), G' = G(L), H = X_\ell, D = \text{End}_K(X) \otimes \mathbb{Z}/\mathbb{Z}, R = F_F/\ell R_F \), we conclude that for all but finitely
many $\ell \in S$ there exists $\lambda|\ell$ such that $G(L)$ acts trivially on $X_{\lambda}$. Using the Galois equivariance of the non-zero form $\psi_F^{(\lambda)}$, we conclude that for all but finitely many $\ell \in S$ the character $\chi_{\ell}^{d}$ kills $G(L)$. We write $G'$ for the kernel of $\chi_{\ell}^{d}$. We have $G(L) \subset G' \subset G(K)$.

Recall that the kernel of $\bar{\chi}_L : G(K) \to (\mathbb{Z}/\ell\mathbb{Z})^*$ coincides with $G(K(\mu_{\ell}))$ and $(\mathbb{Z}/\ell\mathbb{Z})^*$ is a cyclic group of order $\ell - 1$. This implies that the field $K' = K(a)^G$ of $G'$-invariants is a subfield of $K(\mu_{\ell})$ and $[K(\mu_{\ell}) : K']$ divides $(\ell - 1, d)$, since $\bar{\chi}_L$ establishes an isomorphism between $\text{Gal}(K(\mu_{\ell})/K')$ and $\{s \in \text{Im}(\bar{\chi}_{\ell}) \subset (\mathbb{Z}/\ell\mathbb{Z})^* : s^d = 1\}$. One has only to notice that $K' \subset L$, since $G(L) \subset G' = G(K')$.

**Corollary 1.4.** Assume that the torsion subgroup of $X(L)$ is infinite. Then the intersection of $L$ and $K(c)$ has infinite degree over $K$.

**Proof.** Indeed, either there is a prime $\ell$ such that the $\ell$-torsion in $X(L)$ is infinite or for infinitely many primes $\ell$ the $\ell$-torsion in $X(L)$ is not zero. Now, one has only to apply the previous two theorems.

## 2. Weil classes and admissible forms

Suppose $A$ is an abelian variety defined over $K$, $k$ is a CM-field, $\iota : k \hookrightarrow \text{End}_K^0(A)$ is an embedding and $C$ is an algebraically closed field containing $K$ (for instance, $C = \mathbb{C}$ or $C = \mathbb{Q}$). Let $\text{Lie}(A)$ be the tangent space of $A$ at the origin, a $K$-vector space. If $\sigma$ is an embedding of $k$ into $C$, let

$$n_\sigma = \dim_C \{ t \in \text{Lie}(A) \otimes_K C : \iota(\alpha)t = \sigma(\alpha)t \text{ for all } \alpha \in k \}.$$ 

Write $\overline{\sigma}$ for the composition of $\sigma$ with the involution complex conjugation of $k$.

Recall that a triple $(A, k, \iota)$ is of Weil type if $A$ is an abelian variety over an algebraically closed field $C$ of characteristic zero, $k$ is a CM-field and $\iota : k \hookrightarrow \text{End}_K^0(A)$ is an embedding such that $n_{\sigma} = n_{\overline{\sigma}}$ for all embeddings $\sigma$ of $k$ into $C$.

It is known [15] that $(A, k, \iota)$ is of Weil type if and only if $\iota$ makes $\text{Lie}(A) \otimes_K C$ into a free $k \otimes_{\mathbb{Q}} C$-module (see p. 525 of [10] for the case where $k$ is an imaginary quadratic field). Now, assume that $A = X$ and the image $\iota(k)$ contains the centre $F$ of $\text{End}_K(X) \otimes \mathbb{Q}$ (for instance, $F = k$). Notice that in the case of Weil type the degree $[k : \mathbb{Q}]$ divides $\dim(A)$; in particular, $\dim(A)$ is even.

Our goal is to construct an admissible form, using a triple $(A, k, \iota)$ of Weil type.

Recall that the degree $[k : \mathbb{Q}]$ divides $\dim(A)$, put $d = \dim(X)/[k : \mathbb{Q}]$ and consider the space of Weil classes ([1, 15, 16])

$$W_{k,X} = \text{Hom}_{k}(\Lambda_k^{2d}V(X), \mathbb{Q}(d)) \hookrightarrow \text{Hom}_{\mathbb{Q}}(\Lambda_0^{2d}V(X), \mathbb{Q}(d)) = H^{2d} (X(\mathbb{C}), \mathbb{Q}(d)).$$

Clearly, $W_{k,X}$ carries a natural structure of one-dimensional $k$-vector space. If one fixes an isomorphism of one-dimensional $\mathbb{Q}$-vector spaces $\mathbb{Q} \cong \mathbb{Q}(2d)$ then one may naturally identify $\text{Hom}_{\mathbb{Q}}(\Lambda_0^{2d}V(X), \mathbb{Q}(d))$ with $\text{Hom}_{\mathbb{Q}}(\Lambda_0^{2d}V(X), \mathbb{Q})$ and $W_{k,X}$ can be described as the space of all $2d$-linear skew-symmetric forms $\psi \in \text{Hom}_{\mathbb{Q}}(\Lambda_0^{2d}V, \mathbb{Q})$ with

$$\psi(fv_1, v_2, \ldots, v_{2d}) = \psi(v_1, fv_2, \ldots, v_{2d}) = \cdots = \psi(v_1, v_2, \ldots, fv_{2d})$$

for all $f \in F; v_1, \ldots, v_{2d} \in V(X)$. 

Yuri G. Zarhin
Torsion of abelian varieties

Since $(X, k, \ell)$ is of Weil type, all elements of $W_k$ are Hodge classes by proposition 4.4 of [1]. Therefore, by theorem 2.11 of [1] they must be also absolute Hodge cycles; cf. [1].

**Lemma 2.1.** Let $\mu_k$ be the finite multiplicative group of all roots of unity in $k$. There is a continuous character $\chi_{X,k} : G(K) \to \mu_k \subset k^*$ such that for each prime $\ell$ the subgroup

$$W_k \subset W_{k,X} \otimes Q\ell \subset H^{2d}(X(C), Q)(d) \otimes Q\ell = H^{2d}(X, Q\ell)(d)$$

is $G(K)$-stable and the action of $G(K)$ on $W_k$ is defined via the character

$$\chi_{X,k} : G(K) \to \mu_k \subset k^* = \text{Aut}_k(W_{k,X}).$$

**Proof.** Since all elements of $k$ are endomorphisms of $X$ defined over $K$, it follows easily that $W_{k,X} \otimes Q\ell$ is $G(K)$-stable and $G(K)$ acts on $W_{k,X} \otimes Q\ell$ via a certain character $\chi_{X,k,\ell} : G(K) \to [k \otimes Q\ell]^* = \prod_{\lambda \mid k_\ell} k_\lambda$.

Let us consider the $Q$-vector subspace

$$C_{\text{AH}}^d(X) \subset H^{2d}(X(C), Q)(d) \subset H^{2d}(X, Q\ell)(d)$$

of absolute Hodge classes. Then $C_{\text{AH}}^d(X)$ is $G(K)$-stable and the action of $G(K)$ on $C_{\text{AH}}^d(X)$ does not depend on $\ell$ and factors through a finite quotient (cf. [1], proposition 2.9b). Since $W_{k,X}$ consists of Hodge classes and $X$ is an abelian variety, all Weil classes are absolute Hodge classes, i.e. $W_{k,X} \subset C_{\text{AH}}^d(X)$ ([1], theorem 2.11). This implies easily that the subgroup $\text{Im} (\chi_{X,k,\ell})$ is finite and contained in $k^*$, since the intersection of $W_{k,X} \otimes Q\ell$ and $C_{\text{AH}}^d(X)$ coincides with $W_{k,X}$. (In fact, $W_{k,X}$ coincides even with the intersection of $W_{k,X} \otimes Q\ell$ and $H^{2d}(X(C), Q)(d)$.) This implies also that $\chi_{X,k,\ell}$ does not depend on the choice of $\ell$. So, we may view $\chi_{X,k,\ell}$ as the continuous homomorphism

$$\chi_{X,k} = \chi_{X,k,\ell} : G(K) \to \mu_k \subset k^*,$$

which does not depend on the choice of $\ell$. □

Let $r$ be the order of the finite group $\text{Im} (\chi_{X,k})$. Clearly, $r$ divides the order of $\mu_k$.

Let us put $Y = X^r$ and consider the Künneth chunk

$$H^{2d}(X(C), Q)(d)^{\otimes r} \subset H^{2dr}(X(C)^r, Q)(dr) = H^{2dr}(Y(C), Q)(dr)$$

of the $2dr$th rational cohomology group of $Y$. One may easily check that the tensor power

$$W_{k,X}^{\otimes r} \subset H^{2d}(X(C), Q)(d)^{\otimes r} \subset H^{2dr}(X(C)^r, Q)(dr) = H^{2dr}(Y(C), Q)(dr)$$

coincides with the space $W_{k,Y}$ of Weil classes on $Y$ attached to the ‘diagonal’ embedding

$$k \to \text{End}^0(X) \subset \text{End}^0(X^r) = \text{End}^0(Y).$$

Since the centres of $\text{End}^0(X)$ and $\text{End}^0(X^r)$ coincide, the image of $k$ in $\text{End}^0(Y)$ does contain the centre of $\text{End}^0(Y)$.

One may easily check that $G(K)$ acts on $W_{k,Y} = W_{k,X}^{\otimes r}$ via the character $\chi_{X,k}^r$, which is trivial, i.e. $W_{k,Y}$ consists of $G(K)$-invariants.
Let us fix an isomorphism of one-dimensional $\mathbb{Q}$-vector spaces $\mathbb{Q} \cong \mathbb{Q}(2dr)$ and choose a non-zero element
\[
\psi \in W_{k,Y} \subset H^{2dr}(Y,\mathbb{Q})(dr) = \text{Hom}_\mathbb{Q}(\Lambda^{2dr}_\mathbb{Q}V(Y),\mathbb{Q}).
\]
Then a skew-symmetric $2dr$-linear form $\psi$ is admissible.

Applying to $\psi$ the theorems of the previous section, we obtain the following statement, which implies the case 4 (in the hypothesis (H)) of Theorem 0.5.

**Theorem 2.2.** Assume that the centre $F$ of $\text{End}^0 X$ is a CM-field and $(X,F,id)$ is of Weil type. Let us put $d = #(\mu_F) \times 2\dim (X)/[F: \mathbb{Q}] \in \mathbb{Z}_+$. Let $L$ be an infinite Galois extension of $K$.

1. Let $\ell$ be a prime such that the $\ell$-torsion in $X(L)$ is infinite. Let $L^{(\ell)}$ be the intersection of $L$ and $K(\ell)$. Then the field extension $K(\ell)/L^{(\ell)}$ has finite degree dividing $(d, \ell - 1)$ if $\ell$ is odd and dividing 2 if $\ell = 2$. In addition, $L$ contains $\mathbb{Q}(\ell)$.
2. Let $S$ be the set of primes $\ell$ such that $X(L)$ contains a point of order $\ell$ and assume that $S$ is infinite. Then for all but finitely many $\ell \in S$ the field extension $K(\mu_\ell)/K(\mu_2) \cap L$ has degree dividing $(d, \ell - 1)$.

**Remark 2.3.** Since $[F: \mathbb{Q}]$ divides $2 \dim (X) = 2g$, one may easily find an explicit positive integer $M = M(g)$, depending only on $g$ and divisible by $(#(\mu_F) \times 2\dim (X)/[F: \mathbb{Q}])^2$.

**3. Proof of Theorem 0.5**

We may and will assume that $X$ is $K$-simple. Then the centre $F$ of $\text{End}^0 X$ is either a totally real number field or a CM-field. If $F$ is totally real then the assertion of Theorem 0.5 is proved in [20] with $N = 1$. So, further, we assume that $F$ is a CM-field. We also know that the assertion of Theorem 0.5 is true when $(X,F)$ is of Weil type (Case 4 of Hypothesis (H)).

**3.1. Cases 1 and 3 of Hypothesis (H)**

Enlarging $K$ if necessary, we may and will assume that $X$ is absolutely simple and has semistable reduction. Then the results of [14] imply that in both cases $\text{Hdg}_X$ is semisimple. This means that $(X,F,id)$ is of Weil type (cf. for instance, [14]). Now one has only to apply the result of the previous section with $d = #(\mu_F) \times 2\dim (X)/[F: \mathbb{Q}]$ and get the assertion of Theorem 0.5 with $N = M(g)$.

**3.2. Case 2 of Hypothesis (H)**

We know that the assertion of the theorem is true if $(X,F,id)$ is of Weil type. So we may assume that $(X,F,id)$ is not of Weil type.

Let us consider the trace map
\[
\text{Tr}_{\text{Lie}(X)} : F \subset \text{End}^0(X) \leftrightarrow \text{End}_K(\text{Lie}(X)) \to K \subset \mathbb{C}.
\]
Our assumption means that the image $\text{Tr}_{\text{Lie}(X)}(F)$ is not contained in $\mathbb{R}$. On the other hand, let us fix an embedding of $F$ into $\mathbb{C}$ and let $L$ be the normal closure of $F$ into $\mathbb{C}$. Clearly, $L$ is a CM-field containing $\text{Tr}_{\text{Lie}(X)}(F)$. Since $\text{Tr}_{\text{Lie}(X)}(F) \subset K$, the intersection $L \cap K$ contains an element, which is not totally real. Since any subfield of a CM-field is either totally real or CM, the field $L \cap K$ is a CM-subfield of $K$. 
Remark 3·1. If \( K \) is a number field not containing a CM-field one may give another proof, using theory of abelian \( \lambda \)-adic representations \([11]\) instead of Weil/Hodge classes. The crucial point is that in this case Serre’s tori \( T_m \) are isomorphic to the multiplicative group \( \mathbb{G}_m \) ([11], section 3·4).

Corollary 3·2. Let \( X \) be a \( K \)-simple abelian variety of odd dimension. Assume that \( K \) does not contain a CM-subfield (e.g. \( K \subset \mathbb{R} \)). If \( X(L) \) contains infinitely many points of finite order then \( L \) contains infinitely many roots of unity.

Proof. In the case of the totally real centre \( F \) this assertion is proved in ([20], theorem 6, p. 142) without restrictions on the dimension. So, in order to prove Corollary 3·2, it suffices to check that \( F \) is not a CM-field.

Assume that \( F \) is a CM-field. Since \( \dim (X) \) is odd, \( (X, F, \text{id}) \) is not of Weil type. Now, the arguments used in the proof of Case 2 imply that \( K \) contains a CM-subfield. This gives us a contradiction.

Remark 3·3. The assertion of Corollary 3·2 cannot be extended to the even-dimensional case. In Section 4 we give an explicit counterexample.

Remark 3·4. Let \( X \) be a \( g \)-dimensional abelian variety that is not necessarily \( K \)-simple and let \( F \) be the centre of \( \text{End}^{0}(X) \). Assume that

\[
\text{Tr}_{\text{Lie} (X)} (F) \subset \mathbb{R}.
\]

Then the assertion of Theorem 0·5 holds true for \( X \). Indeed, if \( Y \) is a \( K \)-simple abelian subvariety of \( X \) and \( F_Y \) is the centre of \( \text{End}^{0}(Y) \) then one may easily check that either \( F_Y \) is a totally real number field or \( (Y, F_Y, \text{id}) \) is of Weil type.

4. Example

In this section we construct an abelian surface \( X \) over \( \mathbb{Q} \) and a Galois extension \( L \) of \( \mathbb{Q} \) such that \( L \) contains only finitely many roots of unity but \( X(L) \) contains infinitely many points of finite order. Of course, the intersection of \( L \) and \( \mathbb{Q}(\ell) \) is of infinite degree over \( \mathbb{Q} \).

4·1 Let \( E \) be an elliptic curve over \( \mathbb{Q} \) without complex multiplication (e.g. \( j(E) \) is not an integer). Let us put

\[
Y = \{(e_1, e_2, e_3) \in E^3 \mid e_1 + e_2 + e_3 = 0\}.
\]

Clearly, \( Y \) is an abelian surface over \( \mathbb{Q} \) isomorphic to \( E^2 \). Denote by \( s \) an automorphism of \( Y \) induced by the cyclic permutation of factors of \( E^3 \), i.e.

\[
s(e_1, e_2, e_3) = (e_3, e_1, e_2) \quad \forall (e_1, e_2, e_3) \in Y.
\]

Let \( C \) be the cyclic subgroup in \( \text{Aut}(X) \) of order 3 generated by \( s \).

By a theorem of Serre [12] the homomorphism

\[
\rho_{\ell, E} : G(\mathbb{Q}) \to \text{Aut}_{\mathbb{Z}_\ell} (T_{\ell}(E)) \cong \text{GL}(2, \mathbb{Z}_\ell)
\]

is surjective for all but finitely many \( \ell \). Notice that the composition

\[
\text{det} \rho_{\ell, E} : G(\mathbb{Q}) \to \text{GL}(2, \mathbb{Z}_\ell) \to \mathbb{Z}_\ell^*
\]

coincides with \( \chi_{\ell} : G(K) \to \mathbb{Z}_\ell^* \) [12]. In particular, if \( \mathbb{Q}(E(\ell^\infty)) \) is the field of definition of all points on \( E \) of \( \ell \)-power order then \( \mathbb{Q}(E(\ell^\infty))/\mathbb{Q} \) is the Galois extension
with the Galois group $GL(2, \mathbb{Z})$. In addition, the cyclotomic field $\mathbb{Q}(\ell)$ is the maximal abelian subextension of $\mathbb{Q}(E(\ell^n))$ and the subgroup $Gal(\mathbb{Q}(E(\ell^n))/\mathbb{Q}(\ell)) \subset Gal(\mathbb{Q}(E(\ell^n))/\mathbb{Q})$ coincides with $SL(2, \mathbb{Z}_\ell)$.

Let us fix such an $\ell$, assuming in addition that $\ell - 1$ is divisible by 3 but not by 9. Let $\mu_{3,\ell}$ be the group of cubic roots of unity in $\mathbb{Z}_\ell^\times$. Then there exists a continuous surjective homomorphism $pr_3: \mathbb{Z}_\ell^\times \rightarrow \mu_{3,\ell}$, coinciding with the identity map on $\mu_{3,\ell}$.

Let us define field $L$ as a subextension of $\mathbb{Q}(E(\ell^n))$ such that $\mathbb{Q}(E(\ell^n))/L$ is a cubic extension, whose Galois (sub)group coincides with

$$\mu_{3,\ell} \cdot \text{id} = \{ \gamma \cdot \text{id} \mid \gamma \in \mu_{3,\ell} \} \subset GL(2, \mathbb{Z}_\ell).$$

It follows immediately that $L$ is a Galois extension of $\mathbb{Q}$ and does not contain a primitive $\ell$th root of unity. This implies that 1 and $-1$ are the only roots of unity in $L$.

Let us choose a primitive cubic root of unity $\gamma \in \mu_{3,\ell}$ and let $\iota: \mu_{3,\ell} \rightarrow C$ be the isomorphism which sends $\gamma$ to $s$.

Now, let us define $X$ as the twist of $Y$ via the cubic character

$$\kappa := \iota pr_3 \chi = \iota pr_3 \det \rho_{\ell,E}: G(\mathbb{Q}) \rightarrow \mu_{3,\ell} \rightarrow C \subset \text{Aut}(Y).$$

The Galois module $T_\ell(X)$ is the twist of $T_\ell(E)^2$ via $\kappa$. Namely,

$$T_\ell(X) = \{(v_1, v_2, v_3) \in T_\ell(E) \oplus T_\ell(E) \oplus T_\ell(E) \mid v_1 + v_2 + v_3 = 0\}$$

as the $\mathbb{Z}_\ell$-module but

$$\rho_{\ell,E}(\sigma)(v_1, v_2, v_3) = \kappa(\sigma)(\rho_{\ell,E}(\sigma)(v_1), \rho_{\ell,E}(\sigma)(v_2), \rho_{\ell,E}(\sigma)(v_3))$$

for all $\sigma \in G(\mathbb{Q})$. Now, we construct explicitly $G(L)$-invariant elements of $T_\ell(X)$. Starting with any $v \in T_\ell(E)$, put

$$w = (\gamma^{-1}v, \gamma v, v) = (\gamma^2 v, \gamma v, v) \in T_\ell(E) \oplus T_\ell(E) \oplus T_\ell(E).$$

Clearly, $w \in T_\ell(X)$ and $sw = gw$. Let us check that $w$ is $G(L)$-invariant. Clearly,

$$G(L) = \{ \sigma \in G(\mathbb{Q}) \mid \rho_{\ell,E}(\sigma) \in \mu_{3,\ell} \cdot \text{id} \}.$$ 

Let $\sigma \in G(L)$ with $\rho_{\ell,E}(\sigma) = \zeta \text{id}$, $\zeta \in \mu_{3,\ell}$. If $\zeta = 1$, i.e. $\rho_{\ell,E}(\sigma) = \text{id}$; then all elements of $V_\ell(X)$ are $\sigma$-invariant. Since $\mu_{3,\ell} = \{1, \gamma, \gamma^{-1}\}$, we may assume that $\zeta = \gamma$, i.e. $\rho_{\ell,E}(\sigma) = \gamma \cdot \text{id}$, and therefore $\det \rho_{\ell,E}(\sigma) = \gamma^2 = \gamma^{-1}$. Then

$$\rho_{\ell,E}(\sigma)(w) = \iota (pr_3(\det \rho_{\ell,E}(\sigma)))(\rho_{\ell,E}(\sigma)(\gamma^2 v), \rho_{\ell,E}(\sigma)(\gamma v), \rho_{\ell,E}(\sigma)(v)) = \iota (\gamma^2)(\gamma w) = s^2(\gamma w) = s \gamma^2 w = \gamma^2 w = w.$$ 

This proves that $w$ is $G(L)$-invariant.

Now, I claim that $X(L)$ contains infinitely many points, whose order is a power of $\ell$. Indeed, starting with a non-divisible element $v \in T_\ell(E)$ and identifying the group $X_{\ell^n}$ with the quotient $T_\ell(X)/\ell^n T_\ell(X)$, we get an $L$-rational point $(\gamma^2 v, \gamma v, v) \mod \ell^n T_\ell(X) \in T_\ell(X)/\ell^n T_\ell(X) = X_{\ell^n}$ of order $\ell^n$.

5. Another example

Let $K$ be an imaginary quadratic field with class number 1 and let $E$ be an elliptic curve over $\mathbb{Q}$ such that $\text{End}_K(E) = O_K$ is the ring of integers in $K$. In this section we
construct a Galois extension $L$ of $K$ such that $E(L)$ contains infinitely many points of finite order but the intersection of $L$ and $K(c)$ is of finite degree over $K$ (even coincides with $K$).

We write $\iota : \mathbb{C} \to \mathbb{C}$ for the complex conjugation $z \mapsto \bar{z}$. We write $R$ for $O_K$. Clearly, $\text{End}_\mathbb{Q}(E) = \mathbb{Z} \neq R$. It follows easily that
\[
\iota(ux) = \bar{u}(x) \quad \forall x \in E(\mathbb{C}), u \in R.
\]
Notice that $K$ is abelian over $\mathbb{Q}$. Since $\mathbb{Q}(c) = \mathbb{Q}(ab)$, $K \subset \mathbb{Q}(c)$ and therefore
\[
K(c) = \mathbb{Q}(c).
\]

5.1 Let $\ell$ be a prime number. We write $R_\ell$ for $R \otimes \mathbb{Z}_\ell$. It is well known that $T_\ell(E)$ is a free $R \otimes \mathbb{Z}_\ell$-module of rank 1 and therefore
\[
\text{End}_{R_\ell}(T_\ell(E)) = R_\ell, \quad \text{Aut}_{R_\ell}(T_\ell(E)) = R_\ell^*.
\]
Let us consider the corresponding $\ell$-adic representation
\[
\rho_{\ell,E} : G(\mathbb{Q}) \to \text{Aut}_{\mathbb{Z}_\ell}(T_\ell(E)) \cong \text{GL}(2, \mathbb{Z}_\ell).
\]
Clearly, $G_\ell := \rho_{\ell,E}(G(\mathbb{Q}))$ is not a subgroup of $R_\ell^* = \text{Aut}_{R_\ell}(T_\ell(E))$ but
\[
H_\ell := \rho_{\ell,E}(G(K)) \subseteq R_\ell^*.
\]
It is also known ([12], section 4.5) that
\[
H_\ell = R_\ell^*
\]
for all but finitely many primes $\ell$. Let us fix such an $\ell$, assuming in addition that $\ell$ is unramified and splits in $K$. This implies that $\ell = q\bar{q}$ for some $q \in K$ and
\[
O_K = q \cdot O_K + \bar{q} \cdot O_K, \quad R_\ell = R_q \oplus R_\bar{q}, \quad R_q = \mathbb{Z}_\ell, \quad R_\bar{q} = \mathbb{Z}_\ell.
\]
\[
qR_\ell = \ell R_q \oplus R_\bar{q} = \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell \subset \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell = R_\ell,
\]
\[
qR_\ell = R_q \oplus \ell R_\bar{q} = \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell \subset \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell = R_\ell,
\]
\[
R_\ell^* = R_q^* \times R_\bar{q}^*, \quad R_q^* = \mathbb{Z}_\ell^*, \quad R_\bar{q}^* = \mathbb{Z}_\ell^*.
\]
We also have
\[
T_\ell(E) = T_q(E) \oplus T_{\bar{q}}(E),
\]
where
\[
T_q(E) \cong R_q \cdot T_\ell(E), \quad T_{\bar{q}}(E) \cong R_{\bar{q}} \cdot T_\ell(E)
\]
are free $\mathbb{Z}_\ell$-modules of rank 1. This implies that for each positive integer $i$
\[
q^iT_q(E) = \ell^iT_q(E), \quad \bar{q}^iT_{\bar{q}}(E) = T_{\bar{q}}(E),
\]
\[
\bar{q}^iT_q(E) = \ell^iT_q(E), \quad \bar{q}^iT_{\bar{q}}(E) = T_{\bar{q}}(E)
\]
and therefore
\[
T_\ell(E)/\ell^iT_\ell(E) = T_q(E)/\ell^iT_q(E) \oplus T_{\bar{q}}(E)/\ell^iT_{\bar{q}}(E) = T_q(E)/q^iT_q(E) \oplus T_{\bar{q}}(E)/\bar{q}^iT_{\bar{q}}(E).
\]
It is also clear that multiplication by \( q^i \) is an automorphism of \( T_q(E) \) and multiplication by \( \bar{q}^i \) is an automorphism of \( T_{\bar{q}}(E) \).

It follows easily that a point \( x \in E_{\ell^i} = E_{\ell^i}/\ell^i T_{\ell^i}(E) \) satisfies \( q^i x = 0 \) (respectively \( \bar{q}^i x = 0 \)) if and only if \( x \in T_q(E)/\ell^i T_q(E) = T_q(E)/q^i T_q(E) \) (respectively \( x \in T_{\bar{q}}(E)/\ell^i T_{\bar{q}}(E) = T_{\bar{q}}(E)/\bar{q}^i T_{\bar{q}}(E) \)).

Let us put

\[
\tau := \rho_{\ell,E}(t) \in G_{\ell} \subset \Aut_{\Z}(T_{\ell}(E)).
\]

Then \( \tau^2 = \text{id} \) and

\[
\tau(R_q^* \times \{1\})\tau^{-1} = \{1\} \times R_q^* \subset R_{\ell}^*, \quad \tau(\{1\} \times R_q^*)\tau^{-1} = R_q^* \times \{1\} \subset R_{\ell}^*.
\]

It is also clear that

\[
\tau(T_q(E)) = T_q(E), \quad \tau(T_{\bar{q}}(E)) = T_{\bar{q}}(E).
\]

Let us consider the field \( K(E(\ell^\infty)) \) of definition of all points on \( E \) of \( \ell \)-power order. It is the Galois extension of \( K \) with the Galois group \( R_{\ell}^* = R_q^* \times R_{\bar{q}}^* \). It is also normal over \( Q \) and \( \Gal(K(E(\ell^\infty))/Q) = G_{\ell} \), since \( E \) is defined over \( Q \) and \( K \) is normal over \( Q \).

Let us define \( L \) as a subextension of \( K(E(\ell^\infty))/K \) such that

\[
\Gal(K(E(\ell^\infty))/L) = \{1\} \times R_q^* \subset R_{\ell}^* = R_q^* = \Gal(K(E(\ell^\infty))/K).
\]

One may easily check that \( L \) coincides with the field \( K(E(q^\infty)) \) of definition of all torsion points on \( E \) which are killed by a power of \( q \). In particular, \( E(L) \) contains infinitely many points whose order is a power of \( \ell \). Let us consider the field \( L' = \iota(L) \). Clearly, \( K \subset L' \subset K(E(\ell^\infty)) \) and \( L' \) coincides with the field \( K(E(\bar{q}^\infty)) \) of definition of all torsion points on \( E \) which are killed by a power of \( \bar{q} \). It is also clear that

\[
\Gal(K(E(\ell^\infty))/L) = \tau(\{1\} \times R_q^*)\tau^{-1} = R_q^* \times \{1\} \subset R_q^* \times R_{\bar{q}}^* = R_{\ell}^* = \Gal(K(E(\ell^\infty))/K).
\]

Since the subgroups \( \{1\} \times R_q^* \) and \( R_q^* \times \{1\} \) generate the whole group \( R_{\ell}^* = \Gal(K(E(\ell^\infty))/K) \),

\[
L \cap \iota(L) = L \cap L' = K.
\]

It follows that if \( M/K \) is a subextension of \( L/K \) such that \( M \) is normal over \( Q \) then \( M = K \). Since \( K(c) = Q(c) \), \( L \cap K(c) = L \cap Q(c) \) is a subfield of \( Q(c) \) and therefore is normal (even abelian) over \( Q \). It follows that

\[
L \cap K(c) = K.
\]

6. Abelian subextensions

The following statement may be viewed as a variant of Theorem 0.5 for arbitrary abelian varieties over number fields.

**Theorem 6.1.** Let \( X \) be an abelian variety over a number field \( K \). Then

1. if for some prime \( \ell \) the \( \ell \)-primary part of \( \text{TORS}(X(L)) \) is infinite then \( L \) contains an abelian infinite subextension \( E \subset L \) such that \( \Gal(E/K) \cong \Z_{\ell} \) and \( E/K \) is ramified only at divisors of \( \ell \);

2. let \( P = P(X,L) \) be the set of primes \( \ell \) such that \( X(L) \) contains a point of order \( \ell \). If \( P \) is infinite then for all but finitely many primes \( \ell \in P \) there exist a finite
subextension \( E^{(t)} \subset L \) such that \( E^{(t)}/K \) is a ramified cyclic extension which is unramified outside divisors of \( \ell \). In addition, the degree \( [E^{(t)}: K] \) is prime to \( \ell \) and degree \( [E^{(t)}: K] \) tends to infinity while \( \ell \) tends to infinity.

**Corollary 6.2 (Theorem of Bogomolov).** If \( \text{TORS}(X(L)) \) is infinite then \( L \) contains an infinite abelian subextension of \( K \).

**Proof of Theorem 6.1.** First, we may and will assume that \( X \) is \( K \)-simple, i.e. the centre \( F \) of the endomorphism algebra of \( X \) is a number field.

Secondly, there is a positive integer \( d \) such that if \( m \) is a positive integer with \( \varphi(m) \leq 2g = 2\dim(X) \) then \( d \) is divisible by \( m \).

Thirdly, let \( \lambda \) be a prime ideal in \( \mathcal{O}_F \) dividing a prime number \( \ell \). Then, in the notation of Section 1, the following statement is true.

**Lemma 6.3.**

1. The composition
   \[ \pi_\lambda := (\det_{F_\lambda} \rho_{\lambda, X})^d : G(K) \to \text{Aut}_{F_\lambda} V_\lambda(X) \to F_\lambda^* \to F_\lambda^* \]
   is an abelian representation of \( G(K) \) unramified outside divisors of \( \ell \).

2. For all but finitely many \( \lambda \) the composition
   \[ \bar{\pi}_\lambda := (\det_{F_\lambda} \bar{\rho}_{\lambda, X})^d : G(K) \to \text{Aut}_{OF/\lambda}X_\lambda \to (OF/\lambda)^* \to (OF/\lambda)^* \]
   is an abelian representation of \( G(K) \) unramified outside divisors of \( \ell \) and its image is a cyclic group.

We will prove this lemma at the end of this section. Now, let us finish the proof of Theorem 6.1, assuming the validity of the lemma.

First, notice that the ratio
\[ e = 2\dim(X)/[F:Q] \]
is a positive integer. Secondly, for all but finitely many primes \( p \) there exists a finite collection of Weil numbers, i.e. certain algebraic integers \( \{\alpha_1, \ldots, \alpha_e\} \subset F(a) \) such that

(a) (Weil’s condition) there is a positive integer \( q > 1 \) such that \( q \) is an integral power of \( p \) and all \( |\alpha_i|^q = q \) for all embeddings \( F(a) \subset \mathbb{C} \);

(b) for all \( \ell \neq p \) and \( \lambda \) the product \( (\prod \alpha_i) \in \mathcal{O}_F \) and the group \( \text{Im}(\pi_\lambda) \) contains \( \prod \alpha_i^d \);

(c) for all but finitely many \( \lambda \) the subgroup \( \text{Im}(\bar{\pi}_\lambda) \) contains \( (\prod \alpha_i)^d \bmod \lambda \in (OF/\lambda)^* \).

Indeed, let us choose a prime ideal \( \mathfrak{v} \) in the ring \( \mathcal{O}_K \) of all algebraic integers in \( K \) such that \( X \) has good reduction at \( \mathfrak{v} \). Let
\[ \text{Fr}_\mathfrak{v} \in \text{Im}(\rho_{\lambda, X}) \subset \text{Aut}_{F_\lambda} V_\lambda(X) \]
be the Frobenius element \( \text{Fr}_\mathfrak{v} \) at \( \mathfrak{v} \) (defined up to conjugacy) ([9, 11]). Then the set of its eigenvalues belongs to \( F(a) \), does not depend on the choice of \( \lambda \) and satisfies all the desired properties with \( p \) the residual characteristic of \( \mathfrak{v} \) and \( q = \#(O_K/\mathfrak{v})([13], \text{ chapter 7, proposition 7.21 and proof of proposition 7.23}).
This implies that the field \(E'\) of \(\ker(\pi_\lambda)\)-invariants is an abelian subextension of \(L\), unramified outside divisors of \(\ell\) and \(\Gal(E'/K)\) is isomorphic to \(\Im(\pi_\lambda)\). Choosing a collection of Weil numbers attached to prime \(p \neq \ell\), we easily conclude that \(\Im(\pi_\lambda)\) is an infinite commutative \(\ell\)-adic Lie group \([11]\) and therefore there is a continuous quotient of \(\Im(\pi_\lambda)\), isomorphic to \(\mathbb{Z}_\ell\). One has to take as \(E\) the subextension of \(E'\) corresponding to this quotient.

**Proof of assertion 2.** We know that for all but finitely many \(\ell \in P\) there exists \(\lambda\) dividing \(\ell\) such that \(X_\lambda\) consists of \(G(L)\)-invariants. This means that the field \(E^{(\ell)}\) of \(\ker(\pi_\lambda)\)-invariants is a cyclic subextension of \(L\), unramified outside divisors of \(\ell\) and \(\Gal(E^{(\ell)}/K)\) is isomorphic to \(\Im(\pi_\lambda)\). In order to prove that \([E^{(\ell)}: K]\) tends to infinity, let us assume that there exist an infinite subset \(P' \subset P\) and a positive integer \(D\) such that \#(\Gal(E^{(\ell)}/K)) \geq [E^{(\ell)}: K]\) divides \(D\) for all \(\ell \in P'\). This means that

\[
\pi_\lambda^D : G(K) \to (O_F/\lambda)^*
\]

is a trivial homomorphism for infinitely many \(\lambda\). In order to get a contradiction, let us choose a collection of Weil numbers \(\{\alpha_1, \ldots, \alpha_c\}\) enjoying the properties described above.

Clearly the product \(\alpha_S := \prod \alpha_i^d\) is not a root of unity. In addition, if \(\alpha_S \in O_F\) then there are only finitely many \(\lambda\) such that \(\alpha_S^D - 1\) is an element of \(\lambda\). Therefore for all but finitely many \(\lambda\) the group

\[
\Im((\pi_\lambda)^D) \subset (O_F/\lambda)^*
\]

contains an element of type \(\alpha_S^D \mod \lambda\) different from 1. This implies that \((\pi_\lambda)^D\) is a non-trivial homomorphism for all but finitely many \(\lambda\). This gives the desired contradiction.

**Proof of Lemma 6.3.** Let \(v\) be a prime ideal in the ring \(O_K\) of all algebraic integers in \(K\). We write \(I_v \subset G(K)\) for the corresponding inertia subgroup defined up to conjugacy. Assume that the residual characteristic of \(v\) is different from \(\ell\). It is known \([4]\) that for any \(\sigma \in I_v\) there exists a positive integer \(m\) such that \(\rho_{\ell,X}(\sigma)^m\) is an unipotent operator in \(V_\ell(X)\) and its characteristic polynomial has coefficients in \(Z\). This implies that if \(m\) is the smallest integer enjoying this property then the characteristic polynomial is divisible by the \(m\)th cyclotomic polynomial. This implies that \(2g \geq \varphi(m)\) and therefore \(m\) divides \(d\). Since \(V_\ell(X)\) is a Galois-invariant subspace of \(V_\ell(T_\ell(X))\) and (for all but finitely many \(\ell\)) \(X_\lambda\) is a Galois-invariant subspace of \(T_\ell(X)/T_\ell(X)\), a Galois automorphism \(\sigma^d\) acts as an unipotent operator in \(V_\ell(X)\) and (for all but finitely many \(\lambda\)) in \(X_\lambda\). One has only to recall that the determinant of an unipotent operator is always 1.

**Acknowledgement.** I would like to thank the MPI für Mathematik for its hospitality.

**REFERENCES**

[1] P. Deligne, Hodge cycles on abelian varieties (notes by J. S. Milne), in *Hodge cycles, motives and Shimura varieties*. Lecture Notes in Math., vol. 900 (Springer-Verlag, 1982), pp. 9–100.
Torsion of abelian varieties

[2] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.* 73 (1983), 349–366.

[3] G. Faltings. Complements to Mordell, in *Rational points*. Aspects of Mathematics, vol. E6 (Friedr. Viehweg & Sohn, 1984), pp. 204–227.

[4] A. Grothendieck. Modèles de Néron et monodromie. in *Groupes de monodromie en géométrie algébrique*. SGA7 I, Lecture Notes in Math., vol. 288 (Springer-Verlag, 1972), pp. 313–523.

[5] H. Imai. A remark on the rational points of abelian varieties with values in cyclotomic $\mathbb{Z}_p$-extensions. *Proc. Japan Acad.* 51 (1975), 12–16.

[6] D. Masser and G. Wüstholz. Refinements for the Tate conjecture for abelian varieties, in *Abelian varieties* (Walter de Gruyter, 1995), pp. 211–223.

[7] B. Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.* 18 (1972), 183–266.

[8] D. Mumford. *Abelian varieties*, 2nd edn (Oxford University Press, 1974).

[9] K. A. Ribet. Galois action on division points of abelian varieties with real multiplication. *Amer. J. Math.* 98 (1976), 751–804.

[10] K. A. Ribet. Torsion points of abelian varieties in cyclotomic extensions, pp. 315–319. Appendix to: N. M. Katz, S. Lang. Finiteness theorems in geometric classfield theory. *L'Enseign. Math.* 27 (1981), 285–319.

[11] J.-P. Serre. *Abelian $\ell$-adic representations and elliptic curves*, 2nd edn (Addison-Wesley, 1989).

[12] J.-P. Serre. Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. *Invent. Math.* 15 (1972), 259–331.

[13] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publ. Math. Soc. Japan, vol. 11 (Princeton University Press, 1971).

[14] A. Silverberg and Yu. G. Zarhin. Hodge groups of abelian varieties with purely multiplicative reduction. *Izvestiya Rossiskoi Akademii Nauk, ser. mat.* 60 (1996), 149–158; *Izvestiya: Mathematics* 60 (1996), 379–389.

[15] A. Silverberg and Yu. G. Zarhin. Connectedness extensions for abelian varieties. *Math. Zeit.* 228 (1998), 387–403.

[16] A. Weil. Abelian varieties and the Hodge ring, in *Œuvres scientifiques*, vol. III (Springer-Verlag, 1979), pp. 421–429.

[17] K. Wingberg. On the rational points of Abelian varieties over $\mathbb{Z}_p$-extensions of number fields. *Math. Ann.* 279 (1987), 9–24.

[18] Yu. G. Zarhin. Torsion of Abelian varieties over fields in finite characteristic. *Math. Notes* 22 (1978), 493–498.

[19] Yu. G. Zarhin. A finiteness theorem for unpolarized Abelian varieties over number fields with prescribed places of bad reduction. *Invent. Math.* 79 (1985), 309–321.

[20] Yu. G. Zarhin. Endomorphisms and torsion of abelian varieties. *Duke Math. J.* 54 (1987), 131–145.

[21] Yu. G. Zarhin. Torsion of Abelian varieties over $GL(2)$-extensions of number fields. *Math. Ann.* 284 (1989), 631–646.

[22] Yu. G. Zarhin. Torsion and endomorphisms of abelian varieties over infinite extensions of number fields. *Izv. Akad. Nauk SSSR, ser. mat.* 55 (1991); *Math. USSR Izv.* 38 (1992), 647–657.

[23] S. Zhang. Equidistribution of small points on abelian varieties. *Ann. of Math.* 147 (1998), 159–165.

[24] R. Coleman. Ramified torsion points on curves. *Duke Math. J.* 54 (1987), 615–640.