1. Introduction

As usual, \( \mathbb{Z}, \mathbb{Q}, \mathbb{C} \) denote the ring of integers, the field of rational numbers and the field of complex numbers respectively. Let \( p \) be an odd prime. Recall that \( p \) is called a Fermat prime if \( p = 2^{2^r} + 1 \) for some positive integer \( r \); e.g., 3, 5, 17, 257 are Fermat prime.

Let us fix a primitive \( p \)-th root of unity \( \zeta_p \in \mathbb{C} \).

Let \( \mathbb{Q}(\zeta_p) \) be the \( p \)-th cyclotomic field. It is well-known that \( \mathbb{Q}(\zeta_p) \) is a CM-field. If \( p \) is a Fermat prime then the only CM-subfield of \( \mathbb{Q}(\zeta_p) \) is \( \mathbb{Q}(\zeta_p) \) itself, since the Galois group of \( \mathbb{Q}(\zeta_p)/\mathbb{Q} \) is a cyclic 2-group, whose only element of order 2 acts as the complex conjugation. All other subfields of \( \mathbb{Q}(\zeta_p) \) are totally real.

Let \( f(x) \in \mathbb{C}[x] \) be a polynomial of degree \( n \geq 4 \) without multiple roots. Let \( C_{f,p} \) be a smooth projective model of the smooth affine curve

\[
y^p = f(x).
\]

It is well-known (\[6\], pp. 401–402, \[8\], Prop. 1 on p. 3359, \[13\], p. 148) that the genus \( g(C_{f,p}) \) of \( C_{f,p} \) is \( (p-1)(n-1)/2 \) if \( p \) does not divide \( n \) and \( (p-1)(n-2)/2 \) if it does. The map

\[
(x, y) \mapsto (x, \zeta_p y)
\]

gives rise to a non-trivial birational automorphism

\[
\delta_p : C_{f,p} \to C_{f,p}
\]
of period \( p \).

Let \( J^{(f,p)} = J(C_{f,p}) \) be the jacobian of \( C_{f,p} \); it is an abelian variety, whose dimension equals \( g(C_{f,p}) \). We write \( \text{End}(J^{(f,p)}) \) for the ring of endomorphisms of \( J^{(f,p)} \). By functoriality, \( \delta_p \) induces an automorphism of \( J^{(f,p)} \) which we still denote by \( \delta_p \); it is known (\[13\], p. 149, \[14\], p. 448) that

\[
\delta_p^{-1} + \cdots + \delta_p + 1 = 0
\]
in \( \text{End}(J^{(f,p)}) \). This gives us an embedding

\[
\mathbb{Z}[\zeta_p] \cong \mathbb{Z}[\delta_p] \subset \text{End}(J^{(f,p)})
\]
(\[13\], p. 149, \[14\], p. 448)).

Our main result is the following statement.

---

Partially supported by the NSF.
Theorem 1.1. Let $K$ be a subfield of $\mathbb{C}$ such that all the coefficients of $f(x)$ lie in $K$. Assume also that $f(x)$ is an irreducible polynomial in $K[x]$ of degree $n \geq 5$ and its Galois group over $K$ is either the symmetric group $S_n$ or the alternating group $A_n$. Then $\mathbb{Z}[\delta_p]$ is a maximal commutative subring in $\text{End}(J^{(f,p)})$. If $p$ is a a Fermat prime (e.g., $p = 3, 5, 17, 257$) then

$$\text{End}(J^{(f,p)}) = \mathbb{Z}[\delta_p] \cong \mathbb{Z}[\zeta_p].$$

When $p = 3$ one may obtain an additional information about Hodge classes on self-products of the corresponding trigonal jacobian.

Theorem 1.2. Let $K$ be a subfield of $\mathbb{C}$ such that all the coefficients of $f(x)$ lie in $K$. Assume also that $f(x)$ is an irreducible polynomial in $K[x]$ of degree $n \geq 5$ and its Galois group over $K$ is either the symmetric group $S_n$ or the alternating group $A_n$. If $3$ does not divide $n - 1$ then:

(i) Every Hodge class on each self-product of $J^{(f,3)}$ could be presented as a linear combination of products of divisor classes. In particular, the Hodge conjecture is true for each self-product of $J^{(f,3)}$.

(ii) If $K$ is a number field containing $\sqrt{-3}$ then every Tate class on each self-product of $J^{(f,3)}$ could be presented as a linear combination of products of divisor classes. In particular, the Tate conjecture is true for each self-product of $J^{(f,3)}$.

Example 1.3. The polynomial $x^n - x - 1 \in \mathbb{Q}[x]$ has Galois group $S_n$ over $\mathbb{Q}$ ([13], p. 42). Therefore the ring of endomorphism (over $\mathbb{C}$) of the jacobian $J(C(n,3))$ of the curve $C(n,3) : y^3 = x^n - x - 1$ is $\mathbb{Z}[\zeta_n]$ if $n \geq 5$.

If $n = 3k - 1$ for some integer $k \geq 2$ then all Hodge classes on each self-products of $J(C(n,3))$ could be presented as linear combinations of products of divisor classes. In particular, the Hodge conjecture is true for all these self-products. Notice that $J(C(n,3))$ is an abelian variety defined over $\mathbb{Q}$ of dimension $n - 1 = 3k - 2$.

Remarks 1.4. (i) If $f(x) \in K[x]$ then the curve $C_{f,p}$ and its jacobian $J^{(f,p)}$ are defined over $K$. Let $K_a \subset \mathbb{C}$ be the algebraic closure of $K$. Clearly, all endomorphisms of $J^{(f,p)}$ are defined over $K_a$. This implies that in order to prove Theorem 1.3, it suffices to check that $\mathbb{Z}[\delta_p]$ is a maximal commutative subring in the ring of $K_a$-endomorphisms of $J^{(f,p)}$ or equivalently, that $\mathbb{Q}[\delta_p]$ is a maximal commutative $\mathbb{Q}$-subalgebra in the algebra of $K_a$-endomorphisms of $J^{(f,p)}$.

(ii) Assume that $p = 3$ and $\mathbb{Z}[\delta_3] = \text{End}(J^{(f,3)})$. The endomorphism algebra $\text{End}(J^{(f,p)}) = \text{End}(J^{(f,p)}) \otimes \mathbb{Q}$ is the imaginary quadratic field $\mathbb{Q}(\sqrt{-3})$. There are exactly two embeddings

$$\sigma, \bar{\sigma} : \mathbb{Q}(\delta_3) \hookrightarrow K_a \subset \mathbb{C}$$

and they are complex-conjugate. We have

$$\mathbb{Q}(\delta_3) \otimes \mathbb{Q} \mathbb{C} = \mathbb{C} \oplus \mathbb{C}.$$

By functoriality, $\mathbb{Q}(\delta_3)$ acts on the $\mathbb{C}$-vector space $H^{1,0}(J^{(f,3)}) = \Omega^1(J^{(f,3)})$ of differentials of the fist kind. This action gives rise to a splitting of the $\mathbb{Q}(\delta_3) \otimes \mathbb{Q} \mathbb{C} = \mathbb{C} \oplus \mathbb{C}$-module

$$H^{1,0}(J^{(f,3)}) = H^{1,0}_\sigma \oplus H^{1,0}_{\bar{\sigma}}.$$
The dimensions $n_\sigma := \dim C(H^1_{\sigma})$ and $n_{\bar{\sigma}} := \dim C(H^1_{\bar{\sigma}})$ are called the *multiplicities* of $\sigma$ and $\bar{\sigma}$ respectively. Clearly, $n_\sigma$ (resp. $n_{\bar{\sigma}}$) coincides with the multiplicity of the eigenvalue $\sigma(\delta_3)$ (resp. $\bar{\sigma}(\delta_3)$) of the induced $C$-linear operator

$$\delta_3^\natural : \Omega^1(J^{(f,3)}) \to \Omega^1(J^{(f,3)}).$$

By a theorem of Ribet ([1], Th. 3 on p. 526), if the multiplicities $n_\sigma$ and $n_{\bar{\sigma}}$ are relatively prime and $\End^C(J^{(f,3)}) = Q(\delta_3)$ then every Hodge class on each self-product of $J^{(f,3)}$ could be presented as a linear combination of products of divisor classes. Therefore, the assertion (i) of Theorem 1.1 would follow from Theorem 1.1 (with $p = 3$) if we know that the multiplicities $n_\sigma$ and $n_{\bar{\sigma}}$ are relatively prime while 3 does not divide $n - 1$.

(iii) One may easily check that $n_\sigma$ (resp. $n_{\bar{\sigma}}$) coincides with the multiplicity of the eigenvalue $\sigma(\delta_3)$ (resp. $\bar{\sigma}(\delta_3)$) of the induced $C$-linear operator

$$\delta_3^\natural : \Omega^1(C^{(f,3)}) \to \Omega^1(C^{(f,3)}).$$

2. Permutation groups and permutation modules

Let $B$ be a finite set consisting of $n \geq 5$ elements. We write $\Perm(B)$ for the group of permutations of $B$. A choice of ordering on $B$ gives rise to an isomorphism

$$\Perm(S) \cong S_n.$$  

We write $\Alt(B)$ for the only subgroup in $\Perm(B)$ of index 2. Clearly, $\Alt(B)$ is normal and isomorphic to the alternating group $A_n$. It is well-known that $\Alt(B)$ is a simple non-abelian group of order $n!/2$. Let $G$ be a subgroup of $\Perm(B)$.

Let $F$ be a field. We write $F^B$ for the $n$-dimensional $F$-vector space of maps $h : B \to F$. The space $F^B$ is provided with a natural action of $\Perm(B)$ defined as follows. Each $s \in \Perm(B)$ sends a map $h : B \to F_2$ into $sh : b \mapsto h(s^{-1}(b))$. The permutation module $F^B$ contains the $\Perm(B)$-stable hyperplane

$$(F^B)^0 = \{ h : B \to F \mid \sum_{b \in B} h(b) = 0 \}$$

and the $\Perm(B)$-invariant line $F \cdot 1_B$ where $1_B$ is the constant function 1. The quotient $F^B/(F^B)^0$ is a trivial 1-dimensional $\Perm(B)$-module.

Clearly, $(F^B)^0$ contains $F \cdot 1_B$ if and only if $\text{char}(F)$ divides $n$. If this is not the case then there is a $\Perm(B)$-invariant splitting

$$F^B = (F^B)^0 \oplus F \cdot 1_B.$$  

Clearly, $F^B$ and $(F^B)^0$ carry natural structures of $G$-modules. Their (Brauer) characters depend only on characteristic of $F$.

Let us consider the case of $F = Q$. Then the character of $Q^B$ sends each $g \in G$ into the number of fixed points of $g$ ([14], ex. 2.2,p.12); it takes on values in $Z$ and called the *permutation character* of $B$. Let us denote by $\chi = \chi_B : G \to Q$ the character of $(Q^B)^0$.

It is known that the $Q[G]$-module $(Q^B)^0$ is absolutely simple if and only if $G$ acts doubly transitively on $B$ ([15], ex. 2.6, p. 17). Clearly, $1 + \chi$ is the permutation character. In particular, $\chi$ also takes on values in $Z$.

Now, let us consider the case of $F = F_p$.

If $p \mid n$ then let us define the $\Perm(B)$-module

$$(F^B_p)^0 := (F^B_p)^0/(F_p \cdot 1_B).$$
If $p$ does not divide $n$ then let us put

$$(\mathbb{F}_p^B)^0 := (\mathbb{F}_p^B)^0.$$  

**Remark 2.1.** Clearly, $\dim_{\mathbb{F}_p}(\mathbb{F}_p^B)^0 = n - 1$ if $n$ is not divisible by $p$ and $\dim_{\mathbb{F}_p}(\mathbb{F}_p^B)^0 = n - 2$ if $p \mid n$. In both cases $(\mathbb{F}_p^B)^0$ is a faithful $G$-module.

One may easily check that if the $\mathbb{F}_p[G]$-module $(\mathbb{F}_p^B)^0$ is absolutely simple then the $\mathbb{Q}[G]$-module $(\mathbb{Q}^B)^0$ is also absolutely simple and therefore $G$ acts doubly transitively on $B$.

Let $G^{(p)}$ be the set of $p$-regular elements of $G$. Clearly, the Brauer character of the $G$-module $\mathbb{F}_p^B$ coincides with the restriction of $1 + \chi_B$ to $G^{(p)}$. This implies easily that the Brauer character of the $G$-module $(\mathbb{F}_p^B)^0$ coincides with the restriction of $\chi_B$ to $G^{(p)}$.

**Remark 2.2.** Let us denote by $\phi_B = \phi$ the Brauer character of the $G$-module $(\mathbb{F}_p^B)^0$. One may easily check that $\phi_B$ coincides with the restriction of $\chi_B$ to $G^{(p)}$ if $p$ does not divide $n$ and with the restriction of $\phi_B - 1$ to $G^{(p)}$ if $p \mid n$. In both cases $\phi_B$ takes on values in $\mathbb{Z}$.

**Example 2.3.** Suppose $n = p = 5$ and $G = \text{Alt}(B) \cong A_5$. Then in the notations of [1], p. 2 and [3], p. 2 $\chi_B = 1 + \chi_4$ and the restriction of $\phi_B - 1 = \chi_4 - 1$ to $G^{(p)}$ coincides with absolutely irreducible Brauer character $\varphi_2$. This implies that the $\text{Alt}(B)$-module $(\mathbb{F}_p^B)^0$ is absolutely simple.

The following elementary assertion is based on Lemma 7.1 on p. 52 of [12] and Th. 9.2 on p. 145 of [4]. (The case of $p = 2$ is Lemma 5.1 of [2].)

**Lemma 2.4.** Assume that $G$ acts doubly transitively on $B$. If $p$ does not divide $n$ then $\text{End}_G((\mathbb{F}_p^B)^0) = \mathbb{F}_p$. In particular, if the $G$-module $(\mathbb{F}_p^B)^0$ is semisimple then it is absolutely simple.

**Proof.** It suffices to check that $\dim_{\mathbb{F}_p}(\text{End}_G((\mathbb{F}_p^B)^0)) \leq 1$. In order to do that, recall that the double transitivity implies that $\dim_{\mathbb{F}_p}(\text{End}_G((\mathbb{F}_p^B)^0)) = 2$ (Lemma 7.1 on p. 52 of [12]). Now the desired inequality follows easily from the existence of the $G$-invariant splitting

$$\mathbb{F}_p^B = (\mathbb{F}_p^B)^0 \oplus \mathbb{F}_p \cdot 1_B.$$  

**Remark 2.5.** Assume that $n = \#(B)$ is divisible by $p$. Let us choose $b \in B$ and let $G' := G_b$ be the stabilizer of $b$ in $G$ and $B' = B \setminus \{b\}$. Then $n' = \#(B') = n - 1$ is not divisible by $p$ and there is a canonical isomorphism of $G'$-modules

$$(\mathbb{F}_p^{B'})^0 \cong (\mathbb{F}_p^B)^0$$

defined as follows. First, there is a natural $G'$-equivariant embedding $\mathbb{F}_p^{B'} \subset \mathbb{F}_p^B$ which could be obtained by extending each $h : B' \to \mathbb{F}_p$ to $B$ by letting $h(b) = 0$. Second, this embedding identifies $(\mathbb{F}_p^{B'})^0$ with a hyperplane of $(\mathbb{F}_p^B)^0$ which does not contain $1_B$. Now the composition

$$(\mathbb{F}_p^{B'})^0 = (\mathbb{F}_p^{B'})^0 \subset (\mathbb{F}_p^B)^0 \to (\mathbb{F}_p^B)^0/(\mathbb{F}_p \cdot 1_B) = (\mathbb{F}_p^B)^0$$


gives us the desired isomorphism. This implies that if the $G_0$-module $(\mathbf{F}_p^B)^0$ is absolutely simple then the $G$-module $(\mathbf{F}_p^B)^0$ is also absolutely simple.

For example, if $G = \text{Perm}(B)$ (resp. $\text{Alt}(B)$) then $G_0 = \text{Perm}(B')$ (resp. $\text{Alt}(B')$) and therefore the $\text{Perm}(B')$-modules (resp. $\text{Alt}(B')$)-modules $(\mathbf{F}_p^B)^0$ and $(\mathbf{F}_p^B)^0$ are isomorphic. We use this observation in order to prove the following statement.

The following assertion goes back to Dickson.

**Lemma 2.6.** Assume that $G = \text{Perm}(B)$ or $\text{Alt}(B)$. Then the $G$-module $(\mathbf{F}_p^B)^0$ is absolutely simple.

**Proof.** In light of Example 2.3, we may assume that $(n, p) \neq (5, 5)$. In light of Remark 2.5 we may assume that $p$ does not divide $n$ and therefore $$(\mathbf{F}_p^B)^0 = (\mathbf{F}_p^B)^0.$$ The natural representation of $\text{Perm}(B) = S_n$ in $(\mathbf{F}_p^B)^0$ is irreducible (3, Th. 5.2 on p. 133).

Since $\text{Alt}(B)$ is normal in $\text{Perm}(B)$, the $\text{Alt}(B)$-module $(\mathbf{F}_p^B)^0$ is semisimple, thanks to Clifford’s theorem ([2], §49, Th. 49.2). Since $n \geq 5$, the action of $\text{Alt}(B) \cong A_n$ on $B \cong \{1, \ldots, n\}$ is doubly transitive. Applying Lemma 2.4, we conclude that the $\text{Alt}(B)$-module $(\mathbf{F}_p^B)^0$ is absolutely simple. (See also [19].) \qed

3. CYCLIC COVERS AND JACOBIANS

Throughout this paper we fix a prime $p$ and assume that $K$ is a field of characteristic zero. We fix its algebraic closure $K_\alpha$ and write $\text{Gal}(K)$ for the absolute Galois group $\text{Aut}(K_\alpha/K)$. We also fix in $K_\alpha$ a primitive $p$th root of unity $\zeta$.

Let $f(x) \in K[x]$ be a separable polynomial of degree $n \geq 4$. We write $\mathfrak{A}_f$ for the set of its roots and denote by $L = L_f = K(\mathfrak{A}_f) \subset K_\alpha$ the corresponding splitting field. As usual, the Galois group $\text{Gal}(L/K)$ is called the Galois group of $f$ and denoted by $\text{Gal}(f)$. Clearly, $\text{Gal}(f)$ permutes elements of $\mathfrak{A}_f$ and the natural map of $\text{Gal}(f)$ into the group $\text{Perm}(\mathfrak{A}_f)$ of all permutations of $\mathfrak{A}_f$ is an embedding. We will identify $\text{Gal}(f)$ with its image and consider it as a permutation group of $\mathfrak{A}_f$. Clearly, $\text{Gal}(f)$ is transitive if and only if $f$ is irreducible in $K[x]$. Therefore the $\text{Gal}(f)$-module $(\mathbf{F}_p^{\mathfrak{A}_f})^0$ is defined. The canonical surjection

$$\text{Gal}(K) \twoheadrightarrow \text{Gal}(f)$$

provides $(\mathbf{F}_p^{\mathfrak{A}_f})^0$ with canonical structure of the $\text{Gal}(K)$-module via the composition

$$\text{Gal}(K) \twoheadrightarrow \text{Gal}(f) \subset \text{Perm}(\mathfrak{A}_f) \subset \text{Aut}((\mathbf{F}_p^{\mathfrak{A}_f})^0).$$

Let us put

$$V_{f,p} = (\mathbf{F}_p^{\mathfrak{A}_f})^0.$$  

Let $C = C_{f,p}$ be the smooth projective model of the smooth affine $K$-curve $y^p = f(x)$.

So, $C$ is a smooth projective curve defined over $K$. The rational function $x \in K(C)$ defined a finite cover $\pi : C \to \mathbf{P}^1$ of degree $p$. Let $B' \subset C(K_\alpha)$ be the set of ramification points. Clearly, the restriction of $\pi$ to $B'$ is an injective map.
\( \pi : B' \hookrightarrow \mathbf{P}^1(K_\alpha) \), whose image is the disjoint union of \( \infty \) and \( \mathfrak{R}_f \) if \( p \) does not divide \( \deg(f) \) and just \( \mathfrak{R}_f \) if it does. We write
\[
B = \pi^{-1}(\mathfrak{R}_f) = \{ (\alpha, 0) \mid \alpha \in \mathfrak{R}_f \} \subset B' \subset C(K_\alpha).
\]
Clearly, \( \pi \) is ramified at each point of \( B \) with ramification index \( p \). We have \( B' = B \) if and only if \( n \) is divisible by \( p \). If \( n \) is not divisible by \( p \) then \( B' \) is the disjoint union of \( B \) and a single point \( \infty' := \pi^{-1}(\infty) \); in addition, the ramification index of \( \pi \) at \( \pi^{-1}(\infty) \) is also \( p \). If \( p \) does divide \( n \) then \( \pi^{-1}(\infty) \) consists of \( p \) unramified points denoted by \( \infty_1, \ldots, \infty_p \). This implies that the inverse image \( \pi'(n(\infty)) = n\pi'(\infty) \) of the divisor \( n(\infty) \) is always divisible by \( p \) in the divisor group of \( C \). Using Hurwitz’s formula, one may easily compute genus \( g = g(C) = g(C_{p,f}) \) of \( C \) ([18], pp. 401–402, [13], Prop. 1 on p. 3359, [14], p. 148). Namely, \( g \) is \( (p - 1)(n - 1)/2 \) if \( p \) does not divide \( p \) and \( (p - 1)(n - 2)/2 \) if it does. See §1 of [18] for an explicit description of a smooth complete model of \( C \) (when \( n > p \)).

Assume that \( K \) contains \( \zeta \). There is a non-trivial birational automorphism of \( C \)
\[
\delta_p : (x, y) \mapsto (x, \zeta y).
\]
Clearly, \( \delta_p^n \) is the identity map and the set of fixed points of \( \delta_p \) coincides with \( B' \).

Let \( J^{(f,p)} = J(C) = J(C_{f,p}) \) be the jacobian of \( C \). It is a \( g \)-dimensional abelian variety defined over \( K \) and one may view \( \delta_p \) as an element of
\[
\text{Aut}(C) \subset \text{Aut}(J(C)) \subset \text{End}(J(C))
\]
such that
\[
\delta_p \neq \text{Id}, \quad \delta_p^n = \text{Id}
\]
where \( \text{Id} \) is the identity endomorphism of \( J(C) \). Here \( \text{End}(J(C)) \) stands for the ring of all \( K_\alpha \)-endomorphisms of \( J(C) \). As usual, we write \( \text{End}^0(J(C)) = \text{End}^0(J^{(f,p)}) \) for the corresponding \( \mathbf{Q} \)-algebra \( \text{End}(J(C)) \otimes \mathbf{Q} \).

Lemma 3.1. \( \text{Id} + \delta_p + \cdots + \delta_p^{n-1} = 0 \) in \( \text{End}(J(C)) \). Therefore the subring \( \mathbf{Z}[[\delta_p]] \subset \text{End}(J(C)) \) is isomorphic to the ring \( \mathbf{Z}[\zeta_p] \) of integers in the \( p \)th cyclotomic field \( \mathbf{Q}(\zeta_p) \). The \( \mathbf{Q} \)-subalgebra
\[
\mathbf{Q}[[\delta_p]] \subset \text{End}^0(J(C)) = \text{End}^0(J^{(f,p)})
\]
is isomorphic to \( \mathbf{Q}(\zeta_p) \).

Proof. See [13], p. 149, [14], p. 448. \( \square \)

Remarks 3.2. (i) Assume that \( p \) is odd and \( n = \deg(f) \) is divisible by \( p \) say, \( n = pm \) for some positive integer \( m \). Then \( n \geq 5 \).

Let \( \alpha \in K_\alpha \) be a root of \( f \) and \( K_1 = K(\alpha) \) be the corresponding subfield of \( K_\alpha \). We have
\[
f(x) = (x - \alpha)f_1(x)
\]
with \( f_1(x) \in K_1[x] \). Clearly, \( f_1(x) \) is a separable polynomial over \( K_1 \) of odd degree \( pm - 1 = n - 1 \geq 4 \). It is also clear that the polynomials
\[
h(x) = f_1(x + \alpha), h_1(x) = x^{n-1}h(1/x) \in K_1[x]
\]
are separable of the same degree \( pm - 1 = n - 1 \geq 4 \).

The standard substitution
\[
x_1 = 1/(x - \alpha), y_1 = y/(x - \alpha)^m
\]
establishes a birational isomorphism between \( C_{f,p} \) and a superelliptic curve

\[
C_{b_1}: y_1^p = h_1(x_1)
\]

(see [19], p. 3359). But \( \deg(h_1) = pm - 1 \) is not divisible by \( p \). Clearly, this isomorphism commutes with the actions of \( \delta_p \). In particular, it induces an isomorphism of \( \mathbb{Z}[\delta_p] \)-modules \( J^{(f,p)}(K_a) \) and \( J^{(h_1,p)}(K_a) \) which commutes with the action of \( \text{Gal}(K_1) \).

(ii) Assume, in addition, that \( f(x) \) is irreducible in \( K[x] \) and \( \text{Gal}(f) \) acts \( s \)-transitively on \( \mathfrak{N}_f \) for some positive integer \( s \geq 2 \). Then the Galois group \( \text{Gal}(h_1) \) of \( h_1 \) over \( K_1 \) acts \( s - 1 \)-transitively on the set \( \mathfrak{N}_{h_1} \) of roots of \( h_1 \). In particular, \( h_1(x) \) is irreducible in \( K_1[x] \).

It is also clear that if \( \text{Gal}(f) = S_n \) or \( A_n \) then \( \text{Gal}(h_1) = S_{n-1} \) or \( A_{n-1} \) respectively.

Let us put \( \eta = 1 - \delta_p \). Clearly, \( \eta \) divides \( p \) in \( \mathbb{Z}[\delta_p] \cong \mathbb{Z}[\delta_p], \) i.e., there exists \( \eta' \in \mathbb{Z}[\delta_p] \) such that

\[
\eta' \eta = \eta' = \eta = p \in \mathbb{Z}[\delta_p].
\]

By a theorem of Ribet [10] the \( \mathbb{Z}_p \)-Tate module \( T_p(J^{(f,p)}) \) is a free \( \mathbb{Z}_p[\delta_p] \)-module of rank \( 2g/(p - 1) = n - 1 \) if \( p \) does not divide \( n \) and \( n - 2 \) if \( p \) does. Let \( J^{(f,p)}(\eta) \) be the kernel of \( \eta \) in \( J^{(f,p)}(K_a) \). Clearly, \( J^{(f,p)}(\eta) \) is killed by multiplication by \( p \), i.e., it may be viewed as a \( \mathbb{F}_p \)-vector space. It follows from Ribet’s theorem that

\[
\dim_{\mathbb{F}_p} J^{(f,p)}(\eta) = \frac{2g}{p - 1}.
\]

In addition, \( J^{(f,p)}(\eta) \) carries a natural structure of Galois module. Notice that

\[
\eta'(J^{(f,p)}) \subset J^{(f,p)}(\eta)
\]

where \( J^{(f,p)}_\eta \) is the kernel of multiplication by \( p \) in \( J^{(f,p)}(K_a) \).

Let \( \Lambda \) be the centralizer of \( \delta_p \) in \( \text{End}(J^{(f,p)}) \). Clearly, \( \Lambda \) commutes with \( \eta \) and \( \eta' \). It is also clear that the subgroup \( J^{(f,p)}(\eta) \) is \( \Lambda \)-stable. This observation leads to a natural homomorphism

\[
\kappa : \Lambda \to \text{End}_{\mathbb{F}_p}(J^{(f,p)}(\eta)).
\]

I claim that its kernel coincides with \( \eta \Lambda \). Indeed, assume that \( u(J^{(f,p)}(\eta)) = \{0\} \) for some \( u \in \Lambda \). This implies that \( u \eta' = \eta' u \) kills \( J^{(f,p)}_\eta \). This implies, in turn, that there exists \( v \in \text{End}(J^{(f,p)}) \) such that

\[
\eta' = \eta' = \eta \eta
\]

Clearly, \( v \) commutes with \( \eta \) and therefore with \( \delta_p = 1 - \eta \), i.e., \( v \in \Lambda \). Since

\[
p = \eta \eta' = \eta \eta,
\]

and therefore \( u = v \eta \). On the other hand, it is clear that \( \eta \Lambda = \Lambda \eta \) kills \( J^{(f,p)}(\eta) \). Therefore the natural map

\[
\Lambda/\eta \Lambda \to \text{End}_{\mathbb{F}_p}(J^{(f,p)}(\eta))
\]

is an embedding; further we will identify \( \Lambda/\eta \Lambda \) with its image in \( \text{End}_{\mathbb{F}_p}(J^{(f,p)}(\eta)) \).

**Theorem 3.3** (Prop. 6.2 in [13], Prop. 3.2 in [14]). There is a canonical isomorphism of the \( \text{Gal}(K) \)-modules

\[
J^{(f,p)}(\eta) \cong V_{f,p}.
\]
Remark 3.4. Clearly, the natural homomorphism $\text{Gal}(K) \to \text{Aut}_{\mathbb{F}_p}(V_{f,p})$ coincides with the composition

$$\text{Gal}(K) \to \text{Gal}(f) \subset \text{Perm}(\mathfrak{R}_f) \subset \text{Aut}((\mathbb{F}_p^{|s|})^0) = \text{Aut}_{\mathbb{F}_p}(V_{f,p}).$$

The following assertion is an immediate corollary of Lemma 2.4.

Lemma 3.5. Assume that $\text{Gal}(f) = S_n$ or $A_n$. If $n \geq 5$ then the $\text{Gal}(f)$-module $V_{f,p}$ is absolutely simple.

Theorem 3.6. Assume that $p > 2$ and $n \geq 4$. Let $\Lambda = \Lambda \otimes \mathbb{Q}$ be the centralizer of $\mathbb{Q}(\delta_p)$ in $\text{End}^0(J^{(f,p)})$. Then $\Lambda$ could not be a central simple $\mathbb{Q}(\delta_p)$-algebra of dimension $(2g/(p-1))^2$ where $g$ is genus of $C_{f,p}$.

Proof. Assume that $\Lambda$ is a central simple $\mathbb{Q}(\delta_p)$-algebra of dimension $(2g/(p-1))^2$. We need to arrive to a contradiction. We start with the following statement.

Lemma 3.7. Assume that $\Lambda$ is a central simple $\mathbb{Q}(\delta_p)$-algebra of dimension $(2g/(p-1))^2$. Then there exist a $(p-1)/2$-dimensional abelian variety $Z$ over $K_a$, a positive integer $r$, an embedding

$$\mathbb{Q}(\delta_p) \cong \mathbb{Q}(\delta) \hookrightarrow \text{End}^0(Z)$$

and an isogeny $\phi : Z^r \to J^{(f,p)}$ such that the induced isomorphism

$$\text{Mat}_r(\text{End}^0(Z)) = \text{End}^0(Z^r) \cong \text{End}^0(J^{(f,p)}),$$

maps identically

$$\mathbb{Q}(\delta_p) \subset \text{End}^0(Z) \subset \text{Mat}_r(\text{End}^0(Z)) = \text{End}^0(Z^r)$$

onto

$$\mathbb{Q}(\delta_p) \subset \text{End}^0(J^{(f,p)}).$$

(Here $\text{End}^0(Z) \subset \text{Mat}_r(\text{End}^0(Z))$ is the diagonal embedding.) In particular, $Z$ and $J^{(f,p)}$ are abelian varieties of CM-type over $K_a$.

Proof of Lemma 3.4. Clearly, there exist a positive integer $r$ and a central division algebra $H$ over $\mathbb{Q}(\delta_p) \cong \mathbb{Q}(\zeta_p)$ such that $\Lambda \cong \text{Mat}_r(H)$. This implies that there exist an abelian variety $Z$ over $K_a$ with

$$\mathbb{Q}(\delta_p) \subset H \subset \text{End}^0(Z)$$

and an isogeny $\phi : Z^r \to J^{(f,p)}$ such that the induced isomorphism $\text{End}^0(Z^r) \cong \text{End}^0(J^{(f,p)})$ maps identically

$$\mathbb{Q}(\delta_p) \subset \text{End}^0(Z) \subset \text{End}^0(Z^r)$$

onto $\mathbb{Q}(\delta_p) \subset \text{End}^0(J^{(f,p)})$. We still have to check that

$$2\dim(Z) = p - 1.$$

In order to do that let us put $g' = g/r$. Then $\dim_{\mathbb{Q}(\delta_p)}(H) = (\frac{2g'}{p-1})^2$ and therefore $\dim_{\mathbb{Q}}(H) = \frac{(2g')^2}{p-1}$. Since $H$ is a division algebra and $\text{char}(K_a) = 0$, the number $\frac{(2g')^2}{p-1}$ must divide $2\dim(Z) = 2g'$. This means that $2g'$ divides $p - 1$. On the other hand,

$$\mathbb{Q}(\delta_p) \subset H \subset \text{End}^0(Z).$$

This implies that $p - 1 = [\mathbb{Q}(\delta_p) : \mathbb{Q}]$ divides $2\dim(Z)$ and therefore $2\dim(Z) = p - 1$. \qed
Now let us return to the proof of Theorem \ref{thm:3.6}. Recall that \( n \geq 4 \). We write \( \Omega^1(X) \) for the space of differentials of first kind for any smooth projective variety \( X \) over \( K_a \). Clearly, \( \phi \) induces an isomorphism \( \phi^*: \Omega^1(J^{(f,p)}) \cong \Omega^1(Z)^r = \Omega^1(Z)^r \) which commutes with the natural actions of \( Q(\delta_p) \). Since \( \dim(Z) = \frac{p-1}{2} \), we have \( \dim_k(\Omega^1(Z)) = \frac{p-1}{2} \). Therefore, the induced \( K_a \)-linear automorphism

\[
\delta^*_p: \Omega^1(Z) \to \Omega^1(Z)
\]

has, at most, \( \frac{p-1}{2} \) distinct eigenvalues. Clearly, the same is true for the action of \( \delta_p \) in \( \Omega^1(Z)^r \). Since \( \phi \) commutes with \( \delta_p \), the induced \( K_a \)-linear automorphism

\[
\delta^*_p: \Omega^1(J^{(f,p)}) \to \Omega^1(J^{(f,p)})
\]

has, at most, \( \frac{p-1}{2} \) distinct eigenvalues.

On the other hand, let \( P_0 \) be one of the \( \delta_p \)-invariant points (i.e., a ramification point for \( \pi \)) of \( C_{f,p}(K_a) \). Then

\[
\tau: C_{f,p} \to J^{(f,p)}, \quad P \mapsto \text{cl}((P) - (P_0))
\]

is an embedding of \( K_a \)-algebraic varieties and it is well-known that the induced map

\[
\tau^*: \Omega^1(J^{(f,p)}) \to \Omega^1(C_{f,p})
\]

is a \( K_a \)-linear isomorphism obviously commuting with the actions of \( \delta_p \). (Here \( cl \) stands for the linear equivalence class.) This implies that \( \delta_p \) has, at most, \( \frac{p-1}{2} \) distinct eigenvalues in \( \Omega^1(C_{f,p}) \).

One may easily check that \( \Omega^1(C_{f,p}) \) contains differentials \( dx/y^i \) for all positive integers \( i < p \) satisfying \( ni \geq (p + 1) \) if \( p \) does not divide \( n \) (\cite{1}, Th. 3 on p. 403; see also \cite{2}, Prop. 2 on p. 3359). Since \( n \geq 4 \) and \( p \geq 3 \), we have \( ni \geq (p + 1) \) for all \( i \) with \( \frac{p-1}{2} \leq i < p \). Therefore the differentials \( dx/y^i \in \Omega^1(C_{f,p}) \) for all \( i \) with \( \frac{p-1}{2} \leq i < p - 1 \); clearly, they all are eigenvectors of \( \delta_p \) with eigenvalues \( \zeta^{-i} \) respectively. (Recall that \( \zeta \in K_a \) is a primitive \( p \)th root of unity and \( \delta_p \) is defined in \( \S 1 \) by \( (x, y) \mapsto (x, \zeta y) \).) Therefore \( \delta_p \) has in \( \Omega^1(C_{f,p}) \), at least, \( \frac{p-1}{2} \) distinct eigenvalues. Contradiction.

Now assume that \( p \) divides \( n \). Then \( n \geq 5 \). By Remark \ref{rem:3.2}, \( C_{f,p} \) is birationally isomorphic over \( K_a \) to a curve \( C_1 = C_{h_1,p} : y_1^2 = h_1(x_1) \) where \( h_1(x_1) \in K_a[x_1] \) is a separable polynomial of degree \( n - 1 \); in addition, one may choose this isomorphism in such a way that it commutes with the actions of \( \delta_p \) on \( C_{f,p} \) and \( C_{h_1,p} \). This implies that \( \delta_p \) has, at most, \( \frac{p-1}{2} \) distinct eigenvalues in \( \Omega^1(C_{h_1,p}) \).

On the other hand, \( n - 1 \geq 4 \) and \( n - 1 \) is not divisible by \( p \). Recall that \( \deg(h_1) = n - 1 \). We conclude, as above, that for all \( i \) with \( \frac{p-1}{2} \leq i < p - 1 \) the differentials \( dx_1/y_1^i \in \Omega^1(C_{h_1,p}) \). Now, the same arguments as in the case of \( p \) not dividing \( n \) lead to a contradiction. \( \square \)

**Theorem 3.8.** Suppose \( n \geq 4 \) and \( p > 2 \). Assume that \( Q(\delta_p) \) is a maximal commuting subalgebra in \( \text{End}^0(J^{(f,p)}) \). Then:

(i) The center \( \mathcal{C} \) of \( \text{End}^0(J^{(f,p)}) \) is a CM-subfield of \( Q(\delta_p) \);

(ii) If \( p \) is a Fermat prime then \( \text{End}^0(J^{(f,p)}) = Q(\delta_p) \cong Q(\zeta_p) \) and therefore \( \text{End}(J^{(f,p)}) = \mathbb{Z}[\delta_p] \cong \mathbb{Z}[\zeta_p] \).
Proof. Clearly, $C \subset \mathbb{Q}(\delta_p)$. Since $\mathbb{Q}(\delta_p)$ is a CM-field, $C$ is either a totally real field or a CM-field. If $p$ is a Fermat prime then each subfield of $\mathbb{Q}(\delta_p)$ (distinct from $\mathbb{Q}(\delta_p)$ itself) is totally real. Therefore, (ii) follows from (i).

In order to prove (i), let us assume that $C$ is totally real. We are going to arrive to a contradiction which proves (i). Replacing, if necessary, $K$ by its subfield finitely generated over the rationals, we may assume that $K$ (and therefore $K_a$) is isomorphic to a subfield of the field $\mathbb{C}$ of complex numbers. Since the center $\mathcal{E}$ of $\text{End}^0(J_{f,p})$ is totally real, the Hodge group of $J_{f,p}$ must be semisimple. This implies that the pair $(J_{f,p}, \mathbb{Q}(\delta_p))$ is of Weil type $(\mathbb{S})$, i.e., $\mathbb{Q}(\delta_p)$ acts on $\Omega^1(J_{f,p})$ in such a way that for each embedding $\sigma : \mathbb{Q}(\delta_p) \hookrightarrow \mathbb{C}$ the corresponding multiplicity

$$n_\sigma = \dim(J_{f,p})$$

Now assume that $p$ does not divide $n$. We have

$$\frac{\dim(J_{f,p})}{[\mathbb{Q}(\delta_p) : \mathbb{Q}]} = \frac{g(C_{f,p})}{p-1} = \frac{(n-1)}{2}$$

and therefore

$$n_\sigma = \frac{(n-1)}{2}$$

Since the multiplicity $n_\sigma$ is always an integer, $n$ is odd. Therefore $n \geq 5$. Let us consider the embedding $\sigma$ which sends $\delta_p$ to $\zeta$. Elementary calculations ([6], Th. 3 on p. 403) show that for all integers $i$ with

$$0 \leq i \leq n - 1 - \frac{(n+1)}{p}$$

the differentials $x^i dx / y^{p-1} \in \Omega^1(C_{f,p})$; clearly, they constitute a set of $K_a$-linearly independent eigenvectors of $\delta_p$ with eigenvalue $\zeta$. In light of the $\delta_p$-equivariant isomorphism

$$\Omega^1(J_{f,p}) \rightarrow \Omega^1(C_{f,p}),$$

we conclude that

$$\frac{(n-1)}{2} = n_\sigma \geq [n - 1 - \frac{(n+1)}{p}] + 1.$$  

This implies that $\frac{(n-1)}{2} > n - 1 - \frac{(n+1)}{p}$. It follows easily that $n < \frac{p+2}{p-2} \leq 5$ and therefore $n < 5$. This gives us the desired contradiction when $p$ does not divide $n$.

Now assume that $p$ divides $n$. Then $n \geq 5$ and $n - 1 \geq 4$. Again, as in the proof of Theorem 3.6, the usage of Remark 3.2 allows us to apply the already proven case (when $p$ does not divide $n - 1$) to $C_{h_1,p}$ with $\deg(h_1) = n - 1$.

**Remark 3.9.** Let us keep the notations and assumptions of Theorem 3.8. Assume, in addition that $p = 3$. Then $\mathbb{Q}(\delta_3) = \mathbb{Q}(\zeta_3)$ is an imaginary quadratic field and there are exactly two embeddings $\mathbb{Q}(\delta_3) \hookrightarrow K_a$ which, of course, are complex-conjugate. In this case one could compute explicitly the corresponding multiplicities.
Indeed, first assume that 3 does not divide \( n \). Then \( n = 3k - e \) for some \( k, e \in \mathbb{Z} \) with \( 3 > e > 0 \). Since \( n \geq 4 > 3 \), we have \( k \geq 2 \). By Prop. 2 on p. 3359 of \([18]\), the set
\[
\{x^i dx/y, 0 \leq i < k - 1; x^j dx/y^2, 0 \leq j < 2k - 1 - \left\lfloor \frac{2e}{3} \right\rfloor \}
\]
is a basis of \( \Omega^1(C_{f,3}) \). It follows easily that it is an eigenbasis with respect to the action of \( \delta_3 \). This implies easily that \( Q(\delta_3) \) acts on \( \Omega^1(J^{(f,3)}) = \Omega^1(C_{f,3}) \) with multiplicities \( k - 1 \) and \( 2k - 1 - \left\lfloor \frac{2e}{3} \right\rfloor \).

Assume now that \( n = 3k \) is divisible by 3. Then as in the proof of Theorem 3.6, the usage of Remark 3.2 allows us to reduce the calculation of multiplicities to the case of \( C_{h_1,3} \) with \( \deg(h_1) = n - 1 \). More precisely, we have \( n = 3k \) and \( n - 1 = 3k - 1 \), i.e., \( e = 1 \) and \( k \geq 2 \). This implies that \( Q(\delta_3) \) acts on \( \Omega^1(J^{(f,3)}) = \Omega^1(J^{(h_1,3)}) \) with multiplicities \( k - 1 \) and \( 2k - 1 \).

It follows that if \( n = 3k \) or \( n = 3k - 1 \) then
\[
\dim(J^{(f,3)}) = 3k - 2
\]
and the imaginary quadratic field \( \mathbb{Q}(f_3) \) acts on \( \Omega^1(J^{(f,3)}) \) with mutually prime multiplicities \( k - 1 \) and \( 2k - 1 \). Since \( Q(f_3) \) coincides with \( \text{End}^0(J^{(f,3)}) \), a theorem of Ribet ([19], Th. 3 on p. 526) implies that the Hodge group of \( J^{(f,3)} \) is as large as possible. More precisely, let \( K' \subset K \) be a subfield which admits an embedding into \( \mathbb{C} \) and such that \( f(x) \subset K'[x] \) (such a subfield always exists). Then one may consider \( C_{f,3} \) as a complex smooth projective curve and \( J^{(f,3)} \) as a complex abelian variety, whose endomorphism algebra coincides with \( \mathbb{Q}(\delta_3) \equiv \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3}) \). Then the Hodge group of \( J^{(f,3)} \) coincides with the corresponding unitary group of \( H_1(J^{(f,3)}(\mathbb{C}), \mathbb{Q}) \) over \( \mathbb{Q}(\zeta_3) \). In particular, all Hodge classes on all self-products of \( J^{(f,3)} \) could be presented as linear combinations of exterior products of divisor classes. As was pointed out in [19], pp. 572–573, the same arguments work also for Tate classes if say, \( K' \) is a number field and all endomorphisms of \( J^{(f,3)} \) are defined over \( K' \). (If \( \sqrt{-3} \in K' \) then all endomorphisms of \( J^{(f,3)} \) are defined over \( K' \) because \( \text{End}(J^{(f,3)}) = \mathbb{Z}[\delta_3] \) and \( \delta_3 \) is defined over \( K' \).

4. Representation theory

**Definition 4.1.** Let \( V \) be a vector space over a field \( F \), let \( G \) be a group and \( \rho : G \to \text{Aut}_F(V) \) a linear representation of \( G \) in \( V \). We say that the \( G \)-module \( V \) is very simple if it enjoys the following property:

If \( R \subset \text{End}_F(V) \) be an \( F \)-subalgebra containing the identity operator \( \text{Id} \) such that
\[
\rho(\sigma) R \rho(\sigma)^{-1} \subset R \quad \forall \sigma \in G
\]
then either \( R = F \cdot \text{Id} \) or \( R = \text{End}_F(V) \).

**Remark 4.2.**

(i) Clearly, the \( G \)-module \( V \) is very simple if and only if the corresponding \( \rho(G) \)-module \( V \) is very simple. It is known ([21], Rem. 2.2(ii)) that a very simple module is absolutely simple.

(ii) If \( G' \) is a subgroup of \( G \) and the \( G' \)-module \( V \) is very simple then the \( G' \)-module \( V \) is also very simple.

**Theorem 4.3.** Suppose a field \( F \), a positive integer \( N \) and a group \( H \) enjoy the following properties:
• $F$ is either finite or algebraically closed;
• $H$ is perfect, i.e., $H = [H, H]$;
• Each homomorphism from $H$ to $S_N$ is trivial;
• Let $N = ab$ be a factorization of $N$ into a product of two positive integers $a$ and $b$. Then either each homomorphism from $H$ to $\text{PGL}_a(F)$ is trivial or each homomorphism from $H$ to $\text{PGL}_b(F)$ is trivial.

Then each absolutely simple $H$-module of $F$-dimension $N$ is very simple. In other words, in dimension $N$ the properties of absolute simplicity and supersimplicity over $F$ are equivalent.

Proof. We may assume that $N > 1$. Let $V$ be an absolutely simple $H$-module of $F$-dimension $N$. Let $R \subset \text{End}_F(V)$ be an $F$-subalgebra containing the identity operator $\text{Id}$ and such that

$$uRu^{-1} \subset R \quad \forall u \in H.$$ 

Clearly, $V$ is a faithful $R$-module and

$$uRu^{-1} = R \quad \forall u \in H.$$ 

**Step 1.** By Lemma 7.4(i) of [21], $V$ is a semisimple $R$-module.

**Step 2.** The $R$-module $V$ is isotypic. Indeed, let us split the semisimple $R$-module $V$ into the direct sum

$$V = V_1 \oplus \cdots \oplus V_r$$

of its isotypic components. Dimension arguments imply that $r \leq \dim(V) = N$. It follows easily from the arguments of the previous step that for each isotypic component $V_i$ its image $sV_i$ is an isotypic $R$-submodule for each $s \in H$ and therefore is contained in some $V_j$. Similarly, $s^{-1}V_j$ is an isotypic submodule obviously containing $V_i$. Since $V_i$ is the isotypic component, $s^{-1}V_j = V_i$ and therefore $sV_i = V_j$. This means that $s$ permutes the $V_i$; since $V$ is $H$-simple, $H$ permutes them transitively. This gives rise to the homomorphism $H \rightarrow S_r$, which must be trivial, since $r \leq N$ and therefore $S_r$ is a subgroup of $S_N$. This means that $sV_i = V_i$ for all $s \in H$ and $V = V_i$ is isotypic.

**Step 3.** Since $V$ is isotypic, there exist a simple $R$-module $W$ and a positive integer $d$ such that $V \cong W^d$. We have

$$d \cdot \dim(W) = \dim(V) = N.$$ 

Clearly, $\text{End}_R(V)$ is isomorphic to the matrix algebra $\text{Mat}_d(\text{End}_R(W))$ of size $d$ over $\text{End}_R(W)$.

Let us put

$$k = \text{End}_R(W).$$

Since $W$ is simple, $k$ is a finite-dimensional division algebra over $F$. Since $F$ is either finite or algebraically closed, $k$ must be a field. In addition, $k = F$ if $F$ is algebraically closed and $k$ is finite if $F$ is finite. We have

$$\text{End}_R(V) \cong \text{Mat}_d(k).$$

Clearly, $\text{End}_R(V) \subset \text{End}_F(V)$ is stable under the adjoint action of $H$. This induces a homomorphism

$$\alpha : H \rightarrow \text{Aut}_F(\text{End}_R(V)) = \text{Aut}_F(\text{Mat}_d(k)).$$
Since $k$ is the center of $\text{Mat}_d(k)$, it is stable under the action of $H$, i.e., we get a homomorphism $H \to \text{Aut}(k/F)$, which must be trivial, since $H$ is perfect and $\text{Aut}(k/F)$ is abelian. This implies that the center $k$ of $\text{End}_H(V)$ commutes with $H$. Since $\text{End}_H(V) = F$, we have $k = F$. This implies that $\text{End}_H(V) \cong \text{Mat}_d(F)$ and

$$\alpha : H \to \text{Aut}_F(\text{Mat}_d(F)) = \text{GL}(d, F)/F^* = \text{PGL}_d(F)$$

is trivial if and only if $\text{End}_H(V) \subset \text{End}_H(V) = F \cdot \text{Id}$. Since $\text{End}_H(V) \cong \text{Mat}_d(F)$, $\alpha$ is trivial if and only if $d = 1$, i.e. $V$ is an absolutely simple $R$-module.

It follows from the Jacobson density theorem that $R \cong \text{Mat}_m(F)$ with $dm = N$. This implies that $\alpha$ is trivial if and only if $R \cong \text{Mat}_N(F)$, i.e., $R = \text{End}_F(V)$.

The adjoint action of $H$ on $R$ gives rise to a homomorphism

$$\beta : H \to \text{Aut}_F(\text{Mat}_m(F)) = \text{PGL}_m(F).$$

Clearly, $\beta$ is trivial if and only if $R$ commutes with $H$, i.e. $R = F \cdot \text{Id}$.

It follows that we are done if either $\alpha$ or $\beta$ is trivial. Now one has only to recall that $N = dm$. \hfill \Box

### Corollary 4.4

Let $p$ be a prime, $V$ a vector space over $F_p$ of finite dimension $N$. Let $H \subset \text{Aut}(V)$ be a non-abelian simple group. Suppose that the $H$-module $V$ is absolutely simple and $H$ is not isomorphic to a subgroup of $S_N$. Then the $H$-module $V$ is very simple if one of the following conditions holds:

1. $N$ is a prime;
2. $N = 8$ or twice a prime. In addition, $H$ is not isomorphic to $\text{PSL}_2(F_p)$ and either $H$ is not isomorphic to $A_5$ or $p$ is not congruent to $\pm 1$ modulo $5$;
3. $\#(H) \geq ((p^{\left\lfloor \sqrt{N} \right\rfloor} - 1)^{\left\lfloor \sqrt{N} \right\rfloor})/(p - 1)$
4. $\#(H) \geq (p^N - 1)/(p - 1)$.

**Proof.** Let us split $N$ into a product $N = ab$ of two positive integers $a$ and $b$. In the case (i) either $a$ or $b$ is $1$ and the target of the corresponding projective linear group $\text{PGL}_1(F_p) = \{1\}$. In the case (ii) either one of the factors is $1$ and we are done or one of the factors is $2$ and it suffices to check that each homomorphism from $H$ to $\text{PGL}_2(F_p)$ is trivial. Since $H$ is simple, each non-trivial homomorphism $\gamma : H \to \text{PGL}_2(F_p)$ is an injection, whose image lies in $\text{PSL}_2(F_p)$. In other words, $\gamma(H)$ is a subgroup of $\text{PSL}_2(F_p)$ isomorphic to $H$. Since $H$ is not isomorphic to $\text{PSL}_2(F_p)$, the subgroup $\gamma(H)$ is proper and simple non-abelian. It is known ([7], Th. 6.25 on p. 412 and Th. 6.26 on p. 414) that each proper simple non-abelian subgroup of $\text{PSL}_2(F_p)$ is isomorphic to $A_5$ and such a subgroup exists if and only if $p$ is congruent to $\pm 1$ modulo $5$. This implies that such $\gamma$ does not exist and settles the case (ii). In order to do the case (iii) notice that one of the factors say, $a$ does not exceed $\left\lfloor \sqrt{N} \right\rfloor$. This implies easily that the order of $\text{GL}_a(F_p)$ does not exceed $((p^{\left\lfloor \sqrt{N} \right\rfloor} - 1)^{\left\lfloor \sqrt{N} \right\rfloor})$ and therefore the order of $\text{PGL}_a(F_p)$ does not exceed $((p^{\left\lfloor \sqrt{N} \right\rfloor} - 1)^{\left\lfloor \sqrt{N} \right\rfloor})/(p - 1)$. Hence, the order of $H$ is strictly greater than the order of $\text{PGL}_a(F_p)$ and therefore there are no injective homomorphisms from $H$ to $\text{PGL}_a(F_p)$. Since $H$ is simple, each homomorphism from $H$ is either trivial or injective. This settles the case (iii). The case (iv) follows readily from the case (iii). \hfill \Box
Corollary 4.5. Suppose \( n \geq 5 \) is an integer, \( B \) is an \( n \)-element set. Suppose \( p = 3 \). Then the Alt(\( B \))-module \((\mathbb{F}_3^B)^{00}\) is very simple.

Proof. By Lemma 2.3, \((\mathbb{F}_3^B)^{00}\) is absolutely simple and \( N = \dim_{\mathbb{F}_3}((\mathbb{F}_3^B)^{00}) \) is either \( n - 1 \) or \( n - 2 \). The group Alt(\( B \)) is a simple non-abelian group, whose order \( n!/2 \) is greater than the order of \( S_{n-1} \) and the order of \( S_{n-2} \). Therefore each homomorphism from Alt(\( B \)) to \( S_N \) is trivial. On the other hand, one may easily check that
\[
n!/2 > 3^{n-1}/2 > (3^N - 1)/(3 - 1)
\]
for all \( n \geq 5 \). Now one has only to apply Corollary 4.4(iv) to \( H = \text{Alt}(B) \) and \( p = 3 \). \( \Box \)

Corollary 4.6. Suppose \( p > 3 \) is a prime, \( n \geq 8 \) is a positive integer, \( B \) is an \( n \)-element set. Then the Alt(\( B \))-module \((\mathbb{F}_p^B)^{00}\) is very simple.

Proof. Recall that \( N = \dim_{\mathbb{F}_p}((\mathbb{F}_p^B)^{00}) \) is either \( n - 1 \) or \( n - 2 \). In both cases
\[
[\sqrt{N}] - 1 < [n/3].
\]
Clearly, Alt(\( B \)) \( \cong \mathbb{A}_n \) is perfect and every homomorphism from Alt(\( B \)) to \( S_N \) is trivial.

We are going to deduce the Corollary from Theorem 4.3 applied to \( F = \mathbb{F}_p \) and \( H = \text{Alt}(B) \). In order to do that let us consider a factorization \( N = ab \) of \( N \) into a product of two positive integers \( a \) and \( b \). We may assume that \( a > 1, b > 1 \) and say, \( a \leq b \). Then
\[
a - 1 \leq [\sqrt{N}] - 1 < [n/3].
\]
Let
\[
\alpha : \mathbb{A}_n \cong \text{Alt}(B) \to \text{PGL}_n(\mathbb{F}_p)
\]
be a group homomorphism. We need to prove that \( \alpha \) is trivial. Let \( \mathbb{F}_p \) be an algebraic closure of \( \mathbb{F}_p \). Since PGL\(_n(\mathbb{F}_p) \subset \text{PGL}_n(\mathbb{F}_p) \), it suffices to check that the composition
\[
\mathbb{A}_n \cong \text{Alt}(B) \to \text{PGL}_n(\mathbb{F}_p) \subset \text{PGL}_n(\mathbb{F}_p)
\]
which we continue denote by \( \alpha \), is trivial.

Let
\[
\pi : \mathbb{A}_n \to \mathbb{A}_n
\]
be the universal central extension of the perfect group \( \mathbb{A}_n \). It is well-known that \( \mathbb{A}_n \) is perfect and the kernel (Schur’s multiplier) of \( \pi \) is a cyclic group of order 2, since \( n \geq 8 \). One could lift \( \alpha \) to the homomorphism
\[
\alpha' : \mathbb{A}_n \to \text{GL}_n(\mathbb{F}_p).
\]
Clearly, \( \alpha \) is trivial if and only if \( \alpha' \) is trivial. In order to prove the triviality of \( \alpha' \), let us put \( m = [n/3] \) and notice that \( \mathbb{A}_n \) contains a subgroup \( D \) isomorphic to \((\mathbb{Z}/3\mathbb{Z})^m\) (generated by disjoint 3-cycles). Let \( D' \) be a Sylow 3-subgroup in \( \pi^{-1}(D) \). Clearly, \( \pi \) maps \( D' \) isomorphically onto \( D \). Therefore, \( D' \) is a subgroup of \( \mathbb{A}_n \) isomorphic to \((\mathbb{Z}/3\mathbb{Z})^m\).

Now, let us discuss the image and the kernel of \( \alpha' \). First, since \( \mathbb{A}_n \) is perfect, its image lies in SL\(_n(\mathbb{F}_p)\), i.e., one may view \( \alpha' \) as a homomorphism from \( \mathbb{A}_n \) to SL\(_n(\mathbb{F}_p)\). Second, the only proper normal subgroup in \( \mathbb{A}_n \) is the kernel of \( \pi \). This implies that if \( \alpha' \) is nontrivial then its kernel meets \( D' \) only at the identity element and therefore \( \text{SL}_n(\mathbb{F}_p) \) contains the subgroup \( \alpha'(D') \) isomorphic to \((\mathbb{Z}/3\mathbb{Z})^m\). Since
$p \neq 3$, the group $\alpha'(D')$ is conjugate to an elementary 3-group of diagonal matrices in $\text{SL}_n(F_p)$. This implies that

$$m \leq a - 1.$$ 

Since $m = [n/3]$, we get a contradiction which implies that our assumption of the nontriviality of $\alpha'$ was wrong. Hence $\alpha'$ is trivial and therefore $\alpha$ is also trivial.

\[ \square \]

**Theorem 4.7.** Suppose $n \geq 5$ is a positive integer, $B$ is an $n$-element set, $p$ is a prime. Then the $\text{Alt}(B)$-module $(F_p^B)^{00}$ is very simple.

**Proof.** The case of $p = 2$ was proven in [2], Ex. 7.2. The case of $p = 3$ was done in Corollary 4.4. So, we may assume that $p \geq 5$. In light of Corollary 4.6 we may assume that $n < 8$, i.e., $5 \leq n \leq 7$.

Assume that $n \neq p$. Then $p$ does not divide $n$ and $n - 1$ is either a prime or twice a prime. Therefore

$$N = \dim_{F_p}(F_p^B)^{00} = n - 1$$

is either a prime or twice a prime. Now the very simplicity of $(F_p^B)^{00}$ follows from the cases (i) and (ii) of Corollary 4.4.

Assume now that $n = p$. Then either $n = p = 5$ or $n = p = 7$. In both cases

$$N = \dim_{F_p}(F_p^B)^{00} = n - 2$$

is a prime. Now the very simplicity of $(F_p^B)^{00}$ follows from Corollary 4.4(i). \[ \square \]

5. **Jacobians and Endomorphisms**

Recall that $K$ is a field of characteristic zero, $f(x) \in K[x]$ is a polynomial of degree $n \geq 5$ without multiple roots, $\mathfrak{R}_f \subset K_a$ the set of its roots, $K(\mathfrak{R}_f)$ its splitting field,

$$\text{Gal}(f) = \text{Gal}(K(\mathfrak{R}_f)/K) \subset \text{Perm}(\mathfrak{R}_f).$$

**Remark 5.1.** Assume that $\text{Gal}(f) = \text{Perm}(\mathfrak{R}_f)$ or $\text{Alt}(\mathfrak{R}_f)$. Taking into account that $\text{Alt}(\mathfrak{R}_f)$ is non-abelian simple, $\text{Perm}(\mathfrak{R}_f)/\text{Alt}(\mathfrak{R}_f) \cong \mathbb{Z}/2\mathbb{Z}$ and $K(\zeta)/K$ is abelian, we conclude that the Galois group of $f$ over $K(\zeta)$ is also either $\text{Perm}(\mathfrak{R}_f)$ or $\text{Alt}(\mathfrak{R}_f)$. In particular, $f$ remains irreducible over $K(\zeta)$. So, in the course of the proof of main results from Introduction we may assume that $\zeta \in K$.

**Theorem 5.2.** Let $p$ be an odd prime and $\zeta \in K$. If the $\text{Gal}(f)$-module $(F_p^\mathfrak{R}_f)^{00}$ is very simple then $\mathbb{Q}(\delta_p)$ coincides with its own centralizer in $\text{End}^0(J^{(f,p)})$ and the center of $\text{End}^0(J^{(f,p)})$ is a CM-subfield of $\mathbb{Q}(\delta_p)$. In particular, if $p$ is a Fermat prime then $\text{End}^0(J^{(f,p)}) = \mathbb{Q}(\delta_p)$ and $\text{End}(J^{(f,p)}) = \mathbb{Z}[[\delta_p]].$

Combining Theorems 5.2, Remark 5.1, Theorem 4.7 and Remark 4.2(ii), we obtain the following statement.

**Corollary 5.3.** Let $p$ be an odd prime. If $f(x) \in K[x]$ is an irreducible polynomial of degree $n \geq 5$ and $\text{Gal}(f) = S_n$ or $A_n$ then $\mathbb{Q}(\delta_p)$ is a maximal commutative subalgebra in $\text{End}^0(J^{(f,p)})$ and the center of $\text{End}^0(J^{(f,p)})$ is a CM-subfield of $\mathbb{Q}(\delta_p)$. In particular, if $p$ is a Fermat prime then $\text{End}^0(J^{(f,p)}) = \mathbb{Q}(\delta_p)$ and $\text{End}(J^{(f,p)}) = \mathbb{Z}[[\delta_p]].$
Proof of Theorem 5.2. Recall that \(J^{(f,p)}\) is a \(g\)-dimensional abelian variety defined over \(K\).

Since \(J^{(f,p)}\) is defined over \(K\), one may associate with every \(u \in \text{End}(J^{(f,p)})\) and \(\sigma \in \text{Gal}(K)\) an endomorphism \(\sigma u \in \text{End}(J^{(f,p)})\) such that
\[
\sigma u(x) = \sigma u(\sigma^{-1}x) \quad \forall x \in J^{(f,p)}(K_a).
\]

Let us consider the centralizer \(\Lambda\) of \(\delta_p\) in \(\text{End}(J^{(f,p)})\). Since \(\delta_p\) is defined over \(K\), we have \(\sigma u \in \Lambda\) for all \(u \in \Lambda\). Clearly, \(Z[\delta_p]\) sits in the center of \(\Lambda\) and the natural homomorphism
\[
\Lambda \otimes Z_p \rightarrow \text{End}_{Z_p[\delta_p]} T_p(J^{(f,p)})
\]
is an embedding. Here \(T_p(J^{(f,p)})\) is the \(Z_p\)-Tate module of \(J^{(f,p)}\) which is a free \(Z_p[\delta_p]\)-module of rank \(\frac{2g}{p-1}\). Notice that
\[
J^{(f,p)}(\eta) = T_p(J^{(f,p)})/\eta T_p(J^{(f,p)}).
\]

Recall also that (Theorem 3.3 and Remark 3.4)
\[
J^{(f,p)}(\eta) = (F^p)^{00}
\]
and \(\text{Gal}(K)\) acts on \((F^p)\) through
\[
\text{Gal}(K) \hookrightarrow \text{Gal}(f) \subset \text{Perm}(\mathfrak{R}_f) \subset \text{Aut}((F^p)^{00}).
\]

Since the \(\text{Gal}(f)\)-module \((F^p)^{00}\) is very simple, the \(\text{Gal}(K)\)-module \(J^{(f,p)}(\eta)\) is also very simple, thanks to Remark 3.4(i). On the other hand, if an endomorphism \(u \in \Lambda\) kills \(J^{(f,p)}(\eta) = \ker(1 - \delta_p)\) then one may easily check that there exists a unique \(v \in \text{End}(J^{(f,p)})\) such that \(u = v \cdot \eta\). In addition, \(v \in \Lambda\). This implies that the natural map
\[
\Lambda \otimes Z[\delta_p] Z[\delta_p]/(\eta) \rightarrow \text{End}_{F_p}(J^{(f,p)}(\eta))
\]
is an embedding. Let us denote by \(R\) the image of this embedding. We have
\[
R := \Lambda/\eta \Lambda = \Lambda \otimes Z_p/\eta \Lambda \otimes Z_p \subset \text{End}_{F_p}(J^{(f,p)}(\eta)).
\]

Clearly, \(R\) contains the identity endomorphism and is stable under the conjugation via Galois automorphisms. Since the \(\text{Gal}(K)\)-module \(J^{(f,p)}(\eta)\) is very simple, either \(R = F_p \cdot \text{Id}\) or \(R = \text{End}_{F_p}(J^{(f,p)}(\eta))\). If \(\Lambda/\eta \Lambda = R = F_p \cdot \text{Id}\) then \(\Lambda\) coincides with \(Z[\delta_p]\). This means that \(Z[\delta_p]\) coincides with its own centralizer in \(\text{End}(J^{(f,p)})\) and therefore \(Q(\delta_p)\) is a maximal commutative subalgebra in \(\text{End}^0(J^{(f,p)})\).

If \(\Lambda/\eta \Lambda = R = \text{End}_{F_p}(J^{(f,p)}(\eta))\) then, by Nakayama’s Lemma,
\[
\Lambda \otimes Z_p = \text{End}_{Z_p[\delta_p]} T_p(J^{(f,p)}) \cong \text{Mat}_{\frac{2g}{p-1}}(Z_p[\delta_p]).
\]
This implies easily that the \(Q(\delta_p)\)-algebra \(\Lambda_Q = \Lambda \otimes Q \subset \text{End}^0(X)\) has dimension \(\left(\frac{2g}{p-1}\right)^2\) and its center has dimension 1. This means that \(\Lambda_Q\) is a central \(Q(\delta_p)\)-algebra of dimension \(\left(\frac{2g}{p-1}\right)^2\). Clearly, \(\Lambda_Q\) coincides with the centralizer of \(Q(\delta_p)\) in \(\text{End}^0(J^{(f,p)})\). Since \(\delta_p\) respects the theta divisor on the jacobian \(J^{(f,p)}\), the algebra \(\Lambda_Q\) is stable under the corresponding Rosati involution and therefore is semisimple as a \(Q\)-algebra. Since its center is the field \(Q(\delta_p)\), the \(Q(\delta_p)\)-algebra \(\Lambda_Q\) is central simple and has dimension \(\left(\frac{2g}{p-1}\right)^2\). By Theorem 3.4, this cannot happen. Therefore \(Q(\delta_p)\) is a maximal commutative subalgebra in \(\text{End}^0(J^{(f,p)})\). \(\square\)
Proof of main results. Clearly, Theorem 1.1 follows readily from Corollary 5.3. Theorem 1.2 follows readily from Corollary 5.3 combined with Remark 3.9.

REFERENCES

[1] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, Atlas of finite groups. Clarendon Press, Oxford, 1985.
[2] Ch. W. Curtis, I. Reiner, Representation theory of finite groups and associative algebras. Interscience Publishers, New York London 1962.
[3] H. K. Farahat, On the natural representation of the symmetric group. Proc. Glasgow Math. Association 5 (1961-62), 121–136.
[4] I. M. Isaacs, Character theory of finite groups. Academic Press, New York San Francisco London, 1976.
[5] Ch. Jansen, K. Lux, R. Parker, R. Wilson, An Atlas of Brauer characters. Clarendon Press, Oxford, 1995.
[6] J. K. Koo, On holomorphic differentials of some algebraic function field of one variable over C. Bull. Austral. Math. Soc. 43 (1991), 399–405.
[7] B. Moonen, Yu. G. Zarhin, Hodge and Tate classes on simple abelian fourfolds. Duke Math. J. 77 (1995), 553–581.
[8] B. Moonen, Yu. G. Zarhin, Weil classes on abelian varieties. J. reine angew. Math. 496 (1998), 83–92.
[9] D. Mumford, Abelian varieties, Second edition. Oxford University Press, London, 1974.
[10] K. Ribet, Galois action on division points of Abelian varieties with real multiplications. Amer. J. Math. 98 (1976), 751–804.
[11] K. Ribet, Hodge classes on certain abelian varieties. Amer. J. Math. 105 (1983), 523–538.
[12] D. Passman, Permutation groups. W. A. Benjamin, Inc., New York-Amsterdam, 1968.
[13] B. Poonen, E. Schaefer, Explicit descent for Jacobians of cyclic covers of the projective line. J. reine angew. Math. 488 (1997), 141–188.
[14] E. Schaefer, Computing a Selmer group of a Jacobian using functions on the curve. Math. Ann. 310 (1998), 447–471.
[15] J.-P. Serre, Topics in Galois Theory. Jones and Bartlett Publishers, Boston-London, 1992. 163–176.
[16] J.-P. Serre, Linear representations of finite groups. Springer-Verlag, 1977.
[17] M. Suzuki, Group Theory I. Springer-Verlag, 1982.
[18] C. Towse, Weierstrass points on cyclic covers of the projective line. Trans. AMS 348 (1996), 3355-3377.
[19] A. Wagner, The faithful linear representations of least degree of \( S_n \) and \( A_n \) over a field of odd characteristic. Math. Z. 154 (1977), 103–114.
[20] Yu. G. Zarhin, Hyperelliptic jacobians without complex multiplication. Math. Res. Letters 6 (2000), 123–132.
[21] Yu. G. Zarhin, Hyperelliptic jacobians and modular representations, to appear in "Moduli of abelian varieties" (C. Faber, G. van der Geer, F. Oort, eds.), Birkhäuser.

E-mail address: zarhin@math.psu.edu