Max-Planck-Institut für Mathematik
Bonn

Superelliptic Jacobians and central simple representations

by

Yuri G. Zarhin

Max-Planck-Institut für Mathematik
Preprint Series 2024 (12)

Date of submission: May 19, 2024

Superelliptic Jacobians and central simple representations

by

Yuri G. Zarhin

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

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

MPIM 24-12

SUPERELLIPTIC JACOBIANS AND CENTRAL SIMPLE REPRESENTATIONS

YURI G. ZARHIN

Abstract. Let $f(x)$ be a polynomial of degree at least 5 with complex coefficients and without repeated roots. Suppose that all the coefficients of $f(x)$ lie in a subfield K of $\mathbb{C}$ such that:

- K contains a primitive p-th root of unity;
- $f(x)$ is irreducible over K;
- the Galois group $\mathrm{Gal}(f)$ of $f(x)$ acts doubly transitively on the set of roots of $f(x)$;
- the index of every maximal subgroup of $\mathrm{Gal}(f)$ does *not* divide $\deg(f) - 1$.

Then the endomorphism ring of the Jacobian of the superelliptic curve $y^p = f(x)$ is isomorphic to the pth cyclotomic ring for all primes $p > \deg(f)$.

1. Introduction

The aim of this paper is to explain how to compute the endomorphism algebra of Jacobians of smooth projective models of superelliptic curves $y^q = f(x)$ where $q = p^r$ is a prime power and $f(x)$ a polynomial of degree $n \geq 5$ with complex coefficients that is in "general position". Here "general position" means that there is a (sub)field K such that all the coefficients of $f(x)$ lie in K and the Galois group of $f(x)$ acts doubly transitively on the set of its roots (in particular, $f(x)$ is irreducible over K). It turns out that for a broad class of the doubly transitive Galois groups (and under certain mild restrictions on q) the corresponding endomorphism algebra is "as small as possible", i.e., is canonically isomorphic to a product of cyclotomic fields $\mathbb{Q}(\zeta_{p^i})$ $(1 \leq i \leq r)$.

In order to state explicitly our results, let us start with the notation and some basic facts related to cyclotomic fields and cyclotomic polynomials. 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 and $\mathbb{F}_p$ the corresponding (finite) prime field of characteristic p. We write $\mathbb{Z}_p$ and $\mathbb{Q}_p$ for the ring of p-adic integers and the field $\mathbb{Q}_p$ of p-adic numbers respectively. Let r be a positive

---

Partially supported by the Simons Foundation Collaboration grant # 585711. Part of this work was done in December 2023 during my stay at the Max-Planck Institut für Mathematik (Bonn, Germany), whose hospitality and support are gratefully acknowledged.

integer and $q = p^r$. Let
$$\zeta_q \in \mathbb{C}.$$
be a primitive qth root of unity. We write $\mathbb{Q}(\zeta_q)$ be the qth cyclotomic field and
$$\mathbb{Z}[\zeta_q] = \sum_{i=0}^{\phi(q)-1} \mathbb{Z} \cdot \zeta_q^i$$
for its ring of integers. (Hereafter $\phi(q) := (p-1)p^{r-1}$ is the Euler function.)

Let us consider the polynomial
$$\mathcal{P}_q(t) := \sum_{j=0}^{q-1} t^j = \prod_{i=1}^{r} \Phi_{p^i}(t) \in \mathbb{Z}[t]$$
where
$$\Phi_{p^i}(t) = \sum_{j=0}^{p-1} t^{ip^{r-1}} \in \mathbb{Z}[t]$$
is the p^ith *cyclotomic* polynomial.

Let $f(x) \in \mathbb{C}[x]$ be a polynomial of degree $n \ge 4$ without repeated roots. In what follows we always assume that *either p does not divide n or q divides n.*

Let $C_{f,q}$ be a smooth projective model of the smooth affine curve
$$y^q = f(x).$$
It is well known ([16], pp. 401–402, [30], Prop. 1 on p. 3359, [21], p. 148) that the genus $g(C_{f,p})$ of $C_{f,p}$ is $(q-1)(n-1)/2$ if p does not divide n and $(q-1)(n-2)/2$ if q divides n. The map
$$(x, y) \mapsto (x, \zeta_p y)$$
gives rise to a non-trivial biregular automorphism
$$\delta_q : C_{f,q} \to C_{f,q}$$
of period q.

Let $J(C_{f,q})$ be the Jacobian of $C_{f,q}$; it is a $g(C_{f,q})$-dimensional abelian variety. We write $\mathrm{End}(J(C_{f,q}))$ for the ring of endomorphisms of $J(C_{f,q})$ and $\mathrm{End}^0(J(C_{f,q})) = \mathrm{End}(J(C_{f,q})) \otimes \mathbb{Q}$ for the endomorphism algebra of $J(C_{f,q})$. By functoriality, δ_q induces an automorphism of $J(C_{f,q})$, which we still denote by δ_q. It is known ([21, p. 149], [23, p. 448], [34, Lemma 4.8]) that
$$\mathcal{P}_q(\delta_q) = 0 \tag{1}$$
in $\mathrm{End}(J(C_{f,q}))$. Then (1) gives rise to the ring homomorphism,
$$\mathbf{i}_{q,f} : \mathbb{Z}[t]/\mathcal{P}_q(t)\mathbb{Z}[t] \hookrightarrow \mathbb{Z}[\delta_q] \subset \mathrm{End}(J(C_{f,q})),\ t + \mathcal{P}_q(t)\mathbb{Z}[t] \mapsto \delta_q, \tag{2}$$
which is a *ring embedding* ([21, p. 149], [23, p. 448], [34, Lemma 4.8]). (The first map in (2) is actually a ring isomorphism.) This implies

that the subring $\mathbb{Z}[\delta_q]$ of $\mathrm{End}(J(C_{f,q}))$ generated by δ_q is isomorphic to $\mathbb{Z}[t]/\mathcal{P}_q(t)\mathbb{Z}[t]$. It follows that the $\mathbb{Q}$-subalgebra

$$\mathbb{Q}[\delta_q] \subset \mathrm{End}^0(J(C_{f,q})) \tag{3}$$

generated by δ_q has $\mathbb{Q}$-dimension $q-1$, is isomorphic to

$$\mathbb{Q}[t]/\mathcal{P}_q(t)\mathbb{Q}[t] \cong \prod_{i=1}^{r} \mathbb{Q}(\zeta_{p^i})$$

and therefore has dimension $q-1$.

We will need the following elementary observation.

Remark 1.1. (i) Suppose that a prime p is greater than n. Then p does *not* divide $n!$. Since every subgroup H of $\mathrm{Gal}(f)$ is isomorphic to a subgroup of $\mathbf{S}_n$, its order $|H|$ divides $n!$ and therefore is *not* divisible by p. Hence, if $p > n$, then $|H|$ is *not* divisible by p.
(ii) Suppose that H is a transitive subgroup of $\mathrm{Gal}(f)$ with respect to the action on the roots of $f(x)$. Then its order $|H|$ is divisible by n.

Let us formulate our main results.

First, we start with the case $q = p$. Then $\mathcal{P}_p(t)$ coincides with $\Phi_p(t)$ and there is a natural ring isomorphism

$$\mathbb{Z}[t]/\mathcal{P}_p(t)\mathbb{Z}[t] \cong \mathbb{Z}[\zeta_p]$$

that sends (the coset of) t to ζ_p. This gives us the the *ring embedding*

$$\mathbf{i}_{p,f} : \mathbb{Z}[\zeta_p] \hookrightarrow \mathbb{Z}[\delta_p] \subset \mathrm{End}(J(C_{f,p})),\ \zeta_p \mapsto \delta_p. \tag{4}$$

Notice also that the rings $\mathbb{Z}[\delta_p]$ and $\mathbb{Z}[\zeta_p]$ are isomorphic.

Theorem 1.2. *Let $n \ge 5$ be an integer and p an odd prime such that K contains a primitive pth root of unity.*

Suppose that the Galois group $\mathrm{Gal}(f)$ of $f(x)$ contains a subgroup H that acts doubly transitively on the n-element set $\mathfrak{R}_f$ of roots of the polynomial $f(x)$ and enjoys the following properties.

(i) *The index of every maximal subgroup of H does not divide $n-1$.*
(ii) *p does not divide $|H|$. (E.g., $p > n$.)*

Then $\mathrm{End}^0(J(C_{f,p})) = \mathbb{Q}[\delta_p]$ *and* $\mathrm{End}(J^{(f,p)}) = \mathbb{Z}[\delta_p]$.

Theorem 1.3. *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 $n \ge 5$ and its Galois group over K is either the full symmetric group $\mathbf{S}_n$ or the alternating group $\mathbf{A}_n$. Then*

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

Remark 1.4. Theorem 1.3 was stated in [37, Th. 4.2]. Its proof was based on an assertion that a certain "permutational" representation $(\mathbb{F}_p^B)^{00}$ (that is called the *heart* [1]) of the alternating group $\mathrm{Alt}(B) = \mathbf{A}_n$ over $\mathbb{F}_p$ is *very simple* [2] [36, Th. 4.7]. Unfortunately, there is an error in the proof of [36, Th. 4.7] when $n = 5, p > 5$, caused by an improper use of [36, Cor. 4.4] (see [36, p. 108, lines 4-5]). So, the proof in [37] works only under an additional assumption that either $n > 5$ or $p \le 5$.

In this note we handle the remaining case when $n = 5,\ p > 5$. It turns out that if $p \not\equiv \pm 1 \mod 5$ then the representation of the group $\mathbf{A}_5$ is very simple, which allows us to salvage in this case the arguments of [36].

However, if $p \equiv \pm 1 \mod 5$ then the 4-dimensional representation $\left(\mathbb{F}_p^B\right)^{00}$ of $\mathbf{A}_5$, viewed as the representaton of the covering group $\mathrm{SL}(2, \mathbb{F}_5)$, splits into a tensor product of two 2-dimensional representations. In particular, $\left(\mathbb{F}_p^B\right)^{00}$ is *not* very simple, and we use a notion of a *central simple representation* (see Section 4 below), in order to prove Theorem 1.3 in this case.

Remarks 1.5. If $f(x) \in K[x]$ then the curve $C_{f,p}$ and its Jacobian $J(C_{f,p})$ are defined over K. Let $K_a \subset \mathbb{C}$ be the algebraic closure of K. Then all endomorphisms of $J(C_{f,p})$ are defined over K_a. Hence, in order to prove Theorems 1.3 and 6.7, it suffices to check that the ring of all K_a-endomorphisms of $J(C_{f,p})$ coincides with $\mathbb{Z}[\delta_p]$.

Now let us try to relax the restrictions on p, keeping the double transitivity of $\mathrm{Gal}(f)$. Our next result deals with doubly transitive sporadic simple (Galois) groups, whose description may be found in [22], [5, Ch. 6 and Ch. 7, Sect. 7.7, p. 252-253].

Theorem 1.6. *Let p be an odd prime and*

$$\mathrm{Gal}(f) \subset \mathrm{Perm}(\mathfrak{R}_f) \cong \mathbf{S}_n$$

a permutation group that acts doubly transitively on the n-element set $\mathfrak{R}_f$. Suppose that $(n, \mathrm{Gal}(f))$ enjoys one of the following properties.

- **(M)** $n \in \{11, 12, 22, 23, 24\}$, *and* $\mathrm{Gal}(f)$ *is isomorphic to the corresponding Mathieu group* $\mathbf{M}_n$. *If $n = 11$ then we assume additionally that $p > 3$.*
- **(HS)** $n = 176,\ p > 7,$ *and* $\mathrm{Gal}(f))$ *is isomorphic to the sporadic simple Higman-Sims group* HS.
- **(CO3)** $n = 276,\ p \notin \{3, 5, 11\}$, *and* $\mathrm{Gal}(f))$ *is isomorphic to the sporadic simple Conway group* Co_3.

Then $\mathrm{End}^0(J(C_{f,p})) = \mathbb{Q}[\delta_p]$ *and* $\mathrm{End}(J(C_{f,p})) = \mathbb{Z}[\delta_p]$.

[1] See [17, 13] and Section 3 below for the definition of the *heart*.

[2] See [34, 38] and Section 4 below for the definition and basic properties of very simple representations.

Remark 1.7. The case (**M**) of Theorem 1.6 gives a (partial) answer to a question of Ravi Vakil that was asked during my talk at Simons Symposium "Geometry Over Non-closed Fields" (Puerto Rico, March 2015).

Now let us discuss the case when our Galois groups are doubly transitive finite simple *Chevalley groups* - they are classified in [4] and their action described in details in [5, Sect. 7.7]. (For general results about Chevalley groups see [28].)

Theorem 1.8. *Suppose that p be an odd prime and* $\mathrm{Gal}(f)$ *contains a subgroup H that acts doubly transitively on the n-element set $\mathfrak{R}_f$ and is isomorphic to a finite Chevalley group $\mathfrak{G}(\mathfrak{q})$, and the corresponding stabilizers correspond to Borel subgroups of $\mathfrak{G}(\mathfrak{q})$, which are maximal subgroups of index n.*

Suppose that $(n, \mathfrak{G}(\mathfrak{q}), p)$ enjoys one of the following properties.

(**L2**) *Let ℓ be a prime and $\mathfrak{r}$ a positive integer. Then $n = \mathfrak{q}+1$ where $\mathfrak{q} = \ell^{\mathfrak{r}} > 11$ and $\mathfrak{G}(\mathfrak{q})$ is the projective special linear group*

$$\mathbf{L}_2(\mathfrak{q}) = \mathrm{PSL}(2, \mathbb{F}_{\mathfrak{q}})$$

where $\mathbb{F}_{\mathfrak{q}}$ is a finite $\mathfrak{q}$-element field. Assume additionally that either $p \neq \ell$ or $\mathfrak{q} = \ell = p$.

(**Lmq**) *Let $m \geq 3$ be an integer, ℓ a prime, $\mathfrak{r}$ a positive integer. Then $n = (\mathfrak{q}^m - 1)/(\mathfrak{q} - 1)$ where $\mathfrak{q} = \ell^{\mathfrak{r}}$ and $\mathfrak{G}(\mathfrak{q})$ is the projective special linear group*

$$\mathbf{L}_m(\mathfrak{q}) = \mathrm{PSL}(m, \mathbb{F}_{\mathfrak{q}})$$

where $\mathbb{F}_{\mathfrak{q}}$ is a finite $\mathfrak{q}$-element field. Assume additionally that $p \neq \ell$ and

$$(m, \mathfrak{q}) \neq (3,2), (3,4), (4,2), (4,3), (6,2), (6,3).$$

(**U3**) *Let ℓ be a prime and $\mathfrak{r}$ a positive integer. Then $n = \mathfrak{q}^3+1$ where $\mathfrak{q} = \ell^{\mathfrak{r}}$ is a power of a prime ℓ,*

$$\mathfrak{q} \neq 2, 5$$

and $\mathfrak{G}(\mathfrak{q})$ is the projective special unitary group $\mathbf{U}_3(q) = \mathrm{PSU}_3(\mathbb{F}_q)$.

(**Sz**) *Let $\mathfrak{r}$ be a positive integer,*

$$\mathfrak{q} = 2^{2\mathfrak{r}+1}, \quad n = q^2 + 1, \ m = 2^{\mathfrak{r}+1}.$$

Then H is the simple Suzuki group $\mathrm{Sz}(\mathfrak{q}) = {}^2\,\mathrm{B}_2(q)$. In addition, p does not divide $(q+1+m)$.

(**Ree**) *Let $\mathfrak{r}$ be a positive integer,*

$$\mathfrak{q} = 3^{2\mathfrak{r}+1}, \quad n = q^2 + 1, \ m = 3^{\mathfrak{r}+1}.$$

The group H is the simple Ree group $\mathrm{Ree}(\mathfrak{q}) = {}^2\,\mathrm{G}_2(q)$. In addition, p does not divide $3(q+1)(q+m+1)(q-m+1)$.

Then $\mathrm{End}^0(J(C_{f,p})) = \mathbb{Q}[\delta_p]$ *and* $\mathrm{End}(J(C_{f,p})) = \mathbb{Z}[\delta_p]$.

Now let us assume that r is any positive integer (recall that $q = p^r$). In this case we obtain the results about the *endomorphism algebra* $\mathrm{End}^0(J(C_{f,q})) = \mathrm{End}(J(C_{f,q})) \otimes \mathbb{Q}$ of $J(C_{f,q})$ that may be viewed as analogues of Theorems 1.3 and Theorem 1.2 for the endomorphism algebra $\mathrm{End}^0(J(C_{f,q})$.

Theorem 1.9. *Suppose that $n \geq 5$ is an integer, p an odd prime, q divides n, and K contains a primitive qth root of unity.*

Let us assume that the Galois group $\mathrm{Gal}(f)$ of $f(x)$ contains a subgroup H that acts doubly transitively on the n-element set $\mathfrak{R}_f$ of roots of the polynomial $f(x)$ and enjoys the following properties.

(i) *The index of every maximal subgroup of H does not divide $n-1$.*
(ii) *p does not divide $|H|$. (E.g., $p > n$.)*

Then

$$\mathrm{End}^0(J(C_{f,q})) = \mathbb{Q}[\delta_q] \cong \prod_{i=1}^{r} \mathbb{Q}(\zeta_{p^i}).$$

Theorem 1.10. *Let K be a subfield of $\mathbb{C}$ such that all the coefficients of $f(x)$ lie in K. Suppose that $f(x)$ is an irreducible polynomial in $K[x]$ of degree $n \geq 5$ and its Galois group over K is either the full symmetric group $\mathbf{S}_n$ or the alternating group $\mathbf{A}_n$. Assume also that either p does not divide n or q divides n. Then*

$$\mathrm{End}^0(J(C_{f,q})) = \mathbb{Q}[\delta_q] \cong \prod_{i=1}^{r} \mathbb{Q}(\zeta_{p^i}).$$

Remark 1.11. Theorem 1.10 was stated in [34, Th. 1.1]. Similarly (see Remark 1.4), the proof in [34] works only under an additional assumption that either $n > 5$ or $p \leq 5$. In this paper we handle the remaining case $n = 5, p > 5$.

Remark 1.12. An analogue of Theorem 1.10 when $p \mid n$ but q does *not* divide n was proven in [33].

The paper is organized as follows. In Section 2 we discuss complex abelian varieties Z with multiplications from cyclotomic fields, paying special attention to the centralizers of these fields in $\mathrm{End}^0(Z)$ and their action on the differentials of the first kind when Z is a superelliptic Jacobian In Section 3 we discuss modular representations of permutation groups, paying a special attention to the *hearts* of these representations. In Section 4 we introduce central simple representations and recall basic properties of very simple representations that first appeared in [34, 38], paying a special attention to the very simplicity and central simplicity of hearts of permutational representations in the case of doubly transitive permutation groups. In Section 5 we return to our discussion of abelian varieties Z with multiplications from cyclotomic fields $\mathbb{Q}(\zeta_q)$, paying a special attention to the Galois properties of the set of δ_q-invariants. In Section 6 we review results of [37] about endomorphism algebras of superelliptic Jacobians. In Section 7 we prove our main results that deal with the case $q = p$. The proofs for the case of arbitrary q are contained in Section 8.

Acknowledgements. I am grateful to the referee, whose comments helped to improve the exposition.

2. Endomorphism fields of abelian varieties and their centralizers

In what follows E is a number field and O_E the ring of algebraic integers in E. It is well known that O_E is a Dedekind ring and therefore every finitely generated torsion-free O_E-module is projective/locally free and isomorphic to a direct sum of locally free O_E-modules of rank 1. In addition, the natural map

$$O_E \otimes \mathbb{Q} \to E, \ e \otimes c \mapsto c \cdot e \ \forall e \in E, \ c \in \mathbb{Q}$$

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

Let Z be an abelian variety over $\mathbb{C}$ of positive dimension g, let $\mathrm{End}(Z)$ be the ring of its endomorphisms. If n is an integer then we we write n_Z for the endomorphism

$$n_Z : Z \to Z, \ z \mapsto nz.$$

Clearly, $n_Z \in \mathrm{End}(Z)$. By definition, 1_Z is the identity selfmap of Z. In addition, $n_Z : Z \to Z$ is an *isogeny* if and only if $n \neq 0$.

We write

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

for the corresponding endomorphism algebra of Z, which is a finite-dimensional semisimple $\mathbb{Q}$-algebra. Identifying $= \mathrm{End}(Z)$ with

$$\mathrm{End}(Z) \otimes 1 \subset \mathrm{End}(Z) \otimes \mathbb{Q} = \mathrm{End}^0(Z),$$

we may view $\mathrm{End}(Z)$ as an **order** in the $\mathbb{Q}$-algebra $\mathrm{End}^0(Z)$.

The action of $\mathrm{End}(Z)$ by functoriality on the g-dimensional complex vector space $\Omega^1(Z)$ of differentials of the first kind on Z gives us the ring homomorphism $\mathrm{End}(Z) \to \mathrm{End}_{\mathbb{C}}(\Omega^1(Z)$ [27, Ch. 1, Sect. 2.8], which extends by $\mathbb{Q}$-linearity to the homomorphism of $\mathbb{Q}$-algebras

$$j_Z : \mathrm{End}^0(Z) \to \mathrm{End}_{\mathbb{C}}(\Omega^1(Z)), \tag{5}$$

which sends 1_Z to the identity automorphism of the $\mathbb{C}$-vector space $\Omega^1(Z)$. Let E be a number field that is a $\mathbb{Q}$-subalgebra of $\mathrm{End}^0(Z)$ with the same $1 = 1_Z$. Let Σ_E be the $[E : \mathbb{Q}]$-element set of field embeddings $\sigma : E \hookrightarrow \mathbb{C}$. Let us define for each $\sigma \in \Sigma_E$ the corresponding *weight subspace*

$$\Omega^1(Z)_\sigma = \{\omega \in \Omega^1(Z) \mid j_Z(e)\omega = \sigma(e)\omega \ \forall e \in E\} \subset \Omega^1(Z).$$

The well known splitting

$$E \otimes_{\mathbb{Q}} \mathbb{C} = \oplus_{\sigma \in \Sigma_E} E \otimes_{E,\sigma} \mathbb{C} = \oplus_\sigma \mathbb{C}_\sigma \quad \text{where } \mathbb{C}_\sigma = E \otimes_{E,\sigma} \mathbb{C} = \mathbb{C}$$

implies that

$$\Omega^1(Z) = \oplus_{\sigma\in\Sigma_E}\Omega^1(Z)_\sigma.$$

Let us put

$$n_\sigma = \dim_{\mathbb{C}}(\Omega^1(Z)_\sigma).$$

Let D be the centralizer of E in $\mathrm{End}^0(Z)$. Clearly, E lies in the center of D, which makes D is a finite-dimensional E-algebra. It is also clear that each subspace $\Omega^1(Z)_\sigma$ is $j_Z(D)$-invariant, which gives us a $\mathbb{Q}$-algebra homomorphism

$$j_{Z,\sigma}: D \to \mathrm{End}_{\mathbb{C}}(\Omega^1(Z)_\sigma), \tag{6}$$

that sends $1 = 1_Z \in D$ to the identity automorphism of the $\mathbb{C}$-vector space $\Omega^1(Z)_\sigma$.

Lemma 2.1. *Let D be as above. Suppose that D is a central simple E-algebra of dimension d^2 where d is a positive integer. Then:*

(i) *d divides all the multiplicities n_σ. In particular, if $n_\sigma = 1$ for some $\sigma \in \Sigma_E$ then $d = 1$ and $D = E$.*

(ii) *Let M be the the number of σ's with $n_\sigma \neq 0$. Then*

$$dM \le \dim(Z).$$

In particular, if $d = 2\dim(Z)/[E:\mathbb{Q}]$ then $M \le [E:\mathbb{Q}]/2$.

Proof. Our condition on D implies that $D_\sigma = D \otimes_{E,\sigma} \mathbb{C}$ is isomorphic to the matrix algebra $\mathrm{Mat}_d(\mathbb{C})$ of size d over $\mathbb{C}$ for all $\sigma \in \Sigma_E$.

We may assume that $n_\sigma > 0$. Then $\Omega^1(Z)_\sigma \neq \{0\}$ and $j_{Z,\sigma}(D) \neq \{0\}$. Extending $j_{Z,\sigma}$ by $\mathbb{C}$-linearity, we get a $\mathbb{C}$-algebra homomorphism

$$D_\sigma \to \mathrm{End}_{\mathbb{C}}((\Omega^1(Z)_\sigma),$$

which provides $\Omega^1(Z)_\sigma$ with the structure of a $D_\sigma = \mathrm{Mat}_d(\mathbb{C})$-module. This implies that each n_σ is divisible by d. This proves (i). In order to prove (ii), it suffices to notice that

$$\dim(Z) = \sum_\sigma \dim_{\mathbb{C}}(\Omega^1(Z)_\sigma) = \sum_\sigma n_\sigma \ge dM.$$

$\square$

Remark 2.2. (i) Let Λ be the centralizer of δ_p in $\mathrm{End}(J(C_{f,p}))$, which coincides with the centralizer of $\mathbb{Z}[\delta_p]$ in $\mathrm{End}(J(C_{f,p}))$. Let us consider the $\mathbb{Q}$-subalgebra

$$\Lambda_{\mathbb{Q}} = \Lambda \otimes \mathbb{Q} \subset \mathrm{End}(J(C_{f,p})) \otimes \mathbb{Q} = \mathrm{End}^0(J(C_{f,p})).$$

Clearly, $\Lambda_{\mathbb{Q}}$ coincides with the centralizer of $\mathbb{Q}[\delta_p]$ in $\mathrm{End}^0(J(C_{f,p}))$. Since δ_p respects the *theta divisor* on the Jacobian $J(C_{f,p})$, the algebra $\Lambda_{\mathbb{Q}}$ is stable under the corresponding *Rosati involution* and therefore is semisimple as a $\mathbb{Q}$-algebra. It is also clear that the number field $\mathbb{Q}[\delta_p] \cong \mathbb{Q}(\zeta_p)$ lies in the center of $\Lambda_{\mathbb{Q}}$. Hence, $\Lambda_{\mathbb{Q}}$ becomes a semisimple $\mathbb{Q}[\delta_p]$-algebra.

(ii) Let i be an integer such that $1 \le i \le p-1$. We write σ_i for the field embedding
$$\sigma_i : \mathbb{Q}[\delta_p] \hookrightarrow \mathbb{C}$$
that sends δ_p to ζ_p^{-i}. Let us consider the corresponding subspace $\Omega^1(J(C_{f,p}))_{\sigma_i}$ of differentials of the first kind on $J(C_{f,p})$. It is known [37, Remark 3.7] that if p does *not* divide n then
$$n_{\sigma_i} = \dim_{\mathbb{C}}(\Omega^1(J(C_{f,p}))_{\sigma_i}) = \left[\frac{ni}{p}\right]. \tag{7}$$

(iii) It follows from Lemma 2.1 applied to $Z = J(C_{f,p})$ and $E = \mathbb{Q}[\delta_p]$ that if p does *not* divide n and $\Lambda_{\mathbb{Q}}$ is a central simple $\mathbb{Q}[\delta_p]$-algebra of dimension d^2 then d divides all $[ni/p]$ for all integers i with $1 \le i \le p-1$.

(iv) Suppose that either $n = p+1$, or $n-1$ is *not* divisible by p. Then the greatest common divisor of all n_{σ_i}'s is 1 [39, Lemma 8.1(D) on p. 516–517]. It follows that if $\Lambda_{\mathbb{Q}}$ is a central simple $\mathbb{Q}[\delta_p]$-algebra then $\Lambda_{\mathbb{Q}} = \mathbb{Q}[\delta_p]$.

(v) Suppose that p divides $n-1$, say, $n = kp+1$ where k is an integer. Then the greatest common divisor of all n_{σ_i}'s is k. [39, Lemma 8.1(D) on p. 516–517] It follows that if $\Lambda_{\mathbb{Q}}$ is a central simple $\mathbb{Q}[\delta_p]$-algebra of dimension d^2 then d divides k.

(vi) The number of i with $n_{\sigma_i} > 0$ is at least $(p+1)/2$ [36, p. 101]. It follows that if $\Lambda_{\mathbb{Q}}$ is a central simple $\mathbb{Q}[\delta_p]$-algebra of dimension d^2 then, in light of Proposition 2.1,
$$d \cdot \frac{p+1}{2} \le g$$
where $g = \dim(J(C_{f,p}))$ is the genus of $C_{f,p}$. This implies that
$$d \le \frac{2g}{p+1} < \frac{2g}{p-1}.$$

Lemma 2.3. *Let $\mathcal{H}$ be a finite-dimensional E-algebra, and Λ an order in $\mathcal{H}$ that contains O_E. (In particular, Λ is a finitely generated torsion-free O_E-module and the natural map $\Lambda \otimes \mathbb{Q} \to \mathcal{H}$ is an isomorphism of finite-dimensional $\mathbb{Q}$-algebras.)*

Suppose that there are a positive integer d and a maximal ideal $\mathfrak{m}$ of O_E with residue field $k = O_E/\mathfrak{m}$ such that the k-algebra $\Lambda/\mathfrak{m}\Lambda$ is isomorphic to the matrix algebra $\mathrm{Mat}_d(k)$ of size d over k.

Then $\mathcal{H}$ is a central simple E-algebra of dimension d^2.

Proof. Let $C_{\mathbb{Q}}$ the center of $\mathcal{H}$ that is a finite-dimensional commutative E-algebra. Then $C := C_{\mathbb{Q}} \cap \Lambda$ is the center of Λ.

Clearly, C contains O_E and is a saturated O_E-submodule of Λ. The latter means that if $eu \in C$ for some $u \in \Lambda$ and nonzero $e \in O_E$ then $u \in \Lambda$. This implies that the quotient Λ/C is torsion-free (and finitely generated) O_E-module and therefore is projective. It follows that C

is a direct summand of the O_E-module D and therefore there is an O_E-submodule $\mathfrak{P}$ of Λ such that

$$\Lambda = C \oplus \mathfrak{P}.$$

Similarly, O_E is a saturated O_E-submodule of C and, by the same token, there is a locally free O_E-submodule $\mathfrak{Q}$ of C such that

$$C = O_E \oplus \mathfrak{Q} \text{ and } \Lambda = C \oplus \mathfrak{P} = O_E \oplus \mathfrak{Q} \oplus \mathfrak{P}.$$

Then the the natural map of $O_E/\mathfrak{m} = k$-modules,

$$O_E/\mathfrak{m} \oplus \mathfrak{Q}/\mathfrak{m}\mathfrak{Q} = C/\mathfrak{m}C \to \Lambda/\mathfrak{m}\Lambda \cong \mathrm{Mat}_d(k)$$

is *injective* and its image lies in the center k of $\mathrm{Mat}_d(k)$. The k-dimension arguments imply that $\mathfrak{Q}/\mathfrak{m}\mathfrak{Q} = \{0\}$. Since $\mathfrak{Q}$ is finitely generated projective, $\mathfrak{Q} = \{0\}$, i.e., $C = O_E$ and the center of $\mathcal{H}$ is

$$C_{\mathbb{Q}} = C \otimes \mathbb{Q} = O_E \otimes \mathbb{Q} = E.$$

Hence, $\mathcal{H}$ is a finite-dimensional E-algebra with center E.

Let us check the simplicity of $\mathcal{H}$. Let $J_{\mathbb{Q}}$ be a proper two-sided ideal of $\mathcal{H}$. We need to check that $J_{\mathbb{Q}} = \{0\}$. In order to do that, let us consider the intersection $J := J_{\mathbb{Q}} \cap \Lambda$, which is obviously a two-sided ideal of Λ. It is also clear that J is a saturated O_E-submodule of Λ, i.e., the quotient Λ/J is a torsion free (finitely generated) O_E-module. Hence, Λ/J is a projective O_E-module. It follows that J is a direct summand of the O_E-module Λ, i.e., there exists an O_E-submodule $\mathfrak{Q}$ of Λ such that $\Lambda = J \oplus \mathfrak{Q}$. If $\mathfrak{Q} = \{0\}$ then $\Lambda = J$ and

$$\mathcal{H} = \Lambda \otimes \mathbb{Q} = J \otimes \mathbb{Q} = J_{\mathbb{Q}};$$

so $J_{\mathbb{Q}} = \mathcal{H}$, which is not true, because $J_{\mathbb{Q}}$ is a *proper* ideal of $\mathcal{H}$. This implies that $\mathfrak{Q} \ne \{0\}$ and therefore $\mathfrak{Q}/\mathfrak{m}\mathfrak{Q} \ne \{0\}$. We have

$$\Lambda/\mathfrak{m}\Lambda = J/\mathfrak{m}J \oplus \mathfrak{Q}/\mathfrak{m}\mathfrak{Q}.$$

Clearly, $J/\mathfrak{m}J$ is a proper two-sided ideal of the simple algebra $\Lambda/\mathfrak{m}\Lambda \cong \mathrm{Mat}_d(k)$. This implies that $J/\mathfrak{m}J = \{0\}$, which implies that $J = \{0\}$ and therefore $J_{\mathbb{Q}} = \{0\}$.

To summarize: $\mathcal{H}$ is a simple finite-dimensional E-algebra with center E, i.e., a finite-dimensional central simple E-algebra.

On the other hand, the E-dimension of $\mathcal{H}$ equals the rank of the locally free O_E-module Λ, which, in turn, equals the $k = O_E/\mathfrak{m}$-dimension of $\Lambda/\mathfrak{m}\Lambda$. Since $\Lambda/\mathfrak{m}\Lambda \cong \mathrm{Mat}_d(k)$ has k-dimension d^2, the E-dimension of H is also d^2. It follows that $\mathcal{H}$ is a central simple E-algebra of dimension d^2.

□

3. Permutation groups and permutation modules

Our exposition in this section follows closely [36, Sect. 2], see also [17].

Let $n \geq 5$ be an integer, B a n-element set, and $\mathrm{Perm}(B)$ the group of permutations of B, which is isomorphic to the full symmetic group S_n. The group S_n has order $n!$ and contains precisely one (normal) subgroup of index 2 that we denote by $\mathrm{Alt}(B)$. Any isomorphism between $\mathrm{Perm}(B)$ and S_n induces an isomorphism between $\mathrm{Alt}(B)$ and the alternating group $\mathbf{A}_n$. Since $n \geq 5$, the group $\mathrm{Alt}(B)$ is simple non-abelian; its order is $n!/2$. Let G be a subgroup of $\mathrm{Perm}(B)$.

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 $\mathrm{Perm}(B)$ defined as follows. Each $s \in \mathrm{Perm}(B)$ sends a map $h : B \to F$ into $sh : b \mapsto h(s^{-1}(b))$. The permutation module F^B contains the $\mathrm{Perm}(B)$-stable hyperplane

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

and the $\mathrm{Perm}(B)$-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 $\mathrm{Perm}(B)$-module.

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

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

Let G be a subgroup of $\mathrm{Perm}(B)$. Clearly, F^B and $(F^B)^0$ carry natural structures of G-modules or (which is the same) of $F[G]$-modules. (Hereafter $F[G]$ stands for the *group algebra* of G.)

If $F = \mathbb{Q}$ then the character of $\mathbb{Q}^B$ sends each $g \in G$ to the number of fixed points of g in B ([26], ex. 2.2, p.12); it takes on values in $\mathbb{Z}$ and called the *permutation character* of B. Let us denote by $\phi = \phi_B : G \to \mathbb{Q}$ the character of $(\mathbb{Q}^B)^0$.

If $\mathrm{char}(F) = 0$ then the $F[G]$-module $(F^B)^0$ is absolutely simple [3] if and only if the action of G on B is doubly transitive ([26, ex. 2.6, p. 17], [17]). (Notice that $1 + \phi$ is the permutation character. This implies that the character ϕ also takes on values in $\mathbb{Z}$.) In particular, $\mathbb{Q}_p[G]$-module $(\mathbb{Q}_p^B)^0$ is absolutely simple if and only if the action of G on B is doubly transitive.

In what follows we concentrate on the case of $F = \mathbb{F}_p$.

Remark 3.1.
- Let p be a prime that does *not* divide the order of G. This condition is automatically fulfilled if $p > n$, because G, being isomorphic to a subgroup of $\mathbf{S}_n$, has order that divides $n!$.

[3] Recall that a simple $F[G]$-module V is called *absolutely simple* if the centralizer of G in $\mathrm{End}_F(V)$ coincides with F or equivalently the natural homomorphism $F[G] \to \mathrm{End}_F(V)$ of F-algebras is surjective.

- Suppose that the action of G on B is *doubly transitive*. Taking into account that the representation theory of G over $\mathbb{Q}_p$ is "the same over $\mathbb{F}_p$ as over $\mathbb{Q}_p$" ([26, Sect. 15.5, Prop.43], [17]), we conclude that the $\mathbb{F}_p[G]$-module $(\mathbb{F}_p^B)^0$ is *absolutely simple* (see also [39, Cor. 7.5 on p. 513]).

Definition 3.2. Let G be a subgroup of $\mathrm{Perm}(B)$.

If $p \mid n$ then let us define the G-module

$$\left(\mathbb{F}_p^B\right)^{00} := (\mathbb{F}_p^B)^0/(\mathbb{F}_p \cdot 1_B).$$

If p does not divide n then let us put

$$\left(\mathbb{F}_p^B\right)^{00} := (\mathbb{F}_p^B)^0.$$

The G-module $(\mathbb{F}^B)^0$ is called the *heart* of the permutation representation of G on B [17]. It follows from the definition that $\dim_{\mathbb{F}_p}(\left(\mathbb{F}_p^B)^{00}\right)) = n-1$ if n is not divisible by p and $\dim_{\mathbb{F}_p}(\left(\mathbb{F}_p^B)^{00}\right) = n-2$ if $p \mid n$.

Lemma 3.3. *Assume that* $G = \mathrm{Perm}(B)$ *or* $\mathrm{Alt}(B)$. *Then the* G-*module* $\left(\mathbb{F}_p^B\right)^{00}$ *is absolutely simple.*

Proof. This result is well known (and goes back to Dickson). See [3, Th. 5.2 on p. 133], [31], [17], [36, Lemma 2.6]. □

Remark 3.4. It turns out that the case of $n = 5$ and

$$G = \mathrm{Alt}(B) \cong \mathbf{A}_5 \cong \mathrm{PSL}(2, \mathbb{F}_5) = \mathrm{SL}(2, \mathbb{F}_5)/\{\pm 1\}$$

is rather special when

$$p \equiv \pm 1 \bmod 5. \tag{8}$$

Namely, in this case $p > 5$ and the $G = \mathrm{PSL}(2, \mathbb{F}_5)$-module $(\mathbb{F}_p^B)^{00} = (\mathbb{F}_p^B)^0$ viewed as the $\mathrm{SL}(2, \mathbb{F}_5)$-module splits into a nontrivial tensor product. In order to see this, recall [7, Sect. 38] that $\mathrm{SL}(2, \mathbb{F}_5)$ has the ordinary character θ_2 of degree 4 (which, is the lift of ϕ_5 from $\mathbf{A}_5$) and two *ordinary irreducible* characters η_1 and η_2 of degree 2 with

$$\mathbb{Q}(\eta_1) = \mathbb{Q}(\eta_2) = \mathbb{Q}(\sqrt{5}),$$

whose product $\eta_1\eta_2$ coincides with θ_2. By the quadratic reciprocity law, the congruence (8) implies that $\sqrt{5} \in \mathbb{F}_p$ and therefore $\sqrt{5}$ lies in the field $\mathbb{Q}_p$ of p-adic numbers, because $p \neq 2, 5$ is *odd*. This means that

$$\mathbb{Q}_p(\eta_1) = \mathbb{Q}_p(\eta_2) = \mathbb{Q}_p.$$

By a theorem of Janusz [12, Theorem (d) on p. 3-4], characters of both η_1 and η_2 can be realized over $\mathbb{Q}_p$, i.e., there are two-dimensional $\mathbb{Q}_p$-vector spaces V_1 and V_2 and linear representations

$$\rho_1 : \mathrm{SL}(2, \mathbb{F}_5) \to \mathrm{Aut}_{\mathbb{Q}_p}(V_1) \cong \mathrm{GL}(2, \mathbb{Q}_p), \tag{9}$$

$$\rho_2 : \mathrm{SL}(2, \mathbb{F}_5) \to \mathrm{Aut}_{\mathbb{Q}_p}(V_2) \cong \mathrm{GL}(2, \mathbb{Q}_p),$$

whose *characters* are η_1 and η_2 respectively. Let T_1 and T_2 be any $\mathrm{SL}(2,\mathbb{F}_5)$-invariant $\mathbb{Z}_p$-lattices of rank 2 in V_1 and V_2 respectively. Since the order 120 of the group $\mathrm{SL}(2,\mathbb{F}_5)$ is prime to p and the $\mathbb{Q}_p[\mathrm{SL}(2,\mathbb{F}_5)]$-modules V_1 and V_2 are simple, it follows from [26, Sect. 15.5, Prop. 43]) that their *reductions* modulo p

$$\bar{V}_1 = T_1/pT_1, \ \bar{V}_2 = T_2/pT_2$$

are simple $\mathbb{F}_p[\mathrm{SL}(2,\mathbb{F}_5)]$-modules. On the other hand, the tensor product

$$T := T_1 \otimes_{\mathbb{Z}_p} T_2 \subset V_1 \otimes_{\mathbb{Q}_p} V_2$$

is a $\mathrm{SL}(2,\mathbb{F}_5)$ -invariant $\mathbb{Z}_p$-lattice of rank 4 in $V_1 \otimes_{\mathbb{Q}_p} V_2 =: V$. The equality

$$\eta_1\eta_2 = \theta_2 \tag{10}$$

of the corresponding class functions on $\mathrm{SL}(2,\mathbb{F}_5)$ implies (if we take into account that ϕ_B is irreducible) that the $\mathbb{Q}_p[\mathrm{SL}(2,\mathbb{F}_5)]$-module V is simple and the $\mathbb{F}_p[\mathrm{SL}(2,\mathbb{F}_5)]$-module

$$T/pT = \big(T_1 \otimes_{\mathbb{Z}_p} T_2\big)/p = (T_1/pT_1) \otimes_{\mathbb{F}_p} (T_1/pT_1) = \bar{V}_1 \otimes_{\mathbb{F}_p} \bar{V}_2 \tag{11}$$

is simple. On the other hand, the equality (10) implies the existence of an isomorphism

$$u : V = V_1 \otimes_{\mathbb{Q}_p} V_2 \cong (\mathbb{Q}_p^B)^0$$

of the $\mathbb{Q}_p[\mathrm{SL}(2,\mathbb{F}_5)]$-modules.

Obviously,

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

is a $\mathrm{SL}(2,\mathbb{F}_5)$-invariant $\mathbb{Z}_p$-lattice of rank 4 in $(\mathbb{Q}_p^B)^0$. (Here $\mathrm{SL}(2,\mathbb{F}_5)$ acts on $(\mathbb{Q}_p^B)^0$ through the quotient $\mathrm{SL}(2,\mathbb{F}_5)/\{\pm 1\} = \mathbf{A}_5$.) Notice that $u(T)$ is a (may be, another) $\mathrm{SL}(2,\mathbb{F}_5)$-invariant $\mathbb{Z}_p$-lattice of rank 4 in $(\mathbb{Q}_p^B)^0$ and the $\mathbb{F}_p[\mathrm{SL}(2,\mathbb{F}_5)]$-module $u(T)/p\, u(T)$ is obviously isomorphic to T/pT. In light of [26, Sect. 15.1, Th. 32], the *simplicity* of the $\mathbb{F}_p[\mathrm{SL}(2,\mathbb{F}_5)]$-modules T/pT (and, hence, of $u(T)/p\, u(T)$) implies that the $\mathbb{F}_p[\mathrm{SL}(2,\mathbb{F}_5)]$-modules T/pT and $(\mathbb{Z}_p^B)^0/p(\mathbb{Z}_p^B)^0$ are isomorphic. Taking into account (11) and that $(\mathbb{Z}_p^B)^0/p\cdot(\mathbb{Z}_p^B)^0 = (\mathbb{F}_p^B)^0$, we conclude that that the $\mathrm{SL}(2,\mathbb{F}_5)$-modules $\bar{V}_1 \otimes_{\mathbb{F}_p} \bar{V}_2$ and $(\mathbb{F}_p^B)^0$ are isomorphic.

Remark 3.5. One may find an explicit construction of the group embeddings $\mathrm{SL}(2,\mathbb{F}_5) \to \mathrm{GL}(2,\mathbb{F}_p)$ (when p satisfies (8)) in the book of M. Suzuki [29, Ch. 3, Sect. 6].

4. Very simple and central simple representations

Definition 4.1. Let V be a vector space of over a field F, let G be a group and $\rho : G \to \mathrm{Aut}_F(V)$ a linear representation of G in V. Let $R \subset \mathrm{End}_F(V)$ be a F-subalgebra containing the identity map

$$\mathrm{Id} : V \to V.$$

(i) We say that R is G-normal if

$$\rho(\sigma)R\rho(\sigma)^{-1} \subset R \quad \forall \sigma \in G.$$

(ii) We say that a normal G-subalgebra is *obvious* if it coincides either with $F \cdot \mathrm{Id}$ or with $\mathrm{End}_F(V)$.

(iii) We say that the G-module V is *very simple* if every G-normal subalgebra of $\mathrm{End}_F(V)$ is obvious.

(iii) We say that the G-module V is *cental simple* if every G-normal subalgebra of $\mathrm{End}_F(V)$ is a central simple F-algebra.

(iv) We say that the G-module V is *strongly simple* if every G-normal subalgebra of $\mathrm{End}_F(V)$ is a simple F-algebra.

Remark 4.2. (i) Clearly, a very simple G-module is central simple and strongly simple. It is also clear that a central simple G-module is strongly simple.

(ii) Clearly, a subalgebra $R \subset \mathrm{End}_F(V)$ is G-normal if and only if it is $\rho(G)$-normal. It follows readily that the G-module V is very simple (resp. central simple) (resp. strongly simple) if and only if the corresponding $\rho(G)$-module V is very simple (resp. central simple) (resp. strongly simple). It is known [34, Rem. 2.2(ii)] that a very simple module is absolutely simple.

(iii) If R is a G-normal subalgebra of $\mathrm{End}_F(V)$ then

$$\rho(\sigma)R\rho(\sigma)^{-1} = R \quad \forall \sigma \in G.$$

Indeed, suppose that there is $u \in R$ such that for some $\sigma \in G$

$$u \notin \rho(\sigma)R\rho(\sigma)^{-1}.$$

This implies that

$$\rho(\sigma^{-1})u\rho(\sigma^{-1})^{-1} = \rho(\sigma)^{-1}u\rho(\sigma) \notin \rho(\sigma)^{-1}\big(\rho(\sigma)R\rho(\sigma)^{-1}\big)\rho(\sigma) = R.$$

It follows that

$$\rho(\sigma^{-1})R\rho(\sigma^{-1})^{-1} \not\subset R,$$

which contradicts the normality of R, because $\sigma^{-1} \in G$. (Of course, if $\dim_F(V)$ is finite, the desired equality follows readily from the coincidence of F-dimensions of R and $\rho(\sigma)R\rho(\sigma)^{-1}$.)

(iv) If G' is a subgroup of G then every G-normal subalgebra is also a normal G'-subalgebra. It follows that if the G'-module V is very simple then the G-module V is also very simple.

(v) Let us check that a strongly simple G-module V is simple. Indeed, if it is not then there is a *proper* G-invariant F-vector subspace W of V. Then the F-subalgebra

$$R := \{u \in \mathrm{End}_F(V) \mid u(W) \subset W\}$$

is G-normal but even *not semisimple*, because it contains a proper two-sided ideal

$$I(W,V) := \{u \in \mathrm{End}_F(V) \mid u(V) \subset W\}.$$

This proves the simplicity of V.

The centralizer $\mathrm{End}_G(V)$ is obviously G-normal. This implies that it is a division algebra over F. (Actually, it follows from the simplicity of the G-module V.

If the G-module V is central simple (resp. very simple) then normal $\mathrm{End}_G(V)$ is a central division F-algebra (resp. coincides with $F \cdot \mathrm{Id}$).

(vi) If R is a G-normal subalgebra of $\mathrm{End}_F(V)$ then for each $\sigma \in G$ the map

$$R \to R, \ u \mapsto \rho(\sigma)u\rho(\sigma)^{-1}$$

is an *automorphism* of the F-algebra R (in light of (iii)). This implies that if C is the center of R then

$$\rho(\sigma)C\rho(\sigma)^{-1} = C$$

for all $\sigma \in G$. This means that C is a G-normal subalgebra of $\mathrm{End}_F(V)$.

Recall that a module V over a ring R is called *isotypic* if either V is simple or is isomorphic to direct sum of finitely many copies of a simple R-module W. The following assertion is contained in [34, Lemma 7.4]

Lemma 4.3. *Let H be a group, F a field, V a vector space of finite positive dimension N over F. Let $\rho : H \to \mathrm{Aut}_F(V)$ be an irreducible linear representation of H. Let R be a H-normal subalgebra of $\mathrm{End}_F(V)$. Then:*

(i) *The faithful R-module V is semisimple.*
(ii) *Either the R-module V is isotypic or there is a subgroup H' of finite index r in H such that $r > 1$ and r divides N.*

Proposition 4.4. *Let F be a field, whose Brauer group $\mathrm{Br}(F) = \{0\}$. (E.g., F is either finite or an algebraically closed field.) Let V be a vector space of finite positive dimension N over F. Let H be a group and $\rho : H \to \mathrm{Aut}_F(V)$ a linear absolutely irreducible representation of H in V. Suppose that every maximal subgroup of H has index that does not divide N.*

Then the H-module V is central simple.

Proof. Slightly abusing the notation, we write F instead of $F \cdot \mathrm{Id}$.

Let R be a H-normal subalgebra of $\mathrm{End}_F(V)$. It follows from Lemma 4.3 that the faithful R-module V is *isotypic*, i.e., there is a simple faithful R-module W and a positive integer a such that the R-modules V and W^a are isomorphic. The existence of a faithful simple R-module implies that R is a simple F-algebra. In particular, the center k of R is a field. We have

$$F = F \cdot \mathrm{Id} \subset k \subset R \subset \mathrm{End}_F(V).$$

Then V carries the natural structure of a F-vector space. This implies that the degree $[k : F]$ divides $\dim_F(V) = N$.

The center k of H-normal R is also H-normal (see Remark 4.2(v)). This gives rise to the group homomorphism

$$H \to \mathrm{Aut}(k/F),\ \sigma \mapsto \{c \mapsto \rho(\sigma) u \rho(\sigma)^{-1}\}. \tag{12}$$

Here $\mathrm{Aut}(k/F)$ is the automorphism group of the field extension k/F. By Galois theory, the order of $\mathrm{Aut}(k/F)$ divides $[k : F]$, which in turn, divides N. This implies that the kernel of the homomorphism (12) is a subgroup of H, whose index divides N. Our condition on indices of subgroups of H implies that the kernel coincides with the whole H, i.e., the homomorphism (12) is trivial. This means that all elements of k commute with $\rho(\sigma)$ for all $\sigma \in H$. The absolute irreducibility of ρ implies that $k \subset F$ and therefore

$$k = F = F \cdot \mathrm{Id}.$$

So, R is a simple F-algebra with center $F \cdot \mathrm{Id}$, i.e., is a central simple F-algebra. This ends the proof. □

Theorem 4.5. *Let F be a field, whose Brauer group $\mathrm{Br}(F) = \{0\}$. (E.g., F is either finite or an algebraically closed field.) Let V be an F-vector space of finite dimension $N > 1$. Let G be a group and*

$$\rho : G \to \mathrm{Aut}_F(V)$$

be a group homomorphism. Let H be a normal subgroup of G that enjoys the following properties.

(i) *If H' is a subgroup of H of finite index N' and N' divides N then $H' = H$.*
(ii) *H is a simple non-abelian group. Assume additionally that either $H = G$, or H is the only proper normal subgroup of G.*
(iii) *The H-module V is absolutely simple, i.e., the representation of H in V is irreducible and the centralizer $\mathrm{End}_H(V) = F \cdot \mathrm{Id}$.*

Let $R \subset \mathrm{End}_F(V)$ be a G-normal subalgebra. Then there are positive integers a and b that enjoy the following properties.

(a) *$N = ab$;*
(b) *The F-algebra R is isomorphic to the matrix algebra $\mathrm{Mat}_a(F)$ of size a over F. In particular, the G-module V is central simple.*

(c) *The R-module V is semisimple, isotypic and isomorphic to R^b. In addition, the centralizer $\tilde{R} = \mathrm{End}_R(V)$ is a normal G-subalgebra that is isomorphic to the matrix algebra $\mathrm{Mat}_b(F)$ of size b over F.*

(d) *Suppose that $a \neq 1, b \neq 1$ (i.e., R is not obvious). Then both homomorphisms*

$$\mathrm{Ad}_R : G \to \mathrm{Aut}(R) = R^*/F^*\mathrm{Id} \cong \mathrm{GL}(a,F)/F^* = \mathrm{PGL}(a,F),$$

$$\mathrm{Ad}_R(\sigma)(u) = \rho(\sigma)u\rho(\sigma)^{-1} \ \forall u \in R$$

and

$$\mathrm{Ad}_{\tilde{R}} : G \to \mathrm{Aut}(\tilde{R}) = \tilde{R}^*/F^*\mathrm{Id} \cong \mathrm{GL}(b,F)/F^* = \mathrm{PGL}(b,F),$$

$$\mathrm{Ad}_{\tilde{R}}(\sigma)(u) = \rho(\sigma)u\rho(\sigma)^{-1} \ \forall u \in \tilde{R}$$

(with $\sigma \in G$) are injective. In addition,

$$\mathrm{Ad}_R(H) \subset \mathrm{PSL}(a,F), \ \mathrm{Ad}_{\tilde{R}}(H) \subset \mathrm{PSL}(b,F).$$

(e) *The H-module V is central simple.*

Proof. **Step 0**. Since H is a simple group, V is a faithful H-module. In light of (ii), V is a faithful G-module.

Clearly, V is a faithful R-module. Since R is G-normal,

$$\rho(\sigma)R\rho(\sigma)^{-1} = R \quad \forall \sigma \in G. \tag{13}$$

It follows from (ii) that

$$H = [H,H] \subset [G,G] \subset G$$

and either $G = H$ or G/H is a finite simple group (e.g., a cyclic group of prime order).

Step 1. By Lemma 4.3(i), V is a *semisimple* R-module.

Step 2. In light of Lemma 4.3(ii), property (i) implies that the R-module V is *isotypic*.

Step 3. Since the faithful R-module V is an isotypic, there exist a faithful simple R-module W and a positive integer b such that $V \cong W^b$. If we put $a = \dim_F(W)$ then we get

$$ba = b \cdot \dim_F(W) = \dim_F(V) = N.$$

Clearly, $\mathrm{End}_R(V)$ is isomorphic to the matrix algebra $\mathrm{Mat}_b(\mathrm{End}_R(W))$ of size b over $\mathrm{End}_R(W)$.

Consider the centralizer

$$k := \mathrm{End}_R(W)$$

of R in $\mathrm{End}_F(W)$. Since W is a simple R-module, k is a finite-dimensional division algebra over F. Since $\mathrm{Br}(F) = \{0\}$, k must be a field. Hence, the automorphism group $\mathrm{Aut}_F(k)$ of the F-algebra k is actually the automorphism group $\mathrm{Aut}(k/F)$ of the field extension k/F.

It follows that $\mathrm{Aut}_F(k) = \mathrm{Aut}(k/F)$ is finite and its order divides the degree $[k : F]$. We have

$$\tilde{R} = \mathrm{End}_R(V) \cong \mathrm{Mat}_b(k).$$

Clearly, the F-subalgebra $\tilde{R} = \mathrm{End}_R(V) \subset \mathrm{End}_F(V)$ is stable under the "adjoint action" of G, which gives rise to the group homomorphism

$$\mathrm{Ad}_{\tilde{R}} : G \to \mathrm{Aut}(\tilde{R}).$$

Since k is the center of $\mathrm{Mat}_b(k)$, it is stable under the action of G and of its subgroup H. This gives rise to the group homomorphism

$$H \to \mathrm{Aut}(k/F),\ h \mapsto \{\lambda \mapsto \rho(h)\lambda\rho(h)^{-1}\ \forall \lambda \in k\}\ \forall h \in H,$$

whose kernel H' has index $[H : H']$ dividing $[k : F]$. Since V carries the natural structure of a k-vector space, $[k : F]$ divides $\dim_F(V) = N$, the index $[H : H']$ divides N. In light of (i), $H' = H$, i.e., the homomorphism is trivial. This means that center k of $\mathrm{End}_R(V)$ commutes with $\rho(H)$. Since $\mathrm{End}_H(V) = F$, we have $k = F$. This implies that $\mathrm{End}_R(V) \cong \mathrm{Mat}_b(F)$ and

$$\mathrm{Ad}_{\tilde{R}} : G \to \mathrm{Aut}_F(\tilde{R}) = \tilde{R}^*/F^*\mathrm{Id} \cong \mathrm{GL}(b, F)/F^* = \mathrm{PGL}(b, F)$$

kills H if and only if $\tilde{R} = \mathrm{End}_R(V) \subset \mathrm{End}_H(V) = F \cdot \mathrm{Id}$. Since $\tilde{R} = \mathrm{End}_R(V) \cong \mathrm{Mat}_b(F)$, the homomorphism $\mathrm{Ad}_{\tilde{R}}$ kills H if and only if $b = 1$, i.e., V is an absolutely simple (faithful) R-module. This means that if $b > 1$ then $\mathrm{Ad}_{\tilde{R}}$ does *not* kill H, i.e., the normal subgroup $\ker(\mathrm{Ad}_{\tilde{R}})$ of G does *not* contain H. In light of (ii), this implies that the group homomorphism

$$\mathrm{Ad}_{\tilde{R}} : G \to \mathrm{Aut}(\tilde{R}) \cong \mathrm{PGL}(b, F)$$

is *injective* if $b > 1$.

Since V is a semisimple module over the subalgebra R of $\mathrm{End}_F(V)$ and $\tilde{R}$ is the centralizer of R in $\mathrm{End}_F(V)$, it follows from the Jacobson density theorem that

$$R = \mathrm{End}_{\tilde{R}}(V) \cong \mathrm{End}_F(W) \cong \mathrm{Mat}_a(F).$$

The "adjoint action" of G on R gives rise to the homomorphism

$$\mathrm{Ad}_R : G \to \mathrm{Aut}(R) = R^*/F^*\mathrm{Id} \cong \mathrm{PGL}(a, F).$$

Clearly, Ad_R kills H if and only if R commutes with $\rho(H)$, i.e., $R = F \cdot \mathrm{Id}$, which is equivalent to the equality $a = 1$. This means that if $a > 1$ then Ad_R does *not* kill H, i.e., the normal subgroup $\ker(\mathrm{Ad}_R)$ of G does *not* contain H. In light of (ii), this implies that the group homomorphism

$$\mathrm{Ad}_R : G \to \mathrm{Aut}(\tilde{R}) \cong \mathrm{PGL}(a, F)$$

is *injective* if $a > 1$.

To summarize: a normal G-subalgebra R is *not* obvious if and only if

$$a > 1, b > 1.$$

If this is the case then both group homomorphisms

$$\mathrm{Ad}_R : G \to \mathrm{PGL}(a, F),\ \mathrm{Ad}_{\tilde{R}} : G \to \mathrm{PGL}(b, F)$$

are *injective*.

The last assertions of Theorem 4.5(d) about the images of H follow from the equality $H = [H, H]$ and the inclusions

$$[\mathrm{GL}(a, F), \mathrm{GL}(a, F)] \subset \mathrm{SL}(a, F),\ [\mathrm{GL}(b, F), \mathrm{GL}(b, F)] \subset \mathrm{SL}(b, F).$$

The assertion (e) follows readily from the second assertion of (b) (if we replace G by H). This ends the proof. □

Corollary 4.6. *Keeping the assumption and notation of Theorem 4.5, assume additionally that $N = 2\ell$ where ℓ is a prime. If the H-module V is not very simple then there exist group embeddings*

$$G \hookrightarrow \mathrm{PGL}(2, F),\ H \hookrightarrow \mathrm{PSL}(2, F).$$

Proof. Let R be a H-normal non-obvious H-subalgebra and $\tilde{R} = \mathrm{End}_R(V)$. By Theorem 4.6, there are positive integers a and b such that

$$ab = N, a > 1, b > 1; R \cong \mathrm{Mat}_a(F), \tilde{R} \cong \mathrm{Mat}_b(F).$$

Our conditions on N imply that either $a = 2, b = \ell$ or $a = \ell, b = 2$. By Theorem 4.5, there are group embeddings

$$G \hookrightarrow \mathrm{PGL}(a, F),\ H \hookrightarrow \mathrm{PSL}(a, F)$$

and

$$G \hookrightarrow \mathrm{PGL}(b, F),\ H \hookrightarrow \mathrm{PSL}(b, F).$$

Since either a or b is 2, there are group embeddings

$$G \hookrightarrow \mathrm{PGL}(2, F),\ H \hookrightarrow \mathrm{PSL}(2, F).$$

□

Theorem 4.7. *Suppose that $n \geq 5$ is an integer, B is an n-element set, and p is a prime. Let us consider the vector space $\left(\mathbb{F}_p^B\right)^{00}$ over the field $\mathbb{F}_p$ endowed with the natural structure of a* $\mathrm{Perm}(B)$*-module (see Definition 3.2), and let*

$$\rho : \mathrm{Perm}(B) \to \mathrm{Aut}_{\mathbb{F}_p}\left(\left(\mathbb{F}_p^B\right)^{00}\right)$$

be the corresponding structure homomorphism.

Then:

(i) *The* $\mathrm{Perm}(B)$*-module $\left(\mathbb{F}_p^B\right)^{00}$ is very simple.*

(ii) *The* $\mathrm{Alt}(B)$*-module $\left(\mathbb{F}_p^B\right)^{00}$ is very simple if and only if either $n > 5$ or*

$$n = 5,\ p \not\equiv \pm 1 \mod 5.$$

(iii) *Suppose that*

$$n = 5,\ p \equiv \pm 1 \mod 5.$$

and $R \subset \mathrm{End}_{\mathbb{F}_p}(\left(\mathbb{F}_p^B\right)^{00})$ *is a* $\mathrm{Alt}(B)$*-normal subalgebra.*

Then either $R = \mathbb{F}_p \cdot \mathrm{Id}$*, or* $R = \mathrm{End}_{F_p}(\left(\mathbb{F}_p^B\right)^{00})$*, or the* $\mathbb{F}_p$*-algebra* R *is isomorphic to the matrix algebra* $\mathrm{Mat}_2(\mathbb{F}_p)$ *of size 2 over* $\mathbb{F}_p$*.*

(iv) *The* $\mathrm{Alt}(B)$*-module* $\left(\mathbb{F}_p^B\right)^{00}$ *is central simple*

Remark 4.8. The assertion of Theorem 4.7 was earlier proven in the following cases.

(A) $p \in \{2, 3\}$, see [34, Ex. 7.2] and [36, Cor. 4.3].
(B) $p > 3$ and $n \geq 8$, see [36, Cor. 4.6].
(C) $N = \dim_{\mathbb{F}_p}(\left(\mathbb{F}_p^B\right)^{00})$ is a prime. It follows readily from [36, Cor. 4.4(i)] applied to $H = \mathrm{Alt}(B)$ and $V = (\mathbb{F}_p^B)^{00}$. (We may apply this result from [36], because $\mathrm{Alt}(B)$ is a simple non-abelian group of order $n!/2$ and therefore its order is bigger that the order of $\mathbf{S}_N$, since $N \leq n - 1$.)

So, In the course of the proof we may assume that

$$p > 3;\ n \in \{5, 6, 7\}. \tag{14}$$

Proof of Theorem 4.7. We assume that (14) holds.

Step 1. First assume that $p \mid n$. Then either $n = p = 5$ or $n = p = 7$. In both cases

$$N = \dim_{\mathbb{F}_p}((\mathbb{F}_p^B)^{00}) = n - 2$$

is a prime. Now the very simplicity of the $\mathrm{Alt}(B)$-module $(\mathbb{F}_p^B)^{00}$ follows from Remark 4.8(A). So, we may assume that p does *not* divide n and therefore

$$N = n - 1.$$

Step 2. If $n = 6$ then $N = 5$ and the very simplicity of the $\mathrm{Alt}(B)$-module $(\mathbb{F}_p^B)^{00}$ follows from Remark 4.8(C). So, we may assume that

$$n \in \{5, 7\}.$$

Step 3. Suppose that $n = 7$. Then $N = 6 = 2 \times 3$ where 3 is a prime. It follows from Corollary 4.6 that if the $\mathrm{Alt}(B)$-module $(\mathbb{F}_p^B)^{00}$ is *not* very simple then there is a group homomorphism

$$\mathrm{Ad}_R : \mathrm{Alt}(B) \hookrightarrow \mathrm{PSL}(2, \mathbb{F}_p).$$

However, it is known [29, Th. 6.25 on p. 412 and Th. 626 on p. 414] that $\mathrm{PSL}(2, \mathbb{F}_p)$ does *not* contain a subgroup isomorphic to $\mathbf{A}_7$. Since $\mathrm{Alt}(B) \cong \mathbf{A}_7$, we get a contradiction, which implies that the $\mathrm{Alt}(B)$-module $(\mathbb{F}_p^B)^{00}$ is very simple if $n = 7$.

Step 4. Suppose that $n = 5$. We are going to apply Corollary 4.6 to $H = \mathrm{Alt}(B)$, $G = \mathrm{Perm}(B)$ or $\mathrm{Alt}(B)$, and $V = (\mathbb{F}_p^B)^{00}$.

Since p does *not* divide $n = 5$, we get $p > 5$, and $n - 1 = 4 = 2 \times 2$ where 2 is a prime.

- Suppose that the $\mathrm{Perm}(B)$-module $(\mathbb{F}_p^B)^{00}$ is *not* very simple. It follows from Corollary 4.6 (applied to $G = \mathrm{Perm}(B), H = \mathrm{Alt}(B)$) that there is a group embedding
$$\mathrm{Ad}_R : \mathrm{Perm}(B) \hookrightarrow \mathrm{PGL}(2, \mathbb{F}_p).$$
This implies that $\mathrm{PGL}(2, \mathbb{F}_p)$ contains a subgroup isomorphic to S_5, because $\mathrm{Perm}(B) \cong \mathbf{S}_5$. Since $p > 5$, the order 120 of $\mathbf{S}_5$ is *not* divisible by p. However, there are no finite subgroups of $\mathrm{PGL}(2, \mathbb{F}_p)$ that are isomorphic to $\mathbf{S}_5$ [29, Th. 6.25 on p. 412 and Th. 626 on p. 414]; see also [24, Sect. 2.5]. The obtained contradiction proves that the $\mathrm{Perm}(B)$-module $(\mathbb{F}_p^B)^{00}$ is very simple if $n = 5$.
- It follows from Corollary 4.6 (applied to $G = H = \mathrm{Alt}(B)$ and $V = (\mathbb{F}_p^B)^{00}$) that if the $\mathrm{Alt}(B)$-module $(\mathbb{F}_p^B)^{00}$ is *not* very simple then there is an injective group homomorphism
$$\mathrm{Ad}_R : \mathrm{Alt}(B) \hookrightarrow \mathrm{PSL}(2, \mathbb{F}_p).$$
Then the order 60 of the group $\mathrm{Alt}(B)$ divides the order $(p^2 - 1)p/2$ of the group $\mathrm{PSL}(2, \mathbb{F}_p)$. This implies that 5 divides $p^2 - 1 = (p + 1)(p - 1)$, i.e., $p \equiv \pm 1 \mod 5$. This implies that if $n = 5$ and $p \not\equiv \pm 1 \mod 5$ then $\mathrm{Alt}(B)$-module $(\mathbb{F}_p^B)^{00}$ is very simple.

Step 5. Suppose that $n = 5$ and $p \equiv \pm 1 \mod 5$. Let us prove that the $\mathrm{Alt}(B)$-module $(\mathbb{F}_p^B)^{00} = (\mathbb{F}_p^B)^0$ is *not* very simple. Recall (Remark 3.3) that there is a surjective homomorphism $\mathrm{SL}(2, \mathbb{F}_5) \twoheadrightarrow \mathbf{A}_5$, and there are $\mathrm{SL}(2, \mathbb{F}_5)$-modules $\bar{V}_1$ and $\bar{V}_2$ with
$$\dim_{\mathbb{F}_p}(\bar{V}_1) = \dim_{\mathbb{F}_p}(\bar{V}_2) = 2,$$
and an isomorphism of $\mathrm{SL}(2, \mathbb{F}_5)$-modules $(\mathbb{F}_p^B)^0 \cong \bar{V}_1 \otimes_{\mathbb{F}_p} \bar{V}_2$. This isomorphism induces an isomorphism of $\mathbb{F}_p$-algebras
$$\mathrm{End}_{\mathbb{F}_p}((\mathbb{F}_p^B)^0) = \mathrm{End}_{\mathbb{F}_p}(\bar{V}_1) \otimes_{\mathbb{F}_p} \mathrm{End}_{\mathbb{F}_p}(\bar{V}_2),$$
under which (the images of) the subalgebras
$$R = \mathrm{End}_{\mathbb{F}_p}(\bar{V}_1) \otimes 1, \ \tilde{R} = 1 \otimes \mathrm{End}_{\mathbb{F}_p}(\bar{V}_2)$$
are $\mathrm{Alt}(B)$-normal subalgebras of $\mathrm{End}_{\mathbb{F}_p}((\mathbb{F}_p^B)^0)$, see [38, Example 3.1(ii)]. In particular, the $\mathrm{Alt}(B)$-module $(\mathbb{F}_p^B)^{00} = (\mathbb{F}_p^B)^0$ is *not* very simple.

On the other hand, it follows from Theorem 4.5 that if R is a *non*-obvious $\mathrm{Alt}(B)$-normal subalgebra of $\mathrm{End}_{\mathbb{F}_p}((\mathbb{F}_p^B)^0)$ then $R \cong \mathrm{Mat}_a(\mathbb{F}_p)$ where a positive integer a is a *proper* divisor of
$$\dim_{\mathbb{F}_p}((\mathbb{F}_p^B)^0) = 4 = 2^2.$$
This implies that $a = 2$ and $R \cong \mathrm{Mat}_2(\mathbb{F}_p)$.

The assertion (iv) of Theorem 4.7 follows readily from already proven (ii) and (iii). □

Theorem 4.9. *Let $n \in \{11, 12, 22, 23, 24\}$. Let B be an n-element set B and $G \subset \mathrm{Perm}(B)$ the corresponding Mathieu group $\mathbf{M}_n$, which acts doubly transitively on B. Let p be an odd prime. If $n = 11$, then we assume additionally that $p > 3$.*

Then

- *the G-module $(\mathbb{F}_p^B)^{00}$ is central simple;*
- *if $n \neq p+1$ and $n-1$ is divisible by p, then the G-module $(\mathbb{F}_p^B)^{00}$ is very simple.*

Proof. It follows from ([13], [17, Table 1]) that the absolutely simple $G = \mathbf{M}_n$-module $(\mathbb{F}_p^B)^{00}$ is absolutely simple. By [1] the index of every maximal subgroup of $\mathbf{M}_n$ is at least

$$n > n - 1 \geq N = \dim_{\mathbb{F}_p}\left((\mathbb{F}_p^B)^{00}\right)$$

(recall that N is either $n - 1$ or $n - 2$).

In light of Proposition 4.4, the $G = \mathbf{M}_n$-module $(\mathbb{F}_p^B)^{00}$ is central simple. It remains to prove the very simplicity in the "exceptional" cases when $n \neq p + 1$ and $n - 1$ is divisible by p. We prove that in all the exceptional cases the $\mathbf{M}_n$-module $(\mathbb{F}_p^B)^{00}$ is *very* simple. After that the desired result will follow from Theorem 6.6.

- $n = 11$. Then $p = 5$ and $n - 1 = 2 \times 5$ where both 2 and 5 are primes. If the $\mathbf{M}_{11}$-module $(\mathbb{F}_5^B)^{00}$ is *not* very simple then it follows from Theorem 4.5(iii-d) that there is a group embedding $\mathbf{M}_{11} \hookrightarrow \mathrm{PSL}(2, \mathbb{F}_5)$, which is not true. Hence, the $\mathbf{M}_{11}$-module $(\mathbb{F}_5^B)^{00}$ is very simple.
- $n = 12$. Then $n - 1$ is a prime and there are no exceptional cases.
- $n = 22$. Then $n - 1 = 22 - 1 = 3 \cdot 7$ where both 3 and 7 are primes. Then $p = 3$ or 7. If the $\mathbf{M}_{22}$-module $(\mathbb{F}_3^B)^{00}$ is *not* very simple then it follows from Theorem 4.5(iii-d) that there is a group embedding $\mathbf{M}_{22} \hookrightarrow \mathrm{PSL}(3, \mathbb{F}_p)$. Such an embedding does not exist if $p = 3$, because the order of $\mathrm{PSL}(3, \mathbb{F}_3)$ is *not* divisible by 11 while 11 divides the order of $\mathbf{M}_{22}$. Hence, the $\mathbf{M}_{22}$-module $(\mathbb{F}_3^B)^{00}$ is very simple.

  Such an embedding does not exist if $p = 7$ as well, because the order of $\mathrm{PSL}(3, \mathbb{F}_7)$ is *not* divisible by 11, which divides the order of $\mathbf{M}_{22}$. Hence, the $\mathbf{M}_{22}$-module $(\mathbb{F}_7^B)^{00}$ is also very simple.
- $n = 23$. Then $n - 1 = 22 = 2 \cdot 11$ where both 2 and 11 are primes. Then $p = 11$. If the $\mathbf{M}_{23}$-module $(\mathbb{F}_{11}^B)^{00}$ is *not* very simple then it follows from Theorem 4.5(iii-d) that there is a group embedding $\mathbf{M}_{23} \hookrightarrow \mathrm{PSL}(2, \mathbb{F}_{11})$. Such an embedding does not exist. Hence, the $\mathbf{M}_{23}$-module $(\mathbb{F}_{11}^B)^{00}$ is very simple.

- $n = 24$. Then $n-1 = 23$ is a prime and there are no exceptional cases.

$\square$

Proposition 4.10. *Let G be a doubly transitive permutation subgroup of a n-element set B. Let $p > 3$ be a prime. Suppose that (n, G) enjoys one of the following properties.*

(1) *$n = 176$ and G is isomorphic to* HS*;*
(2) *$n = 276$ and G is isomorphic to* Co_3*.*

Then the G-module $(\mathbb{F}_p^B)^{00}$ is central simple.

Proof. It follows from [17, Tables] that in both cases the G-module $(\mathbb{F}_p^B)^{00}$ is absolutely simple.

Case 1. According to the Atlas [1], if H is a maximal subgroup of HS with index $[\mathrm{HS} : H] < 176$ then $[\mathrm{HS} : H] = 100$, which divides neither $176 - 1$ nor $176 - 2$. By Proposition 4.4, the G-module $(\mathbb{F}_p^B)^{00}$ is central simple.

Case 2. According to the Atlas [1], if H is a maximal subgroup subgroup of Co_3 then its index $m = [\mathrm{Co}_3 : H]$ is greater or equal than 276 [1]; in particular, it divides neither $276 - 1$ nor $276 - 2$. By Proposition 4.4, the G-module $(\mathbb{F}_p^B)^{00}$ is central simple as well. $\square$

Theorem 4.11. (i) *Let ℓ be a prime, $\mathfrak{r}$ a positive integer, and $n = \mathfrak{q} + 1$ where $\mathfrak{q} = \ell^{\mathfrak{r}} > 11$.*

(ii) *Let G be a subgroup of* $\mathrm{Perm}(B)$*. Suppose that G contains a subgroup H that is isomorphic to $\mathbf{L}_2(\mathfrak{q}) = \mathrm{PSL}(2, \mathbb{F}_{\mathfrak{q}})$ where $\mathbb{F}_{\mathfrak{q}}$ is a $\mathfrak{q}$-element field.*

If p is an odd prime then the G-module $(\mathbb{F}_p^B)^{00}$ is central simple.

Proof. It suffices to check that the $H \cong \mathbf{L}_2(q)$-module $(\mathbb{F}_p^B)^{00}$ is central simple. First, our conditions on q imply that each subgroup of $\mathbf{L}_2(\mathfrak{q})$ (except $\mathbf{L}_2(\mathfrak{q})$ itself) has index $\ge \mathfrak{q} + 1 = n$ [29, p. 414, (6.27)]. This implies that H acts transitively on the $(\mathfrak{q} + 1)$-element set B and the stabilizer H_b of any $b \in B$ has index $\mathfrak{q} + 1$. It follows from [29, Th. 6.25 on p. 412] that $H_b \subset \mathbf{L}_2(\mathfrak{q})$ is conjugate to the (Borel) subgroup of upper-triangular matrices modulo $\{\pm 1\}$. It follows that the $\mathbf{L}_2(\mathfrak{q})$-set B is isomorphic to the *projective line* $\mathbb{P}^1(\mathbb{F}_{\mathfrak{q}})$ with the standard fractional-linear action of $\mathbf{L}_2(\mathfrak{q})$, which is doubly transitive.

Notice that

$$q + 1 = n > N = \dim_{\mathbb{F}_p}\left((\mathbb{F}_p^B)^{00}\right),$$

because N is either $n - 1$ or $n - 2$. It follows that the index of any maximal subgroup of $\mathbf{L}_2(\mathfrak{q})$ does *not* divide N. On the other hand, according to [17, Table 1], the $H = \mathbf{L}_2(\mathfrak{q})$-module is absolutely simple. It follows now from Proposition 4.4 that the H-module V is central simple. $\square$

Theorem 4.12. *Let O be a Dedekind ring, T a locally free/projective O-module of finite positive rank r. Let E be the field of fractions of O, $\mathfrak{m}$ a maximal ideal in O and $k = O/\mathfrak{m}$ its residue field. Let us consider the r-dimensional E-vector space $T_E = T \otimes_O E$ and the r-dimensional k-vector space $T_k = T/\mathfrak{m}T = T \otimes_O k$.*

Let G be a group and $\rho : G \to \mathrm{Aut}_O(T)$ be a group homomorphism (O-linear representation). Let us consider the corresponding E-linear representation of G

$$\rho_E : G \to \mathrm{Aut}_E(T_E),\ \sigma \mapsto \{t \otimes e \mapsto \rho(\sigma)(t) \otimes e\ \forall t \in T, e \in E\}\ \forall \sigma \in G$$

and the corresponding k-linear representation of G

$$\rho_k : G \to \mathrm{Aut}_k(T_k),\ \sigma \mapsto \{t \otimes c \mapsto \rho(\sigma)(t) \otimes c\ \forall t \in T, c \in k\}\ \forall \sigma \in G.$$

If ρ_k is central simple (resp. very simple) then ρ_E is central simple (resp. very simple).

Proof. We view $T = T \otimes 1$ as a certain G-invariant lattice in $T \otimes_O E = T_E$ and $\mathrm{End}_O(T) = \mathrm{End}_O(T) \otimes 1$ as a certain G-invariant lattice (subalgebra) in $\mathrm{End}_O(T) \otimes_O E = \mathrm{End}_E(T_E)$.

Let R_E be a G-normal E-subalgebra of $\mathrm{End}_E(T_E)$. Let C_E be the center of R_E and J_E a *proper* ideal of R_E. We have

$$E \subset C,\ J \subset R_E,\ J \ne R_E.$$

Let us consider the O-subalgebra $R := R_E \cap \mathrm{End}_O(T)$. Clearly, R is a saturated O-submodule of $\mathrm{End}_O(T)$, i.e., the quotient $\mathrm{End}_O(T)/R$ is torsion free (finitely generated) O-module.

The natural map

$$R \otimes_O E \to R_E,\ u \otimes e \mapsto e \cdot u$$

is an isomorphism of E-algebras. This implies that:

(i) $C := C \cap \mathrm{End}_O(T)$ is the center of R that contains O as a saturated O-submodule, i.e., the quotient C/O is a torsion free (finitely generated) O-module. In addition, C is a saturated O-submodule of R, i.e., R/C is a torsion free finitely generated O-module.

(ii) The intersection $J := J_E \cap \mathrm{End}_O(T)$ is a *proper* ideal of R that is a saturated O-submodule of R, i.e., the quotient R/J is a torsion free (finitely generated) O-module.

Since the O-modules $\mathrm{End}_O(T)/R$, C/O, R/C and R/J finitely generated torsion free, they are *projective*, because the ring O is *Dedekind*. This implies that there are locally free submodules $R_1 \subset \mathrm{End}_O(T)$, $C_1 \subset C$, $D \subset R$, and $I \subset R$ such that

$$\mathrm{End}_O(T) = R \oplus R_1,\ C = O \oplus C_1,\ R = C \oplus D,\ I \oplus J = R. \quad (15)$$

Since J is a proper ideal, $I \ne 0$. Since C_1 and J are torsion-free finitely generated O-modules they are also locally free/projective. Now let us consider the $k = O/\mathfrak{m}$-subalgebra

$$R_k = R \otimes_O k \subset \mathrm{End}_O(T) \otimes_O k = \mathrm{End}_k(T_k)$$

where $T_k := T \otimes_O k$. Clearly,

(1) R_k is a G-normal subalgebra of $\mathrm{End}_k(T_k)$;
(2) $k \oplus (C_1 \otimes_O k)$ lies in the center of R_k.
(3) $R_k = (J \otimes_O k) \oplus (I \otimes_O k) \neq \{0\}$. This implies that $J_k = J \otimes_O k$ is a *proper* two-sided ideal of R_k, because $I \neq \{0\}$ and therefore $I \otimes_O k \neq \{0\}$.

Suppose that ρ_k is central simple. Then R_k is a simple k-algebra with center k. It follows that

$$C_1 \otimes_O k = \{0\},\ J_k = J \otimes_O k = \{0\}.$$

Since C_1 and J are locally free, we conclude that

$$C_1 = \{0\},\ J = \{0\},$$

which implies that

$$J_E = \{0\}, C = O \oplus C_1 = O \oplus \{0\} = O$$

and therefore $C_E = E$. This means that T_E is a central simple E-algebra, which proves that ρ_E is also central simple.

Assume now that ρ_k is very simple. Then either $R_k = k$ or $R_k = \mathrm{End}_k(T_k)$. In the latter case, applying (15), we get

$$\mathrm{End}_k(T_k) = (R \otimes_O k) \oplus (R_1 \otimes_O k) = R_k \oplus (R_1 \otimes_O k) = \mathrm{End}_k(T_k) \oplus (R_1 \otimes_O k).$$

Now k-dimension arguments imply that $R_1 \otimes_O k = \{0\}$ and therefore $R_1 = \{0\}$. This implies that $\mathrm{End}_O(T) = R \oplus R_1 = R$ and therefore $R_E = \mathrm{End}_E(T_E)$.

Assume now that $R_k = k$. It follows from (15) that

$$R = O \oplus (C_1 \oplus D)$$

and therefore

$$k = R \otimes_O k = k \oplus\ (C_1 \oplus D) \otimes_O k.$$

Again, k-dimension arguments imply that $(C_1 \oplus D) \otimes_O k = \{0\}$ and therefore $C_1 \oplus D = \{0\}$. It follows that $R = O$ and therefore $R_E = E$. This proves that ρ_E is semisimple. $\square$

5. Abelian varieties and cyclotomic fields

Let p be a prime, r a positive integer, and $q = p^r$. Let $E = \mathbb{Q}(\zeta_q)$ be the qth cyclotomic field and $O_E = \mathbb{Z}[\zeta_q]$ its ring of integers.

Let us put

$$\eta = \eta_q := 1 - \zeta_q \in \mathbb{Z}[\zeta_q].$$

It is well known [32] that the principal ideal $\eta_q\mathbb{Z}[\zeta_q]$ of $\mathbb{Z}[\zeta_q]$ is maximal and contains $p\mathbb{Z}[\zeta_q]$. Actually,

$$p\mathbb{Z}[\zeta_q] = \eta_q^{\phi(q)}\mathbb{Z}[\zeta_q].$$

It follows that there is $\eta' \in \mathbb{Z}[\zeta_q]$ such that

$$\eta'\mathbb{Z}[\zeta_q] = \eta_q^{\phi(q)-1}\mathbb{Z}[\zeta_q], \ \eta_q\eta' = \eta'\eta_q = p. \tag{16}$$

The residue field $\mathbb{Z}[\zeta_q]/\eta\mathbb{Z}[\zeta_q]$ coincides with $\mathbb{F}_p$. It is also well known [32] that

$$\mathbb{Z}_p[\zeta_q] = \mathbb{Z}[\zeta_q] \otimes \mathbb{Z}_p$$

is the ring of integers in the p-adic qth cyclotomic field $\mathbb{Q}_p(\zeta_q)$ and $\eta_q\mathbb{Z}_p[\zeta_q]$ is the maximal ideal of $\mathbb{Z}_p[\zeta_q]$ with residue field

$$\mathbb{Z}_p[\zeta_q]/\eta_q\mathbb{Z}_p[\zeta_q] = \mathbb{Z}[\zeta_q]/\eta_q\mathbb{Z}[\zeta_q] = \mathbb{F}_p.$$

Let K be a field of characteristic different from p. Let K_a be the algebraic closure of K and $K_s \subset K_a$ the separable algebraic closure of K. We write $\mathrm{Gal}(K)$ for the automorphism group $\mathrm{Aut}(K_a/K) = \mathrm{Gal}(K_s/K)$ of the corresponding field extension.

Let Z be an abelian variety of positive dimension g over K, and $\mathrm{End}_K(Z)$ (resp. $\mathrm{End}(Z)$) the ring of its K-endomorphisms (resp. the ring of all K_a-endomorphisms). By a theorem of Chow, all endomorphisms of Z are defined over K_s. In addition, $Z[p] \subset Z(K_s)$ where $Z[p]$ is the kernel of multiplication by p in $Z(K_a)$. If m is an integer then we write $m_Z \in \mathrm{End}_K(Z)$ for multiplication by m in Z.

Suppose that we are given the ring embedding

$$\mathbf{i} : O_E \hookrightarrow \mathrm{End}_K(Z) \subset \mathrm{End}(Z)$$

such that $1 \in O_E$ goes to the identity automorphism 1_Z of Z. In light of (16), $\mathbf{i}(\eta_q) : Z \to Z$ and $\mathbf{i}(\eta') : Z \to Z$ are isogenies and the kernel $\ker(\mathbf{i}(\eta_q))$ of $\mathbf{i}(\eta_q)$ lies in $Z[p]$. In addition,

$$\ker(\mathbf{i}(\eta_q)) = \mathbf{i}(\eta')(Z[p]) \subset Z[p]. \tag{17}$$

Indeed, since $\eta_q\eta' = p$, we have $\mathbf{i}(\eta_q)\mathbf{i}(\eta') = p_Z$ and

$$\mathbf{i}(\eta')(Z[p]) \subset \ker(\mathbf{i}(\eta_q)).$$

Conversely, suppose that $z \in \ker(\mathbf{i}(\eta_q))$. Since $\mathbf{i}(\eta')$ is an isogeny, it is surjective and therefore there is $\tilde{z} \in Z(K_a)$ such that $\mathbf{i}(\eta')(\tilde{z}) = z$. This implies that

$$0 = \mathbf{i}(\eta_q)(z) = \mathbf{i}(\eta_q)\mathbf{i}(\eta')\tilde{z} = p_Z\tilde{z} = p\tilde{z}.$$

It follows that $\tilde{z} \in Z[p]$ and therefore $\ker(\mathbf{i}(\eta_q)) \subset \mathbf{i}(\eta')(Z[p])$, which ends the proof of (17).

Let us put

$$\boldsymbol{\delta} := \mathbf{i}(\zeta_q) \in \mathrm{End}_K(Z) \subset \mathrm{End}(Z). \tag{18}$$

Remark 5.1. (i) Since $\eta_q = 1 - \zeta_q$, we get $\mathbf{i}(\eta_q)) = 1_Z - \boldsymbol{\delta}$ and therefore

$$\ker(\mathbf{i}(\eta_q)) = \{z \in Z(K_a) \mid \boldsymbol{\delta}(z) = z\} =: Z^{\boldsymbol{\delta}}. \tag{19}$$

(ii) Since $\ker(\mathbf{i}(\eta_q))$ is a subgroup of $Z[p]$, it carries the natural structure of a $\mathbb{F}_p$-vector space. In other words, $\ker(\mathbf{i}(\eta_q))$ is a $\mathbb{F}_p$-vector subspace of $Z[p]$.

(iii) Since the endomorphism $\mathbf{i}(\eta_q)$ is defined over K, $\ker(\mathbf{i}(\eta_q))$ is a $\mathrm{Gal}(K)$-invariant subspace of $Z[p]$. The action of $\mathrm{Gal}(K)$ on $\ker(\mathbf{i}(\eta))$ gives rise to the natural linear representation

$$\rho_\eta = \rho_{\eta,Z} : \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbb{F}_p}(\ker(\mathbf{i}(\eta_q))), \tag{20}$$

$$\sigma \mapsto \{z \mapsto \sigma(z)\ \forall z \in \ker(\mathbf{i}(\eta_q)) \subset Z[p] \subset Z(K_s)\}\ \forall \sigma \in \mathrm{Gal}(K).$$

Lemma 5.2. *$\phi(q) = [E : \mathbb{Q}]$ divides $2\dim(Z) = 2g$ and $\ker(\mathbf{i}(\eta_q))$ is a $\mathbb{F}_p$-vector space of dimension*

$$h_E := \frac{2\dim(Z)}{[E : \mathbb{Q}]} = \frac{2g}{\phi(q)}.$$

Proof. By a result of Ribet [19, Prop. 2.2.1 on p. 769], the $\mathbb{Z}_p$-*Tate module* $T_p(Z)$ of Z is a free module over the ring

$$\mathbb{Z}_p[\boldsymbol{\delta}] = \mathbf{i}(O_E) \otimes \mathbb{Z}_p \cong \mathbb{Z}[\zeta_q] \otimes \mathbb{Z}_p = \mathbb{Z}_p[\zeta_q]$$

of rank $h_E = 2g/\phi(q)$. (In particular, h_E is an integer.) This implies that the $\mathbb{Z}_p[\delta]$-module $Z[p] = T_p(Z)/pT_p(Z)$ is isomorphic to $(\mathbb{Z}_p[\boldsymbol{\delta}]/p)^{h_E}$. It follows from (17) that the $\mathbb{F}_p$-vector space

$$\ker(\mathbf{i}(\eta_q)) \cong (\eta' \mathbb{Z}_p[\zeta_q]/p)^{h_E} =$$

$$(\eta' \mathbb{Z}_p[\zeta_q]/\eta'\eta_q \mathbb{Z}_p[\zeta_q])^{h_E} = (\mathbb{Z}_p[\zeta_q]/\eta_q \mathbb{Z}_p[\zeta_q])^{h_E} = \mathbb{F}_p^{h_E}.$$

This proves that $\ker(\mathbf{i}(\eta_q))$ is a $\mathbb{F}_p$-vector space of dimension h_E. □

Let Λ be the centralizer of $\mathbf{i}(O_E)$ in $\mathrm{End}(Z)$. Clearly, $\mathbf{i}(O_E)$ lies in the center of Λ. It is also clear that

$$\Lambda(\ker \mathbf{i}(\eta_q)) \subset \ker(\mathbf{i}(\eta_q)),$$

which gives rise to the natural homomorphism of $O/\eta_q O = \mathbb{F}_p$-algebras

$$\kappa : \Lambda/\mathbf{i}(\eta_q)\Lambda \to \mathrm{End}_{\mathbb{F}_p}(\ker \mathbf{i}(\eta_q)),\ u + \mathbf{i}(\eta_q)\Lambda \mapsto \{z \mapsto u(z)\}\ \forall z \in \ker \mathbf{i}(\eta_q). \tag{21}$$

Proposition 5.3. *The homomorphism κ defined in (21) is injective.*

Proof. Suppose that $u \in \Lambda$ and $u(\ker \mathbf{i}(\eta_q)) = \{0\}$. We need to prove that $u \in \mathbf{i}(\eta_q)\Lambda$. In order to do that, notice that the endomorphism of Z

$$v := \mathbf{i}(\eta')\ u = u\ \mathbf{i}(\eta') \in \Lambda \subset \mathrm{End}(Z)$$

kills $Z[p]$, because

$$v(Z[p]) = u\ \mathbf{i}\,(\eta')(Z[p]) = u\ (\mathbf{i}\,(\eta')Z[p]) = u\big(\ker \mathbf{i}(\eta_q)\big) = \{0\}.$$

This implies that there is $\tilde{v} \in \mathrm{End}(Z)$ such that $v = p\tilde{v}$. Since v commutes with $\mathbf{i}(O_E)$, $\tilde{v}$ also commutes with $\mathbf{i}(O_E)$, i.e., $\tilde{v} \in \Lambda$. We have

$$\mathbf{i}(\eta')\mathbf{i}(\eta_q)\tilde{v} = p\tilde{v} = v = \mathbf{i}(\eta')u.$$

This implies that in $\mathrm{End}(Z)$

$$\mathbf{i}(\eta')\big(\mathbf{i}(\eta_q)\tilde{v}-u\big)=0.$$

Multiplying it by $\mathbf{i}(\eta_q)$ from the left and taking into account that $\mathbf{i}(\eta_q)\mathbf{i}(\eta')=\mathbf{i}(p)$, we get

$$p\big(\mathbf{i}(\eta_q)\tilde{v}-u\big)=0$$

in $\mathrm{End}(Z)$. It follows that $\mathbf{i}(\eta_q)\tilde{v}=u$. Since $\tilde{v}\in\Lambda$, we are done. □

Remark 5.4. (i) Since Z is defined over K, one may associate with every $u\in\mathrm{End}(Z)$ and $\sigma\in\mathrm{Gal}(K)$ an endomorphism ${}^{\sigma}u\in\mathrm{End}(Z)$ such that

$$ {}^{\sigma}u(z)=\sigma u(\sigma^{-1}z)\quad\forall z\in Z(K_a). \tag{22}$$

(ii) Recall that $\mathbf{i}(O_E)\subset\mathrm{End}_K(Z)$ consists of K-endomorphisms of Z. It follows that if $u\in\mathrm{End}(Z)$ commutes with $\mathbf{i}(O_E)$ then ${}^{\sigma}u$ commutes with $\mathbf{i}(O_E)$ for all $\sigma\in\mathrm{Gal}(K)$. In other words, if $u\in\Lambda$ then ${}^{\sigma}u\in\Lambda$ for all $\sigma\in\mathrm{Gal}(K)$.

(iii) Since $O_E=\mathbb{Z}[\zeta_q]$, we have $\mathbf{i}(O_E)=\mathbb{Z}[\boldsymbol{\delta}]$. It follows that Λ coincides with the centralizer of $\boldsymbol{\delta}$ in $\mathrm{End}(Z)$.

Proposition 5.5. *The image $R:=\kappa(\Lambda/\eta_q\Lambda)$ is a $\mathrm{Gal}(K)$-normal subalgebra of $\mathrm{End}_{\mathbb{F}_p}(\ker\mathbf{i}(\eta_q))$.*

Proof. Let $u\in\Lambda$. Then

$$\bar{u}:=\kappa(u+\eta_q\Lambda)\in R\subset\mathrm{End}_{\mathbb{F}_p}(\ker\mathbf{i}(\eta_q)),$$

$$\bar{u}:z\mapsto u(z)\ \forall z\in\ker\mathbf{i}(\eta_q).$$

Then ${}^{\sigma}u\in\Lambda$ for all $\sigma\in\mathrm{Gal}(K)$ and

$$\overline{{}^{\sigma}u}=\kappa({}^{\sigma}u+\eta_q\Lambda)\in\mathrm{End}_{\mathbb{F}_p}(\ker\mathbf{i}(\eta_q)),$$

$$\overline{{}^{\sigma}u}:z\mapsto\sigma u\sigma^{-1}(z)=\rho_\eta(\sigma)u\rho_\eta(\sigma)^{-1}(z)=\rho_\eta(\sigma)\bar{u}\rho_\eta(\sigma)^{-1}(z).$$

In other words, for each $\bar{u}\in R$

$$\rho_\eta(\sigma)\bar{u}\rho_\eta(\sigma)^{-1}\in R\ \forall\sigma\in\mathrm{Gal}(K).$$

This proves that R is $\mathrm{Gal}(K)$-normal. □

Remark 5.6. (i) Extending $\mathbf{i}$ by $\mathbb{Q}$-linearity, we get a $\mathbb{Q}$-algebra embedding

$$E=O_E\otimes\mathbb{Q}\to\mathrm{End}(Z)\otimes\mathbb{Q}=:\mathrm{End}^0(Z),\ u\otimes c\mapsto cu\ \forall u\in O,c\in\mathbb{Q}$$

that we continue to denote by $\mathbf{i}$. Clearly, $\mathbf{i}(E)$ coincides with the $\mathbb{Q}$-subalgebra $\mathbb{Q}[\boldsymbol{\delta}]$ of $\mathrm{End}^0(Z)$ generated by δ_q. Clearly, $\mathbf{i}:E\to\mathbb{Q}[\boldsymbol{\delta}]$ is a field isomorphism of number fields, and $\mathbf{i}(O_E)$ is the ring of integers in the number field $\mathbb{Q}[\delta]$.

(ii) Let us consider the $\mathbb{Q}$-subalgebra

$$\mathcal{H} = \Lambda \otimes \mathbb{Q} \subset \mathrm{End}(Z) \otimes \mathbb{Q} = \mathrm{End}^0(Z).$$

Then the center of $\mathcal{H}$ contains $\mathbf{i}(O) \otimes \mathbb{Q} = \mathbb{Q}[\boldsymbol{\delta}]$. In other words, $\mathcal{H}$ is a $\mathbb{Q}[\boldsymbol{\delta}]$-algebra of finite dimension.

(iii) We have

$$\Lambda = \mathcal{H} \cap \mathrm{End}(Z). \tag{23}$$

where the intersection is taken in $\mathrm{End}^0(Z)$. (Here we identify $\mathrm{End}(Z)$ with $\mathrm{End}(Z) \otimes 1$ in $\mathrm{End}^0(Z)$.) Indeed, the inclusion $\Lambda \subset \mathcal{H} \cap \mathrm{End}(Z)$ is obvious. Conversely, suppose that $u \in \mathcal{H} \cap \mathrm{End}(Z)$. Then $u \in \mathrm{End}(Z)$ and $mu \in \Lambda$ for some positive integer m. This means that

$$(mu)\boldsymbol{\delta} = \boldsymbol{\delta}(mu),$$

which means that $m(u\boldsymbol{\delta} - \boldsymbol{\delta}u) = 0$ in $\mathrm{End}(Z)$. It follows that $u\boldsymbol{\delta} - \boldsymbol{\delta}u = 0$, i.e., $u \in \Lambda$. It follows that $\mathcal{H} \cap \mathrm{End}(Z) \subset \Lambda$, which ends the proof of (23).

Proposition 5.7. (i) *If the* $\mathrm{Gal}(K)$*-module* $\ker \mathbf{i}(\eta_q)$ *is central simple then* $\mathcal{H}$ *is a central simple* $\mathbb{Q}[\boldsymbol{\delta}]$*-algebra.*

(ii) *If the* $\mathrm{Gal}(K)$*-module* $\ker \mathbf{i}(\eta_q)$ *is very simple then either*

$$\mathcal{H} = \Lambda \otimes \mathbb{Q} = \mathbf{i}(E) = \mathbb{Q}[\boldsymbol{\delta}], \;\; \Lambda = \mathbf{i}(O_E) = \mathbb{Z}[\boldsymbol{\delta}]$$

or $\mathcal{H} = \Lambda \otimes \mathbb{Q}$ *is a central simple* $\mathbb{Q}[\boldsymbol{\delta}]$*-algebra, whose dimension is the square of* $2\mathrm{dim}(Z)/[E : \mathbb{Q}] = 2g/\phi(q)$.

Proof. (i) The central simplicity implies that the $\mathrm{Gal}(K)$-normal subalgebra

$$R = \kappa(\Lambda/\eta\Lambda) \cong \Lambda/\eta\Lambda$$

is a central simple $\mathbb{F}_p$-algebra and therefore is isomorphic to the matrix algebra $\mathrm{Mat}_d(\mathbb{F}_p)$ of a certain size d. Applying Lemma 2.3 to $O = \mathbf{i}(O_E)$, the maximal ideal $\mathfrak{m} = \mathbf{i}(\eta_q O_E)$ and the residue field $k = \mathbb{F}_p$, we conclude that $\mathcal{H}$ is a central simple $\mathbb{Q}[\delta_q]$-algebra.

(ii) The very simplicity implies that either $\Lambda/\eta_q\Lambda = \mathbb{F}_p$ or

$$\Lambda/\eta\Lambda \cong \mathrm{End}_{\mathbb{F}_p}(\ker \mathbf{i}(\eta_q)) \cong \mathrm{Mat}_{h_E}(\mathbb{F}_p).$$

In the latter case, Lemma 2.3 tells us that $\mathcal{H}$ is a central simple $\mathbb{Q}[\boldsymbol{\delta}]$-algebra of dimension h_E^2.

In the former case, Lemma 2.3 tells us that $\mathcal{H}$ is a central simple $\mathbb{Q}[\boldsymbol{\delta}]$-algebra of dimension 1, i.e., $\mathcal{H} = \mathbb{Q}[\boldsymbol{\delta}]$. Hence,

$$\mathbb{Z}[\boldsymbol{\delta}] \subset \Lambda \subset \mathbb{Q}[\boldsymbol{\delta}].$$

Since $\mathbb{Z}[\boldsymbol{\delta}] \cong \mathbb{Z}[\zeta_q]$ is integrally closed and Λ is a free $\mathbb{Z}$-module of finite rank, $\mathbb{Z}[\boldsymbol{\delta}] = \Lambda$.

□

6. Cyclic covers and Jacobians

Hereafter we fix an odd prime p.

Let us assume that K is a subfield of $\mathbb{C}$. We write K_a for the algebraic closure of K in $\mathbb{C}$ and write $\mathrm{Gal}(K)$ for the absolute Galois group $\mathrm{Aut}(K_a/K)$. We also fix in K_a a primitive pth root of unity $\zeta = \zeta_p$.

Let $f(x) \in K[x]$ be a separable polynomial of degree $n \ge 4$. We write $\mathfrak{R}_f$ for the n-element set of its roots and denote by $L = L_f = K(\mathfrak{R}_f) \subset K_a$ the corresponding splitting field of $f(x)$. As usual, the Galois group $\mathrm{Gal}(L/K)$ is called the Galois group of f and denoted by $\mathrm{Gal}(f)$. Clearly, $\mathrm{Gal}(f)$ permutes elements of $\mathfrak{R}_f$ and the natural map of $\mathrm{Gal}(f)$ into the group $\mathrm{Perm}(\mathfrak{R}_f)$ of all permutations of $\mathfrak{R}_f$ is an embedding. We will identify $\mathrm{Gal}(f)$ with its image and consider it as the certain permutation group of $\mathfrak{R}_f$. Clearly, $\mathrm{Gal}(f)$ is transitive if and only if f is irreducible in $K[x]$. Therefore the $\mathrm{Gal}(f)$-module $(\mathbb{F}_p^{\mathfrak{R}_f})^{00}$ is defined. The canonical surjection

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

provides $(\mathbb{F}_p^{\mathfrak{R}_f})^{00}$ with the canonical structure of the $\mathrm{Gal}(K)$-module via the composition

$$\mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(f) \subset \mathrm{Perm}(\mathfrak{R}_f) \subset \mathrm{Aut}((\mathbb{F}_p^{\mathfrak{R}_f})^{00}).$$

Let us put

$$V_{f,p} := (\mathbb{F}_p^{\mathfrak{R}_f})^{00}. \tag{24}$$

Let $C = C_{f,p}$ be the smooth projective model of the smooth affine K-curve

$$y^p = f(x).$$

The genus

$$g = g(C) = g(C_{f,p})$$

of C is $(p-1)(n-1)/2$ if p does *not* divide p and $(p-1)(n-2)/2$ if it does ([16], pp. 401–402, [30], Prop. 1 on p. 3359, [21], p. 148).

Assume that K contains ζ. There is a non-trivial biregular automorphism of C

$$\delta_p : (x, y) \mapsto (x, \zeta y).$$

Clearly, δ_p^p is the identity selfmap of C.

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 δ_p as an element of

$$\mathrm{Aut}(C) \subset \mathrm{Aut}(J(C)) \subset \mathrm{End}(J(C))$$

such that

$$\delta_p \ne \mathrm{Id}, \quad \delta_p^p = \mathrm{Id}$$

where Id is the identity endomorphism of $J(C)$. Here $\mathrm{End}(J(C))$ stands for the ring of all K_a-endomorphisms of $J(C)$. As usual, we write

$\mathrm{End}^0(J(C)) = \mathrm{End}^0(J^{(f,p)})$ for the corresponding $\mathbb{Q}$-algebra $\mathrm{End}(J(C)) \otimes \mathbb{Q}$.

Recall (4) that there is a ring embedding

$$\mathbf{i}_{p,f} : \mathbb{Z}[\zeta_p] \cong \mathbb{Z}[\delta_p] \subset \mathrm{End}(J^{(f,p)}), \ \zeta_p \mapsto \delta_p.$$

Let us put

$$J^{(f,p)}(\eta_p) =: \ker(\mathbf{i}_{p,f}(\eta_p)) \subset J^{(f,p)}(K_a) \tag{25}$$

where $\eta_p = 1 - \zeta_p \in \mathbb{Z}[\delta_p]$ (Section 5).

Remark 6.1. Let

$$\Lambda := \mathrm{End}_{\delta_p}(J^{(f,p)})$$

be the centralizer of δ_p in $\mathrm{End}(J^{(f,p)})$. Clearly,

$$\mathcal{H} := \Lambda \otimes \mathbb{Q} \subset \mathrm{End}(J^{(f,p)}) \otimes \mathbb{Q} \subset \mathrm{End}^0(J^{(f,p)})$$

is the centralizer of $\mathbb{Q}[\delta_p]$ in $\mathrm{End}^0(J^{(f,p)})$.

Theorem 6.2 (Prop. 6.2 in [21], Prop. 3.2 in [23])**.** *There is a canonical isomorphism of the* $\mathrm{Gal}(K)$*-modules*

$$J^{(f,p)}(\eta_p) \cong V_{f,p}.$$

Remark 6.3. Clearly, the natural homomorphism $\mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbb{F}_p}(V_{f,p})$ coincides with the composition

$$\mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(f) \subset \mathrm{Perm}(\mathfrak{R}_f) \subset \mathrm{Aut}\left((\mathbb{F}_p^{\mathfrak{R}_f})^{00}\right) = \mathrm{Aut}_{\mathbb{F}_p}(V_{f,p}).$$

Corollary 6.4.
(i) *If the* $\mathrm{Gal}(f)$*-module* $V_{f,p}$ *is central simple then the* $\mathrm{Gal}(K)$*-module* $J^{(f,p)}(\eta_p)$ *is central simple and* $\mathcal{H} = \Lambda \otimes \mathbb{Q}$ *is a central simple* $\mathbb{Q}[\delta_p]$*-algebra.*
(ii) *If the* $\mathrm{Gal}(f)$*-module* $V_{f,p}$ *is very simple then the* $\mathrm{Gal}(K)$*-module* $J^{(f,p)}(\eta_p)$ *is very simple and either* $\Lambda = \mathbf{i}(O)$ *or* $\mathcal{H} = \Lambda \otimes \mathbb{Q}$ *is a central simple* $\mathbb{Q}[\delta_p]$*-algebra, whose dimension is the square of* $2\mathrm{dim}(J^{(f,p)})/(p-1)$*.*

Proof. It follows from Remark 4.2(ii) combined with Theorem 6.2 that if the $\mathrm{Gal}(f)$-module $V_{f,p}$ is central simple (resp. very simple) then the $\mathrm{Gal}(K)$-module $J^{(f,p)}(\eta_p)$ (defined in (25)) is central simple (resp. very simple). Now the desired result follows readily from Proposition 5.7 applied to $Z = J^{(f,p)}$, $q = p$, and $\mathbf{i} = \mathbf{i}_{p,f}$. □

The following assertion was proven in [37, Th. 3.6].

Theorem 6.5. *Suppose that* $n \geq 4$*. Assume that* $\mathbb{Q}[\delta_p]$ *is a maximal commutative subalgebra of* $\mathrm{End}^0(J^{(f,p)})$*.*

Then $\mathrm{End}^0(J^{(f,p)}) = \mathbb{Q}[\delta_p] \cong \mathbb{Q}(\zeta_p)$ *and therefore* $\mathrm{End}(J^{(f,p)}) = \mathbb{Z}[\delta_p] \cong \mathbb{Z}[\zeta_p]$*.*

Theorem 6.6. *Let* p *be an odd prime and* $\zeta \in K$*. Suppose that the* $\mathrm{Gal}(f)$*-module* $(\mathbb{F}_p^{\mathfrak{R}_f})^{00}$ *enjoys one of the following properties.*

(i) *The* $\mathrm{Gal}(f)$*-module* $V_{f,p} = (\mathbb{F}_p^{\mathfrak{R}_f})^{00}$ *is very simple.*

(ii) *The* $\mathrm{Gal}(f)$*-module* $V_{f,p} = (\mathbb{F}_p^{\mathfrak{R}_f})^{00}$ *is central simple. In addition, either* $n = p+1$*, or* $n-1$ *is not divisible by* p*.*

Then $\mathrm{End}^0(J^{(f,p)}) = \mathbb{Q}[\delta_p]$ *and* $\mathrm{End}(J^{(f,p)}) = \mathbb{Z}[\delta_p]$.

Proof of Theorem 6.6. In light of Theorem 6.5, it suffices to check that $\mathbb{Q}[\delta_p]$ coincides with its own centralizer in $\mathrm{End}^0(J^{(f,p)})$. Recall that $J^{(f,p)}$ is a g-dimensional abelian variety defined over K.

The properties of the $\mathrm{Gal}(f)$-module $(\mathbb{F}_p^{\mathfrak{R}_f})^{00}$ and the integers n, p imply (thanks to Remark 4.2(ii)) that either the $\mathrm{Gal}(K)$-module $J^{(f,p)}(\eta_p)$ is very simple, or the following conditions hold.

(a) The $\mathrm{Gal}(K)$-module $J^{(f,p)}(\eta_p)$ is central simple.

(b) Either $n = p+1$, or $n-1$ is not divisible by p.

In all the cases the normal $\mathbb{F}_p$-subalgebra $R \cong \Lambda/\eta_p\Lambda$ is isomorphic to the matrix algebra $\mathrm{Mat}_d(\mathbb{F}_p)$ for some positive integer d.

Applying Corollary 5.7, we conclude that $\mathcal{H} = \Lambda_{\mathbb{Q}} = \Lambda \otimes \mathbb{Q}$ is a central simple $\mathbb{Q}[\delta_p]$-algebra of dimension d^2 for some positive integer d. In addition, if the $\mathrm{Gal}(K)$-module $J^{(f,p)}(\eta_p)$ is very simple, then either

$$d = 1,\ \mathcal{H} = \mathbb{Q}[\delta_p], \Lambda = \mathbb{Z}[\delta_p]$$

or

$$d = 2g/(p-1).$$

According to Remark 2.2(vi), $d \neq 2g/(p-1)$. So, in the very simple case $\mathcal{H} = \mathbb{Q}[\delta_p], \Lambda = \mathbb{Z}[\delta_p]$.

Now suppose that $J^{(f,p)}(\eta_p)$ is *not* very simple. Then either $n = p+1$ or $n-1$ is not divisible by p. It follows from Remark 2.2(iv) that $d = 1$. This implies that $H = \mathbb{Q}[\delta_p]$. Therefore

$$\mathbb{Z}[\delta_p] \subset \Lambda \subset \mathbb{Q}[\delta_p].$$

This implies that $\Lambda = \mathbb{Z}[\delta_p]$ and therefore the centralizer of $\mathbb{Q}[\delta_p]$ in $\mathrm{End}^0(J^{(f,p)})$ coincides with $\Lambda \otimes \mathbb{Q} = \mathbb{Q}[\delta_p]$.

□

Theorem 6.7. *Let* $n \geq 5$ *be an integer,* p *an odd prime, and* K *contains a primitive* p*th root of unity. Let us put* $N := n-1$ *if* p *does not divide* n *and* $N := n-2$ *if* $p \mid n$*. Suppose that the Galois group* $\mathrm{Gal}(f)$ *of* $f(x)$ *contains a subgroup* H *such that the representation of* H *in* $(\mathbb{F}_p^{\mathfrak{R}_f})^{00}$ *is absolutely irreducible. Assume additionally that*

(i) *the index of every maximal subgroup of* H *does not divide* N*.*

(ii) *Either* $n = p+1$*, or* $n-1$ *is not divisible by* p*.*

Then $\mathrm{End}^0(J^{(f,p)}) = \mathbb{Q}[\delta_p]$ *and* $\mathrm{End}(J^{(f,p)}) = \mathbb{Z}[\delta_p]$.

Proof of Theorem 6.7. Enlarging K if necessary, we may and will assume that $H = \mathrm{Gal}(f)$. It follows from Proposition 4.4 that the absolutely simple H-module $(\mathbb{F}_p^{\mathfrak{R}_f})^{00}$ is central simple. Applying Theorem 6.6, we conclude that $\mathrm{End}^0(J^{(f,p)}) = \mathbb{Q}[\delta_p]$ and $\mathrm{End}(J^{(f,p)}) = \mathbb{Z}[\delta_p]$. □

Remark 6.8. See [5, Sect. 7.7] and [17] for the list of doubly transitive permutation groups $H \subset \mathrm{Perm}(B)$ and primes p such that the H-module $(\mathbb{F}_p^B)^{00}$ is (absolutely) simple. (See also [22, Sect. 4], [4, Main Theorem] and [15].)

7. Jacobians of cyclic covers of prime degree p

Proof of Theorem 1.2. Enlarging K if necessary, we may and will assume that

$$H = \mathrm{Gal}(f) \subset \mathrm{Perm}(\mathfrak{R}_f).$$

Since $p > n$, the prime p divides neither n nor $n-1$. In particular,

$$(\mathbb{F}_p^{\mathfrak{R}_f})^{00} = (\mathbb{F}_p^{\mathfrak{R}_f})^{0}.$$

In light of Remark 3.1 applied to $B = \mathfrak{R}_f$ and $G = H$, the double transitivity of H implies that the H-module $(\mathbb{F}_p^{\mathfrak{R}_f})^0$ is absolutely simple. Now the desired result follows readily from Theorem 6.7. □

Proof of Theorem 1.3. Assume that $n \ge 5$ and $\mathrm{Gal}(f) = \mathrm{Perm}(\mathfrak{R}_f)$ or $\mathrm{Alt}(\mathfrak{R}_f)$. Enlarging K if necessary, we may assume that $\mathrm{Gal}(f) = \mathrm{Alt}(\mathfrak{R}_f)$. Taking into account that $\mathrm{Alt}(\mathfrak{R}_f)$ is non-abelian simple while the field extension $K(\zeta)/K$ is abelian, we conclude that the Galois group of f over $K(\zeta)$ is also $\mathrm{Alt}(\mathfrak{R}_f)$. (In particular, $f(x)$ remains irreducible over $K(\zeta)$.) So, in the course of the proof of Theorem 1.3, we may assume that $\zeta \in K$ and $\mathrm{Gal}(f) = \mathrm{Alt}(\mathfrak{R}_f)$.

It is well known that the index of every maximal subgroup of $\mathrm{Alt}(\mathfrak{R}_f) \cong \mathbf{A}_n$ is at least n; notice that

$$n > N = \dim_{\mathbb{F}_p}(V_{f,p}) = \dim_{\mathbb{F}_p}\left((\mathbb{F}_p^B)^{00}\right).$$

(Recall that $N = n-1$ or $n-2$.) By Theorem 4.7(iv), the $\mathrm{Gal}(f)$-module $V_{f,p} = (\mathbb{F}_p^B)^{00}$ is *central simple*. It is *very simple* if either $n > 5$ or $p \le 5$, thanks to Theorem 4.7(ii). On the other hand, if $n = 5$ and $p > 5$ then $n-1$ is *not* divisible by p. Now the desired result follows readily from Theorem 6.6.

□

Proof of Theorem 1.6. Since $\mathbf{M}_n$, HS and Co_3 are simple nonabelian groups, replacing K by $K(\zeta)$, we may and will assume that $\zeta \in K$. Now the desired result follows readily from Theorem 6.7 combined with Theorem 4.9 and Proposition 4.10.

□

Proof of Theorem 1.8. Enlarging K, we may assume that $\mathrm{Gal}(f) = H \cong \mathfrak{G}(\mathfrak{q})$. Since $\mathfrak{G}(\mathfrak{q})$ is a simple nonabelian group, replacing K by $K(\zeta)$, we may and will assume that $\zeta \in K$. In light of [17, Table 1], our conditions on H and p imply that the H-module $V_{f,p}$ is *absolutely simple*.

Case L2. It follows from Theorem 4.11 that the $\mathrm{Gal}(f)$-module $(\mathbb{F}_p^{\mathfrak{R}_f})^{00} = V_{f,p}$ is central simple.

On the other hand, if $n-1$ is divisible by p then $p = \ell$, because $n-1 = (\mathfrak{q}+1)-1 = \mathfrak{q}$ which is a power of the prime number ℓ. Hence, our assumptions imply that $n = \mathfrak{q}+1 = p+1$. So, either $n-1$ is *not* divisible by p or $n = p+1$. Now we may apply Theorem 6.6, which gives us $\mathrm{End}^0(J^{(f,p)}) = \mathbb{Q}[\delta_p]$ and $\mathrm{End}(J^{(f,p)}) = \mathbb{Z}[\delta_p]$.

Case Lmq. It follows from a result of Guralnick and Tiep [9, Th. 1.1] that every nontrivial projective representation of $\mathrm{Gal}(f) = H = \mathrm{L}_m(\mathfrak{q})$ in characteristic p has dimension $\ge \dim_{\mathbb{F}_p}(V_{f,p})$. In light of [35, Cor. 5.4], the $\mathrm{Gal}(f)$-module $V_{f,p}$ is very simple. Now the desired result follows readily from Theorem 6.7.

Case U3. It follows readily from the Mitchell's list of maximal subgroups of $\mathrm{U}_3(\mathfrak{q})$ ([10, p. 212-213], [8, Th. 6.5.3 and its proof, pp. 329-332] that the index of every maximal subgroup of $\mathrm{U}_3(\mathfrak{q})$ is greater or equal than

$$\mathfrak{q}^3 + 1 = n > N$$

where $N = \dim_{\mathbb{F}_p}(V_{f,p})$ is either $n-1 = \mathfrak{q}^3$ or $n-2 = \mathfrak{q}^3 - 1$. On the other hand, $n-1 = \mathfrak{q}^3$ is a power of the prime ℓ and therefore is *not* divisible by the prime p, since $\ell \ne p$. Now the desired result follows readily from Theorem 6.7.

Case Sz. It follows from the classification of subgroups of $\mathrm{Sz}(\mathfrak{q})$ [11, Remark 3.12(e) on p. 194] that every maximal subgroup of $\mathrm{Sz}(\mathfrak{q})$ has index $\ge \mathfrak{q}^2 + 1 = n$. Since $n-1 = \mathfrak{q}^2$ is a power of 2, the odd prime p does *not* divide $n-1$. Now the desired result follows readily from Theorem 6.7.

Case Ree. Our conditions on p imply that $p \ne 3$. Since $n-1 = \mathfrak{q}^2$ is a power of 3, the prime p does *not* divide $n-1$. It follows from the classification of subgroups of $\mathrm{Ree}(\mathfrak{q})$ [14, Th. C] that every maximal subgroup of $\mathrm{Sz}(\mathfrak{q})$ has index $\ge \mathfrak{q}^3 + 1 = n$. (See also [6, Remark 5.4].) Now the desired result follows readily from Theorem 6.7. □

8. Jacobians of cyclic covers of degree q

In this section we discuss the case when $q = p^r > 2$ where r is any positive integer, K is a subfield of $\mathbb{C}$ and $f(x) \in K[x]$ a degree n polynomial without repeated roots. We assume that $n \ge 5$ and either $q \mid n$ or p does *not* divide n. Let $J(C_{f,q})$ be the Jacobian of the curve $C_{f,q}$ and δ_q the automorphism of $J(C_{f,q})$, whicch are defined in the beginning of Section 1.

Remark 8.1. One may define a positive-dimensional abelian subvariety

$$J^{(f,q)} := \mathcal{P}_{q/p}(\delta_q)(J(C_{f,q}))$$

of $J(C_{f,q})$ [34, p. 355] that is defined over $K(\zeta_q)$ and enjoys the following properties [34] (see also [39]).

(i) If $q = p$ then $J^{(f,p)} = J(C_{f,p})$ (as above).

(ii) $J^{(f,q)}$ is defined over $K(\zeta_q)$.

(iii) $J^{(f,q)}$ is a δ_q-invariant abelian subvariety of $J(C_{f,q})$. In addition $\Phi_q(\delta_q)(J^{(f,q)}) = 0$ where

$$\Phi_q(t) = \sum_{i=0}^{p-1} t^{ip^{r-1}} \in \mathbb{Z}[t]$$

is the qth cyclotomic polynomial. This gives rise to the ring embedding

$$\mathbf{j}_{q,f} : \mathbb{Z}[\zeta_q] \hookrightarrow \mathrm{End}(J^{(f,q)})$$

under which ζ_q goes to to the restriction of δ_q to $J^{(f,q)}$, which we denote by $\boldsymbol{\delta}_q \in \mathrm{End}(J^{(f,q)})$. Then the subring $\mathbb{Z}[\boldsymbol{\delta}_q]$ of $\mathrm{End}(J^{(f,q)})$ is isomorphic to $\mathbb{Z}[\zeta_q]$ (via $\mathbf{j}_{q,f}$), and the $\mathbb{Q}$-subalgebra $\mathbb{Q}[\boldsymbol{\delta}_q]$ of $\mathrm{End}^0(J^{(f,q)})$ is isomorphic to $\mathbb{Q}(\zeta_q)$.

(iv) If p does *not* divide n then there is an isogeny of abelian varieties

$$J(C_{f,q}) \to J(C_{f,q/p}) \times J^{(f,q)}$$

that is defined over $K(\zeta_q)$. (Notice that $q/p = p^{r-1}$, so $J(C_{f,q/p}) = J(C_{f,p^{r-1}})$.) By induction, this gives us an isogeny of abelian varieties

$$J(C_{f,q}) \to J(C_{f,p}) \times \prod_{i=2}^{r} J^{(f,r^i)} = \prod_{i=1}^{r} J^{(f,r^i)}$$

that is also defined over $K(\zeta_q)$ [34, Cor. 4.12].

(v) Suppose that $\zeta_q \in K$. Then the $\mathrm{Gal}(K)$-submodule $\ker(\mathbf{1} - \boldsymbol{\delta}_q)$ of $J^{(f,q)}(K_a)$ is isomorphic to $V_{f,p}$. (See [34, Lemma 4.11], [39, Th. 9.1].) In particular, $\ker(\mathbf{1} - \boldsymbol{\delta}_q)$ is a N-dimensional vector space over $\mathbb{F}_p$ where
   - $N = n - 1$ if p does *not* divide n;
   - $N = n - 2$ if p divides n and q divides n.

   (Here $\mathbf{1}$ stands for the identity automorphism of $J^{(f,q)}$.)

(vii) Let us consider the action of the subfield $\mathbb{Q}[\boldsymbol{\delta}_q]$ of $\mathrm{End}^0(J^{(f,q)})$ on $\Omega^1(J^{(f,q)})$. Let $i < q$ be a positive integer that is *not* divisible by p and $\sigma_i : \mathbb{Q}[\boldsymbol{\delta}_q] \hookrightarrow \mathbb{C}$ be the field embedding that sends $\boldsymbol{\delta}_q$ to ζ_q^{-i}. Clearly,

$$\Omega^1(J^{(f,q)}) = \oplus_i \Omega^1(J^{(f,q)})_{\sigma_i}$$

where $\Omega^1(J^{(f,q)})_{\sigma_i}$ are the corresponding weight subspaces (see Section 2). Let us consider the nonnegative integers

$$n_{\sigma_i} := \dim_{\mathbb{C}}(\Omega^1(J^{(f,q)})_{\sigma_i}).$$

(1) If p does *not* divide n then

$$n_{\sigma_i} = \left[\frac{ni}{q}\right]$$

[34, Remark 4.13]. In addition, the number of i with $n_{\sigma_i} \neq 0$ is strictly greater than

$$\frac{(p-1)p^{r-1}}{2} = \frac{\phi(q)}{2} = \frac{[\mathbb{Q}[\boldsymbol{\delta}_q] : \mathbb{Q}]}{2}$$

[34, p. 357-358]).

(2) If p is odd and q divides n then the GCD of all n_{σ_i}'s is 1 [39, Lemma 8.1(D].

(3) If p is an odd prime that does *not* divide n, and either $n = q+1$ or $n-1$ is *not* divisible by q, then n the GCD of all n_{σ_i}'s is 1 [39, Lemma 8.1(D].

(viii) If p is odd and $\mathbb{Q}[\boldsymbol{\delta}_q]$ is a maximal commutative subalgebra of $\mathrm{End}^0(J^{(f,q)})$ then

$$\mathrm{End}^0(J^{(f,q)}) = \mathbb{Q}[\boldsymbol{\delta}_q],\ \mathrm{End}(J^{(f,q)}) = \mathbb{Z}[\boldsymbol{\delta}_q]$$

([34, Th. 4.16], [39, Th. 8.3]).

Theorem 8.2. *Let $n \geq 5$ be an integer, p an odd prime, and K contains a primitive qth root of unity. Suppose that either p does not divide n or q divides n.*

Let us put $N := n-1$ if p does not divide n and $N := n-2$ if $q \mid n$. Suppose that the Galois group $\mathrm{Gal}(f)$ of $f(x)$ contains a subgroup H such that the representation of H in $\left(\mathbb{F}_p^{\mathfrak{R}_f}\right)^{00} = V_{f,p}$ is absolutely irreducible. Assume additionally that the index of every maximal subgroup of H does not divide N and one of the following conditions holds.

(i) *The representation of H in $\left(\mathbb{F}_p^{\mathfrak{R}_f}\right)^{00} = V_{f,p}$ is very simple.*

(ii) *Either p does not divide n and $n-1$ is not divisible by q, or $n = q+1$, or $q \mid n$.*

Then $\mathrm{End}^0(J^{(f,q)}) = \mathbb{Q}[\boldsymbol{\delta}_q]$ and $\mathrm{End}(J^{(f,q)}) = \mathbb{Z}[\boldsymbol{\delta}_q]$. In particular, $J^{(f,q)}$ is an absolutely simple abelian variety.

Proof. Enlarging K if necessary, we may and will assume that $H = \mathrm{Gal}(f)$. It follows from Proposition 4.4 that the absolutely simple H-module $(\mathbb{F}_p^{\mathfrak{R}_f})^{00} = V_{f,p}$ is central simple.

Recall (Remark 8.1(v)) that the $\mathrm{Gal}(K)$-module $\ker(1-\boldsymbol{\delta}_q)$ is isomorphic to $V_{f,p}$ and therefore is also central simple. In addition, it is very simple if and only if the H-module $V_{f,p}$ is very simple.

Let Λ be the centralizer of $\mathbb{Z}[\boldsymbol{\delta}_q]$ in $\mathrm{End}(J^{(f,q)})$ and

$$\mathcal{H} = \Lambda_{\mathbb{Q}} := \Lambda \otimes \mathbb{Q}$$

the centralizer of $\mathbb{Q}[\boldsymbol{\delta}_q]$ in $\mathrm{End}^0(J^{(f,q)})$. Applying Proposition 5.7 to

$$Z = J^{(f,q)},\ E = \mathbb{Q}[\delta_q],\ \mathbf{i} = \mathbf{j}_{q,f},\ O_E = \mathbb{Z}[\boldsymbol{\delta}_q],$$

we conclude that $\mathcal{H} = \Lambda_{\mathbb{Q}} = \Lambda \otimes \mathbb{Q}$ is a central simple $\mathbb{Q}[\boldsymbol{\delta}_q]$-algebra of dimension d^2 for some positive integer d.

In addition, if the $\mathrm{Gal}(K)$-module $\ker(1 - \boldsymbol{\delta}_q)$ is very simple, then either

$$d = 1,\ \mathcal{H} = \mathbb{Q}[\boldsymbol{\delta}_q], \Lambda = \mathbb{Z}[\boldsymbol{\delta}_q]$$

or

$$d = N = \frac{2g}{\phi(q)} = \dim_{\mathbb{F}_p}(V_{f,p})$$

where

$$g = \dim(J^{(f,q)}),\ \phi(q) = [\mathbb{Q}(\zeta_q) : \mathbb{Q}] = [\mathbb{Q}[\boldsymbol{\delta}_q] : \mathbb{Q}].$$

In light of Remark 8.1(i-ii) combined with Proposition 5.7(ii), $d \neq 2g/[\mathbb{Q}[\boldsymbol{\delta}_q] : \mathbb{Q}]$. So, in the very simple case $\mathcal{H} = \mathbb{Q}[\boldsymbol{\delta}_q], \Lambda = \mathbb{Z}[\boldsymbol{\delta}_q]$.

Now suppose that $\ker(1 - \boldsymbol{\delta}_q)$ is *not very* simple. Then $V_{p,f}$ is not very simple. This implies that either $n = q + 1$, or p does not divide n and $n - 1$ is not divisible by q or $q \mid n$. It follows from Proposition 5.7(i) combined with Remark 8.1(vii) that $d = 1$. This implies that $\mathcal{H} = \mathbb{Q}[\boldsymbol{\delta}_q]$. Therefore

$$\mathbb{Z}[\boldsymbol{\delta}_q] \subset \Lambda \subset \mathbb{Q}[\boldsymbol{\delta}_q].$$

This implies that $\Lambda = \mathbb{Z}[\boldsymbol{\delta}_q]$ and therefore $\mathcal{H} = \mathbb{Q}[\boldsymbol{\delta}_q]$ is a maximal commutative subalgebra of $\mathrm{End}^0(J^{(f,q)})$ Now the desired result follows from Remark 2.2(viii). □

Proof of Theorems 1.10 and 1.9. Enlarging K if necessary, we may assume that K contains a primitive qth root of unity, and

- $\mathrm{Gal}(f) = \mathrm{Alt}(\mathfrak{R}_f) =: H$ in the case of Theorem 1.10;
- $\mathrm{Gal}(f) = H$ in the case of Theorem 1.9.

It follows from Theorem 8.2 that $\mathrm{End}^0(J^{(f,q)}) = \mathbb{Q}[\boldsymbol{\delta}_q] \cong \mathbb{Q}(\zeta_q)$ and $J^{(f,q)}$ is an absolutely simple abelian variety for $q = p^r$ when r is any positive integer. This implies that for distinct positive integers i and j there are no nonzero homomorphisms between $J^{(f,p^i)}$ and $J^{(f,p^j)}$, because they are absolutely simple abelian varieties with non-isomorphic endomorphism algebras. This implies that the endomorphism algebra $\mathrm{End}^0(Y)$ of the product $Y := \prod_{i=1}^r J^{(f,r^i)}$ is $\prod_{i=1}^r \mathbb{Q}(\zeta_{p^i})$, whose $\mathbb{Q}$-dimension is $q - 1$.

In light of Remark 8.1(iv), if p does *not* divide n then Y is isogenous to $J(C_{f,q})$. It follows that $\mathrm{End}^0(J(C_{f,q}))$ also has $\mathbb{Q}$-dimension $(q - 1)$.

However, we know that the $\mathbb{Q}$-algebra $\mathrm{End}^0(J(C_{f,q}))$ contains the $\mathbb{Q}$-subalgebra $\mathbb{Q}[\delta_q]$ of $\mathbb{Q}$-dimension $(q-1)$, thanks to (3). This implies that

$$\mathrm{End}^0(J(C_{f,q})) = \mathbb{Q}[\delta_q] \cong \prod_{i=1}^{r} \mathbb{Q}(\zeta_{p^i}).$$

This ends the proof of Theorem 1.9.

Let us finish the proof of Theorem 1.10, following [34, Remark 4.3 and Proof of Th. 5.2 on p. 360]. It remains to do the case when $q \mid n$, say, $n = qm$ for some positive integer m. Since the case $q = p$ was already covered by already proven Theorem 1.3, we may assume that $q \ge p^2 \ge 9$ and therefore $n \ge 9$. Recall that $\mathrm{Gal}(f) = \mathrm{Alt}(\mathfrak{R}_f) \cong \mathbf{A}_n$. Let $\alpha \in K_a$ be a root of $f(x)$. Let us consider the overfield $K_1 = K(\alpha)$ of K. We have $f(x) = (x-\alpha)f_1(x) \in K_1[x]$ where $f_1(x)$ is a degree $(n-1)$ irreducible polynomial over K_1 with Galois group $\mathbf{A}_{n-1}$. Let us consider the polynomials

$$h(x) = f_1(x+\alpha),\ h_1(x) = x^{n-1} \in K_1[x]$$

of degree $n-1 \ge 9-1 = 8$. Notice that $n-1$ is not divisible by p and the Galois group of $h_1(x)$ over K_1 is still $\mathbf{A}_{n-1}$. The standard substitution

$$x_1 = \frac{1}{x-\alpha},\ y_1 = \frac{y}{(x-\alpha)^m}$$

establishes a birational isomorphisms between the curves $C_{f,q}$ and $C_{h_1,q}$ [30, p. 3359]. This implies that the Jacobians $J(C_{f,q})$ and $J(C_{h_1,q})$ are isomorphic and therefore their endomorphism algebras are also isomorphic. Applying to $J(C_{h_1,q})$ the already proven part of Theorem 1.10, we conclude that the $\mathbb{Q}$-algebra $\mathrm{End}^0(J(C_{h_1,q}))$ has $\mathbb{Q}$-dimension $(q-1)$. This implies that $\mathrm{End}^0(J(C_{f,q}))$ also has $\mathbb{Q}$-dimension $q-1$. However, we know that $\mathrm{End}^0(J(C_{f,q}))$ contains the $\mathbb{Q}$-subalgebra $\mathbb{Q}[\delta_q]$ of $\mathbb{Q}$-dimension $(q-1)$ (3). This implies that

$$\mathrm{End}^0(J(C_{f,q})) = \mathbb{Q}[\delta_q] \cong \prod_{i=1}^{r} \mathbb{Q}(\zeta_{p^i}).$$

This ends the proof of Theorem 1.10.

□

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; https://brauer.maths.qmul.ac.uk/Atlas/v3/

[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] Ch. W. Curtis, W.M. Cantor, G.M. Seitz, *The 2-transitive permutation representations of the finite Chevalley groups.* Trans. Amer. Math. Soc. **218** (1976), 1–59.

[5] J.D. Dixon, B. Mortimer, Permutation groups. GTM **163**, Springer-Verlag, New York, 1996.

[6] T. Eritsyan, Endomorphism rings and algebras of Jacobians of certain superelliptic curves. Ph.D. Thesis, Penn State, 2022.

[7] L. Dornhoff, Group Representation Theory, Part A. Marcel Dekker, Inc., New York, 1971.

[8] D. Gorenstein, R. Lyons, R. Solomon, The classification of the finite simple groups, Number 3. Mathematical Surveys and Monographs **40.3**, AMS, Providence, RI, 1998.

[9] R. M. Guralnick, P.H. Tiep, *Low-dimensional representations of special linear groups in cross characteristics.* Proc. London Math. Soc. (3) **78** (1999), 116–138.

[10] A. R. Hofer, *On unitary collineation groups.* J. Algebra **22** (1972), 211–218.

[11] B. Huppert, N. Blackburn, Finite groups III. Springer-Verlag, Berlin Heidelberg New York, 1982.

[12] G. Janusz, *Simple components of* $\mathbb{Q}[\mathrm{SL}(2,q)]$. Communications in Algebra **1:1** (1974), 1–22.

[13] M. Klemm, Über die Reduktion von Permutationsmoduln. Math. Z. **143:2** (1975), 113–117.

[14] P. B. Kleidman, *The maximal subgroups of the Chevalley groups* $\mathrm{G}_2(q)$ *with* q *odd, the Ree groups* ${}^2\mathrm{G}_2(q)$*, and their automorphism groups.* J. Algebra **117** (1988), 30-71.

[15] A. Kleshchev, L. Morotti, Ph. H. Tiep, *Irreducible restrictions of representations of symmetric and alternating groups in small characteristics.* Advances in Math. **369** (2020), 107184, 66 pp.

[16] J. K. Koo, *On holomorphic differentials of some algebraic function field of one variable over* C. Bull. Austral. Math. Soc. **43** (1991), 399–405.

[17] B. Mortimer, *The modular permutation representations of the known doubly transitive groups.* Proc. London Math. Soc. (3) **41** (1980), 1–20.

[18] D. Mumford, Abelian varieties, Second edition. Oxford University Press, London, 1974.

[19] K. Ribet, *Galois action on division points of Abelian varieties with real multiplications.* Amer. J. Math. 98 (1976), 751–804.

[20] D. Passman, Permutation groups. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[21] B. Poonen, E. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line.* J. reine angew. Math. **488** (1997), 141–188.

[22] C.E. Praeger, L.H. Soicher, Low rank representations and graphs for sporadic groups. Cambridge University Press 1997.

[23] E. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve.* Math. Ann. **310** (1998), 447–471.

[24] J.-P. Serre, *Points d'ordre fini des courbes elliptiques.* Invent. Math. **15** (1972), 259–331.

[25] J.-P. Serre, Topics in Galois Theory. Jones and Bartlett Publishers, Boston-London, 1992. 163–176;

[26] J.-P. Serre, Linear representations of finite groups. Springer-Verlag, 1977.

[27] G. Shimura, Abelian varieties with complex multiplication and modular functions. Princeton University Press, 1997.

[28] R. Steinberg, Lectures on Chevalley Groups. University Lecture Series **66**. American Mathematical Society, Providence, RI, 2016.

[29] M. Suzuki, Group Theory I. Springer-Verlag, 1982.

[30] C. Towse, *Weierstrass points on cyclic covers of the projective line*. Trans. AMS **348** (1996), 3355-3377.

[31] A. Wagner, *The faithful linear representations of least degree of* $\mathbf{S}_n$ *and* $\mathbf{A}_n$ *over a field of odd characteristic*. Math. Z. **154** (1977), 103–114.

[32] L. Washington, Introduction to cyclotomic fields. GTM **83** (1997), Springer Verlag, New York, 1997.

[33] J. Xue, *Endomorphism algebras of Jacobians of certain superelliptic curves*. J. Number Theory **131** (2011), no. 2, 332–342.

[34] Yu. G. Zarhin, *Hyperelliptic Jacobians and modular representations*. In "Moduli of abelian varieties" (C. Faber, G. van der Geer, F. Oort, eds.). Progr. Math. **195** (2001), 473–490.

[35] Yu. G. Zarhin, *Very simple* 2*-adic representations and hyperelliptic Jacobians*. Moscow Math. J. **2:2** (2002), 403-431.

[36] Yu. G. Zarhin, *Cyclic covers of the projective line, their Jacobians and endomorphisms*. J. reine angew. Math. **544** (2002), 91–110.

[37] Yu. G. Zarhin, *The endomorphism rings of cyclic covers of the projective line*. Math. Proc. Cambridge Phil. Soc. **136:2** (2004), 257–267.

[38] Yu. G. Zarhin, *Very simple representations: variations on a theme of Clifford*, p. 151-168. In: Progress in Galois Theory (H. Voelklein and T. Shaska, eds), Springer Science + Business Media Inc., 2005.

[39] Yu. G. Zarhin, *Endomorphism algebras of abelian varieties with special reference to superelliptic Jacobians*. In: Geometry, Algebra, Number Theory, and their information technology applications, p. 477–528 (A. Akbary, S. Gun, eds). Springer Nature Switzerland AG, 2018.

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

Email address: zarhin@math.psu.edu