Computational algorithm for reduction type of CM abelian varieties

Artyom Smirnov, Alexey Zaytsev

PII: S0021-8693(19)30508-3
DOI: https://doi.org/10.1016/j.jalgebra.2019.08.032
Reference: YJABR 17352

To appear in: *Journal of Algebra*

Received date: 10 April 2019

Please cite this article as: A. Smirnov, A. Zaytsev, Computational algorithm for reduction type of CM abelian varieties, *J. Algebra* (2019), doi: https://doi.org/10.1016/j.jalgebra.2019.08.032.

COMPUTATIONAL ALGORITHM FOR REDUCTION TYPE OF CM ABELIAN VARIETIES

ARTYOM SMIRNOV AND ALEXEY ZAYTSEV[1]

Abstract. Let $\mathcal{A}$ be an abelian variety over a number field, with a good reduction at a prime ideal containing a prime number p. Denote A as an abelian variety over a finite field of characteristic p, which is obtained by the reduction of $\mathcal{A}$ at the prime ideal. In this study, we derive an algorithm that allows us to decompose the group scheme A$[p]$ into indecomposable quasi-polarized BT_1-group schemes up to isomorphism. This can be achieved for the unramified p based on its decomposition into prime ideals in the endomorphism algebra of A. We also compute all types of these correspondences for abelian varieties with dimensions up to 5. As a consequence, we establish the relationship between the decompositions of prime p and the corresponding pairs of p-rank and a-number for an abelian variety A.

1. Introduction

In this study, we propose an explicit algorithm for obtaining a general solution to the problem of generalizing the Deuring reduction theorem on elliptic curves with complex multiplication to abelian varieties with complex multiplication.

We recall that the Deuring reduction theorem establishes a one-to-one correspondence between the type of decomposition into primes of ideals generated by a prime number p in the endomorphism algebra of a given elliptic curve (over a number field) and the number of $p-$torsion points of reduced elliptic curves. In particular, the classical Deuring reduction theorem (e.g., see [6], Theorem 12, page 182) states the following.

Theorem 1.1. *Let $\mathcal{E}$ be an elliptic curve over a number field, with* $\mathrm{End}(\mathcal{E}) \cong \mathcal{D}$*, where $\mathcal{D}$ is an order in an imaginary quadratic field K. Let $\mathcal{P}$ be a place of $\bar{\mathbb{Q}}$ over a prime number p, where $\mathcal{E}$ has non-degenerate reduction E. The curve E is supersingular if and only if p has one prime of K above it (p is ramified or inert). The curve E is ordinary if and only if p splits completely in K.*

Thus, as an abstract group, the group of $p-$torsion points of an elliptic curve E is isomorphic to:

$$E[p](\bar{\mathbb{F}}_p) \cong \begin{cases} (0), \text{ if } \quad p\mathcal{O}_K = \mathcal{P}^2 \quad \text{or} \quad p\mathcal{O}_K = \mathcal{P}, \\ \mathbb{Z}/p\mathbb{Z}, \quad \text{if} \quad p\mathcal{O}_K = \mathcal{P}\mathcal{P}^c, \end{cases}$$

where P^c is the complex conjugation of P.

Date: October 2, 2019

[1]High School of Economics,

[1]Skolkovo Institute of Science and Technology,

This result given in terms of the $p-$torsion points and the decomposition into prime ideals can be extended to a dimension of 2 (e.g., see [4]), but the situation becomes more subtle for higher dimensions. The connection between structures of $p-$torsion points and the decomposition of the ideal can be classified only up to isogeny, and it is clear that no such classification exists up to isomorphism. Thus, in order to obtain a classification up to isomorphism (not only up to isogeny), we need to reformulate these connections in terms of indecomposable group schemes (instead of abstract groups) and the Galois groups of the corresponding Galois closure of the CM-field. Recently, some partial results were obtained by [1], [12], and [13], but we cover, extend, and generalize these results to higher dimensions.

Let us describe the classified relationships in a precise manner. Let $\mathcal{A}$ be a simple abelian variety of dimension g, which has complex multiplication by the full ring of integers $\mathcal{O}_K$ of CM field K. Assume that $\mathcal{A}$ has a good reduction at prime $\mathcal{P}$ of $\mathcal{O}_K$, which is denoted by A. In addition, suppose that the prime $p = \mathcal{P} \cap \mathbb{Z}$ is unramified in K. In this study, we propose a general algorithm for computing the correspondences between the decompositions of p into prime ideals in $\mathcal{O}_K$ and decompositions of the group scheme $\mathrm{A}[p]$ into quasi-polarized indecomposable BT_1-group schemes.

The remainder of this paper is organized as follows. In Section 2, we propose a generalization of the Deuring reduction theorem for abelian varieties up to dimension 5 as a corollary of the main relationships in the last section. In Section 3, we develop a theory that provides a basis for the algorithm in Section 4. In Section 5, we describe the algorithm and give the results in general form.

2. Results for abelian varieties up to dimension 5

Let $\mathcal{A}$ be an abelian group scheme of relative dimension n over $\mathrm{Spec}(\mathcal{O}_L)$, where $\mathcal{O}_L$ is the full ring of integers of some number field L. Assume that $\mathcal{A}$ has complex multiplication by the full ring of integers of some CM field K and that $K \subset L$.

Let $\mathcal{P}$ be a prime of $\mathcal{O}_L$ and p be a prime number in $\mathcal{P} \cap \mathbb{Z}$, which is unramified in K. Denote A as the reduction of $\mathcal{A}$ at the prime $\mathcal{P}$. Then, the following relationships exist between a decomposition into prime ideals of the ideal (p) in the full ring of integers $\mathcal{O}_K$ and the invariants of the abelian variety $\mathcal{A}$, i.e., p-rank and a-number.

2.1. **Elliptic curves.** This result is widely known as the Deuring reduction theorem.

ideal decomposition	BT_1 group schemes	p-rank	a-number
PP^c	$\mathbb{Z}/p \times \mu_p$	1	0
P	$I_{1,1}$	0	1

2.2. **Abelian surfaces.** Details of the classification of abelian surfaces were provided by [4] and [13].

ideal decomposition	BT_1 group schemes	p-rank	a-number
$P_1P_1^cP_2P_2^c$	$(\mathbb{Z}/p \times \mu_p)^2$	2	0
PP^c	$(\mathbb{Z}/p \times \mu_p)^2$	2	0
	$I_{1,1}^2$	0	2
$P_1P_1^cP_2$	$\mathbb{Z}/p \times \mu_p \times I_{1,1}$	1	1
P_1P_2	$I_{1,1}^2$	0	2
P	$I_{2,1}$	0	1

2.3. **Abelian threefolds.** We provide the results obtained by [13] for abelian threefolds, as follows.

ideal decomposition	BT_1 group schemes	p-rank	a-number
$\mathcal{P}$	$\mathrm{I}_{3,1}$	0	1
	$\mathrm{I}_{1,1}^3$	0	3
$\mathcal{P}\mathcal{P}^c$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^3$	3	0
	$\mathrm{I}_{3,2}$	0	2
$\mathcal{P}_1\mathcal{P}_2$	$\mathrm{I}_{1,1} \times \mathrm{I}_{2,1}$	0	2
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{1,1}$	2	1
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{2,1}$	1	1
	$\mathrm{I}_{1,1}^3$	0	3
$\mathcal{P}_1\mathcal{P}_2\mathcal{P}_3$	$\mathrm{I}_{1,1}^3$	0	3
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^3$	3	0
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{1,1}^2$	1	2
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_3$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{1,1}^2$	1	2
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{1,1}$	2	1
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3\mathcal{P}_3^c$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^3$	3	0

2.4. **Dimensions** 4 **and** 5**.** Let f be p-rank and a be an a-number corresponding to the abelian variety A. Denote (α, β) as a pair of non-negative integers such that $p\mathcal{O}_K = \mathcal{P}_1 ... \mathcal{P}_\alpha$ and $p\mathcal{O}_{K_0} = \mathcal{Q}_1 ... \mathcal{Q}_\beta$, and denote by K_0 the largest totally real subfield of K with the full ring of integers $\mathcal{O}_{K_0}$.

As a consequence of the main results given for dimensions 4 and 5 in Section 5, the following correspondence between the pairs (a, f) and (α, β) is easy to obtain.

f \ a	1	2	3	4	5	
0		$(1,1)$	$(2,1),\ (2,2)$	$(1,1)$ $(3,2),\ (3,3)$	$(2,1),\ (2,2)$ $(4,2),\ (4,3),\ (4,4)$	$(1,1)$ $(3,2),\ (3,3)$ $(5,3),\ (5,4),\ (5,5)$
1	$(2,1)$	$(3,2)$	$(4,2),\ (4,3)$	$(3,2)$ $(5,3),\ (5,4)$	$(4,2),\ (4,3)$ $(6,3),\ (6,4),\ (6,5)$	
2	$(2,1)$ $(4,2)$	$(3,2)$ $(5,3)$	$(4,2),\ (4,3)$ $(6,3),\ (6,4)$	$(5,3),\ (5,4)$ $(7,4),\ (7,5)$		
3	$(2,1)$ $(4,2)$ $(6,3)$	$(3,2)$ $(5,3)$ $(7,4)$	$(4,2),\ (4,3)$ $(6,3),\ (6,4)$ $(8,4),\ (8,5)$			
4	$(2,1)$ $(4,2)$ $(6,3)$ $(8,4)$	$(3,2)$ $(5,3)$ $(7,4)$ $(9,5)$				
5	$(2,1)$ $(4,2)$ $(6,3)$ $(8,4)$ $(10,5)$					

3. Preliminaries and classification of quasi-polarized indecomposable BT_1-group schemes up to dimension 5

In this section, we provide a brief overview of the category of finite commutative group schemes over a perfect field k with $\mathrm{char(k)} = p > 0$. We also provide a classification of quasi-polarized indecomposable BT_1-group schemes over perfect fields up to dimension 5 via circular words because we were not able to find an explicit classification in previous studies. For more detailed information regarding

the category of finite commutative group schemes over a perfect field, we refer the reader to [5], [9], and [10].

3.1. **Decomposition of the category.** Let k be a perfect field of characteristic $p > 0$. Denote $C = C_k$ as the category of finite commutative group schemes over $\mathrm{Spec}(k)$. By definition, a finite scheme G over $\mathrm{Spec}(k)$ is affine. Therefore, category C is equivalent to the category of commutative finitely generated k-bialgebras (which are automatically flat).

Now, we introduce the following classes of finite commutative group schemes.

Definition 3.1. *A finite commutative group scheme G over $\mathrm{Spec}(k)$ is called:*

- **étale**, *if the structure morphism $G \to \mathrm{Spec}(k)$ is étale;*
- **local**, *if G is connected.*

We write C_{loc} for the full subcategory of C comprising all $G \in C$ that are local and C_{et} for the full subcategory of C comprising all $G \in C$ that are étale.

The following is an important observation.

Lemma 3.2. *Let $G \in G_{loc}$ and $H \in C_{et}$. Then,*

$$\mathrm{Hom}_C(G, H) = \mathrm{Hom}_C(H, G) = (0).$$

Each object $G \in C$ can be written in a unique manner in the form:

$$G = G_{et} \times G_{loc},$$

where $G_{et} \in C_{et}$, $G_{loc} \in C_{loc}$ and

$$\mathrm{Hom}_C(G, H) = \mathrm{Hom}_C(G_{et}, H_{et}) \times \mathrm{Hom}_C(G_{loc}, H_{loc}).$$

The same decomposition holds for the linear dual G^D. Therefore, category C splits into the following four categories:

- $C_{loc,loc}$, the category of all $G \in C_{loc}$ with $G^D \in C_{loc}$;
- $C_{loc,et}$, the category of all $G \in C_{loc}$ with $G^D \in C_{et}$;
- $C_{et,loc}$, the category of all $G \in C_{et}$ with $G^D \in C_{loc}$;
- $C_{et,et}$, the category of all $G \in C_{loc}$ with $G^D \in C_{et}$.

Hence, category C has the following decomposition:

$$C = C_{et,et} \times C_{et,loc} \times C_{loc,et} \times C_{loc,loc}.$$

Each category is abelian, and hence C is itself abelian.

Proposition 3.3. *The following equivalences hold:*

a: *$G \in C_{et,et}$ if and only if Frob_G and Ver_G are isomorphisms;*
b: *$G \in C_{et,loc}$ if and only if Frob_G is isomorphism and Ver_G is nilpotent;*
c: *$G \in C_{loc,et}$ if and only if Frob_G is nilpotent and Ver_G is isomorphism;*
d: *$G \in C_{loc,loc}$ if and only if Frob_G and Ver_G are both nilpotent.*

In the following, we focus on the group scheme $\mathrm{A}[p]$, where A is an abelian variety defined over a finite field $\mathbb{F}_q$, with $p = \mathrm{char}(\mathbb{F}_q)$. The group scheme $\mathrm{A}[p]$ belongs to category C. Furthermore, due to the proposition above and based on the relationship $\mathrm{Frob} \cdot \mathrm{Ver} = \mathrm{Ver} \cdot \mathrm{Frob} = p$ and the fact that p is nilpotent, it follows that:

$$A[p] \in C_{et,loc} \times C_{loc,et} \times C_{loc,loc}.$$

3.2. **Circular words.** We write $C(1)_k$ for the category of finite commutative k-group schemes that are killed by p, where k is a perfect algebraically closed field of characteristic $p > 0$. The Dieudonné functor shows that the full subcategory $C(1)_k$ of C is equivalent to the category of triples (M, $\mathcal{F}$, $\mathcal{V}$), where:

- M is a finite dimensional k-vector space,
- $\mathcal{V} : \mathrm{M} \to \mathrm{M}$ is a Frob_k-linear map, and
- $\mathcal{F} : \mathrm{M} \to \mathrm{M}$ is a Frob_k^{-1}-linear map,

such that $\mathcal{F}\mathcal{V} = \mathcal{V}\mathcal{F} = 0$.

Definition 3.4.
- *A finite locally free commutative group scheme G over a scheme S is called a* **truncated Barsotti–Tate group of level** 1 *or a* BT_1 **group scheme** *if it is killed by p and* $\mathrm{Ker}(\mathrm{Frob}_G) = \mathrm{Im}(\mathrm{Ver}_G)$.
- *A pair (G, λ) is called a* **quasi-polarized** BT_1 *group scheme, where G is* BT_1 *group scheme and $\lambda : G \to G^D$ is a homomorphism of* BT_1 *group schemes.*

In terms of exact sequences, a group scheme $\mathrm{G} \in C(1)_k$ is a BT_1 group scheme if and only if the sequence:

$$\mathrm{G} \xrightarrow{\mathcal{F}_\mathrm{G}} \mathrm{G}^{(p)} \xrightarrow{\mathcal{V}_\mathrm{G}} \mathrm{G} \ ,$$

is exact. For the Dieudonné module, this means that $\mathrm{Ker}(\mathcal{V}) = \mathrm{Im}(\mathcal{F})$ and $\mathrm{Ker}(\mathcal{F}) = \mathrm{Im}(\mathcal{V})$.

In an unpublished manuscript [5], Kraft showed that there is a normal form for an object of $C(1)_k$. The normal form is distinguished into two types of group schemes comprising linear and circular types, and the group scheme $\mathrm{A}[p]$ corresponds only to the circular type.

Definition 3.5. *A* **circular word** *is a finite ordered set of symbols $\mathcal{F}$ and $\mathcal{V}$:*

$$w = L_1 \dots L_t, \qquad L_i \in \{\mathcal{F}, \mathcal{V}\}.$$

We say that two words w_1 and w_2 are equivalent if a cyclic permutation exists that transforms one word into another. Thus, the class of a word is given by $[L_1 \dots L_t] = [L_2 \dots L_t\, L_1] = \dots = [L_t\, L_1 \dots L_{t-1}]$.

A **dual word** $\bar{w}$ to the circular word w is given by replacing $\mathcal{F}$ with $\mathcal{V}$ and $\mathcal{V}$ with $\mathcal{F}$ in w. We only consider self-dual circular words because the scheme $\mathrm{A}[p]$ is symmetric.

For a given word w, we can construct a finite group scheme G_w over k defined by the $k-$vector space:

$$\mathbb{D}(G_w) = \sum_{i=1}^{t} k\, z_i,$$

with the structure of the Diuedonné module given by:

$$\begin{aligned} &\text{if } L_i = \mathcal{F}, \quad \text{then } \mathcal{F} z_i = z_{i+1} \text{ and } \mathcal{V}\, z_{i+1} = 0, \\ &\text{if } L_i = \mathcal{V}, \quad \text{then } \mathcal{V} z_{i+1} = z_i \text{ and } \mathcal{F}\, z_i = 0. \end{aligned}$$

A word w is called **decomposable** if $t', \mu \in \mathbb{Z}_{>0}$, with $\mu \cdot t' = t$ and $L_1, ..., L_{t'} \in \{\mathcal{F}, \mathcal{V}\}$ exist such that:

$$[L_1 ... L_t] = [(L_1 ... L_{t'})^\mu] = [(L_1 ... L_{h'}) ... (L_1 ... L_{h'})].$$

If writing with $\mu > 1$ in this manner is not possible, we say that the word w is **indecomposable**.

Category $C(1)_k$ is abelian and all objects have a finite length. Hence, every object from $C(1)_k$ is a direct sum of indecomposable objects. This decomposition is unique up to isomorphism and permutation of the factors. The following theorem was given by [5].

Theorem 3.6. (1) *A circular word w defines a BT_1-group scheme G_w, and w is indecomposable if and only if G_w is indecomposable.*
(2) *Any BT_1-group scheme over k is a direct sum of indecomposable BT_1-group schemes.*
(3) *For any indecomposable BT_1-group scheme G over k, an indecomposable word w exists such that $G \cong G_w$.*

Corollary 3.7. *A quasi-polarized BT_1-group scheme G over k is indecomposable (i.e., G is not a direct sum of two quasi-polarized BT_1-group schemes) if:*

- *either $G = G_w$, where w is an indecomposable word, for which $[w] = [\bar{w}]$;*
- *or $G = G_u \oplus G_v$, where u and v are distinct indecomposable words such that $[\bar{u}] = [v]$.*

3.3. **Description of p-rank and a-number in terms of circular words.** Next, we give the definitions of the p-rank and a-number of an abelian variety over $\bar{\mathbb{F}}_p$, and describe them in terms of circular words.

Definition 3.8. *Let A be an abelian variety of dimension g over a perfect field k, with $\mathrm{char}(k) = p > 0$.*

- *A number $f(\mathrm{A})$ is called p-**rank** of abelian variety A if:*
$$\mathrm{A}[p](\bar{\mathbb{F}}_p) \cong (\mathbb{Z}/p\mathbb{Z})^{f(\mathrm{A})}.$$
- *A number:*
$$a(\mathrm{A}) = \dim_{\bar{\mathbb{F}}_p} \mathrm{Hom}(\alpha_p, \mathrm{A}[p])$$
*is called a-**number** of abelian variety A.*

The group scheme μ_p is dual to $\mathbb{Z}/p\mathbb{Z}$ and $\mathrm{A}[p]$ is a self-dual group scheme, so it is clear that:
$$f(\mathrm{A}) = \dim_{\bar{\mathbb{F}}_p} \mathrm{Hom}(\mu_p, \mathrm{A}[p]) \qquad \text{and} \qquad 0 \leq f(\mathrm{A}) \leq \dim(A).$$

Since $\mathrm{Ker}(\mathrm{Frob}_k) \cap \mathrm{Ker}(\mathrm{Ver}_k)$ is the product of a certain number of copies of α_p, then we also obtain:
$$a(\mathrm{A}) = \log_p \mathrm{ord} S = \dim_{\bar{\mathbb{F}}_p} \ker\left(\mathrm{Ver}_k : H^0(\mathrm{A}, \Omega^1_{\mathrm{A}}) \to H^0(\mathrm{A}, \Omega^1_{\mathrm{A}})\right),$$
where S is a maximal subgroup scheme in $\mathrm{A}[p]$, which is killed by the action of Frob_k and Ver_k.

Remark 3.9. *Given that the group schemes μ_p and α_p are simple, it follows that the invariants p-rank and a-number are additive, i.e., if G_1 and G_2 are from $C(1)_k$, then:*
$$f(G_1 \oplus G_2) = f(G_1) + f(G_2),$$
$$a(G_1 \oplus G_2) = a(G_1) + a(G_2).$$

We provide an important result that is needed to compute the invariants.

Proposition 3.10. *Let G be a finite group scheme over $\bar{\mathbb{F}}_p$ of local-local type. Then, the group scheme* $\ker(\mathrm{Frob}_G) \cap \ker(\mathrm{Ver}_G)$ *is isomorphic to the $a(G)$ copies of α_p, i.e.,*

$$\alpha_p^{a(G)} \cong \ker(\mathrm{Frob}_G) \cap \ker(\mathrm{Ver}_G),$$

where Frob_G *and* Ver_G *are the morphisms of Frobenius and Verschiebung that act on G, respectively.*

In order to describe the a-number in terms of circular words, for each circular word w, we introduce a new auxiliary invariant comprising the number $c(w)$ corresponding to the word w.

Definition 3.11. *Let w be a circular word and the word w^* is received from w by cyclic permutation of symbols such that the word w^* starts from the symbol $\mathcal{F}$ and is ended by the symbol $\mathcal{V}$. Then, we denote $c(w)$ as a number of subwords of the form $\mathcal{FV}$ in the word w^*. We note that the selected representative w^* of the class $[w]$ always exists, but it may not be unique with the desired property. However, in any case, the number $c(w)$ will not depend on the choice of representative w^*.*

Now, we can describe an a-number in terms of $c(w)$ numbers.

Proposition 3.12. *Let* A *be an abelian variety over $\bar{\mathbb{F}}_p$. Assume that the group scheme* $\mathrm{A}[p]$ *corresponds to a set of indecomposable words $\{w_i\}$ under the equivalence of the categories. Then, a-number of* A *is a sum of $c(w_i)$, i.e.,*

$$a(\mathrm{A}) = \sum_{i=1}^{n} c(w_i).$$

Proof. If $\mathrm{A}[p]$ is a direct sum $G_1 \oplus ... \oplus G_m$ of indecomposable group schemes, then $a(A) = \sum a(G_i)$. Hence, it is sufficient to show that $a(G) = c(w)$ for an indecomposable group scheme $G = G_w$ (corresponding to an indecomposable word w).

A given indecomposable word w describes the operators $\mathcal{F}$ and $\mathcal{V}$ on $\mathbb{D}(G) = \sum \bar{\mathbb{F}}_p z_i$ under the equivalence of the categories of $C_{loc,\,loc}$ and the Diedounne modules. Therefore:

$$a(G) = \dim_{\bar{\mathbb{F}}_p}(\ker \mathcal{F} \cap \ker \mathcal{V}) = \dim_{\bar{\mathbb{F}}_p}\{x \in \mathbb{D}(G) | \mathcal{F}(x) = \mathcal{V}(x) = 0\} =$$

$$= \dim_{\bar{\mathbb{F}}_p}\{x = \sum_{i=1}^{t} x_i z_i | \sum x_i^p \mathcal{F}(z_i) = \sum x^{p^{-1}} \mathcal{V}(z_i) = 0\} =$$

$$= \#\{i | \mathcal{F}(z_i) \neq 0 \text{ and } \mathcal{V}(z_i) \neq 0\} =$$

$$= \text{“number of subwords of the form } \mathcal{FV} \text{ in the word } w^*\text{”} = c(w).$$

□

3.4. **Quasi-polarized indecomposable BT_1-group schemes of order p^{2g} with g up to 5.** Due to Corollary 3.7, we can describe each isomorphism class of the quasi-polarized indecomposable BT_1-group schemes over $\bar{\mathbb{F}}_p$ in terms of self-dual sets of indecomposable circular words.

In order to illustrate the procedure for establishing relationships, we consider an example of the quasi-polarized indecomposable BT_1-group schemes with dimension 2.

From Corollary 3.7, it follows that the indecomposable BT_1-group scheme G is either G_w for an indecomposable word w of length 4 such that $w = \bar{w}$, or $G =$

$G_u \oplus G_v$, where u and v are distinct indecomposable words of length 2 such that $\bar{u} = v$. However, there are only two indecomposable words of length 2, i.e., $\mathcal{FV}$ and $\mathcal{VF}$, but the words $\mathcal{FV}$ and $\mathcal{VF}$ are equivalent. Hence, we have to run over all indecomposable words of length 4 for which $[w] = [\bar{w}]$. The set of all non-equivalent words of length 4 comprises $w_1 = [\mathcal{FFFF}]$, $w_2 = [\mathcal{FFFV}]$, $w_3 = [\mathcal{FFVV}]$, $w_4 = [\mathcal{FVFV}]$, $w_5 = [\mathcal{FVVV}]$, and $w_6 = [\mathcal{VVVV}]$. Only three words comprising w_2, w_3, and w_5, are indecomposable. However, only one word w_3 is self-dual, and thus only this word corresponds to the quasi-polarized indecomposable BT_1-group scheme, which is denoted by $\mathrm{I}_{2,1}$.

Each a-number in the table is computed according to Proposition 3.12. The case where $g = 5$ is the first when a pair (g, a) exists that corresponds to two non-isomorphic group schemes. Thus, we introduce additional notations $\mathrm{J}_{5,2}$ and $\mathrm{J}_{5,3}$ to distinguish these group schemes from $\mathrm{I}_{5,2}$ and $\mathrm{I}_{5,3}$.

Next, we provide a complete list of the isomorphism classes of quasi-polarized indecomposable BT_1-group schemes over $\bar{\mathbb{F}}_p$ of order p^{2g} with g up to 5.

g	circular words	group scheme	a-number
1	$[\mathcal{F}], [\mathcal{V}]$	$\mu_p \times \mathbb{Z}/p\mathbb{Z}$	0
	$[\mathcal{FV}]$	$\mathrm{I}_{1,1}$	1
2	$[\mathcal{FFVV}]$	$\mathrm{I}_{2,1}$	1
3	$[\mathcal{FFFVVV}]$	$\mathrm{I}_{3,1}$	1
	$[\mathcal{FFV}], [\mathcal{VVF}]$	$\mathrm{I}_{3,2}$	2
4	$[\mathcal{FFFFVVVV}]$	$\mathrm{I}_{4,1}$	1
	$[\mathcal{FFFV}], [\mathcal{VVVF}]$	$\mathrm{I}_{4,2}$	2
	$[\mathcal{FFVFVVFV}]$	$\mathrm{I}_{4,3}$	3
5	$[\mathcal{FFFFFVVVVV}]$	$\mathrm{I}_{5,1}$	1
	$[\mathcal{FFFFV}], [\mathcal{VVVVF}]$	$\mathrm{I}_{5,2}$	2
	$[\mathcal{FFFVV}], [\mathcal{VVVFF}]$	$\mathrm{J}_{5,2}$	2
	$[\mathcal{FFFVFVVVFV}]$	$\mathrm{I}_{5,3}$	3
	$[\mathcal{FFVFFVVFVV}]$	$\mathrm{J}_{5,3}$	3
	$[\mathcal{FFVFV}], [\mathcal{VVFVF}]$	$\mathrm{I}_{5,4}$	4

4. Algorithm Fundamentals

For the sake of completeness, let us recall the result given by [13] (Section 4) and adjust it for our use.

In this section, we recall the results given by [13] to demonstrate that the choice of a decomposition group and CM type derives a decomposition of the BT_1-group scheme of a simple abelian variety into irreducible BT_1-group schemes. The scheme $\mathrm{A}[p]$ is obtained after the reduction of a CM abelian variety $\mathcal{A}$ at a place of good reduction. We develop an explicit representation theory based on the approach described by [3] (section 2).

Let $\mathcal{A}$ be an abelian scheme of relative dimension g over $\mathrm{Spec}(\mathcal{O}_L)$, where $\mathcal{O}_L$ is the full ring of integers of a number field L. Assume that $\mathcal{A}$ has a complex multiplication by the full ring of integers of a CM field K and $K \subset L$. Suppose that $\mathcal{A}$ has a good reduction at a prime ideal $\mathcal{B} \subset \mathcal{O}_L$ and a number prime $p \in \mathcal{B} \cap \mathbb{Z}$ is unramified in K.

Let $p\mathcal{O}_K = P_1 \dots P_m$ be a decomposition into distinct prime ideals. Let $\tilde{K}$ be the Galois closure of K over $\mathbb{Q}$ and $p\mathcal{O}_K = \tilde{P}_1 \dots \tilde{P}_l$ be the decomposition into

prime ideals in $\tilde{K}$ (note that p is also unramified in the Galois closure $\tilde{K}$ because it is a composite of all embeddings of K into the fixed algebraic closure of $\mathbb{Q}$).

The ring $\mathcal{O}_K$ is a free $\mathbb{Z}-$module and $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} \cong K$. The semi-simple $\bar{\mathbb{Q}}$-algebra $\mathcal{O}_K \otimes_{\mathbb{Z}} \bar{\mathbb{Q}}$ can be decomposed into irreducible components:

$$\mathcal{O}_K \otimes_{\mathbb{Z}} \bar{\mathbb{Q}} \cong \prod_{\alpha \in \mathrm{Hom}(K,\bar{\mathbb{Q}})} \bar{\mathbb{Q}},$$

and thus it induces a decomposition into simple $\mathcal{O}_K \otimes_{\mathbb{Z}} \bar{\mathbb{F}}_p$-modules:

$$\mathcal{O}_K \otimes_{\mathbb{Z}} \bar{\mathbb{F}}_p \cong \prod_{\alpha \in \mathrm{Hom}(K,\bar{\mathbb{Q}})} \bar{\mathbb{F}}_p,$$

since p is unramified in K. Thus, the representation based on $\bar{\mathbb{F}}_q$-vector space $\mathbb{D}(A[p])$ of the semi-simple algebra $\mathcal{O}_K \otimes_{\mathbb{Z}} \bar{\mathbb{F}}_p$ is a direct sum of irreducible representations:

$$\mathbb{D}(A[p]) \cong \bigoplus_{\alpha \in \mathrm{Hom}(K,\mathbb{C})} V_\alpha,$$

where V_α is an irreducible $\mathcal{O}_K \otimes_{\mathbb{Z}} \bar{\mathbb{F}}_p$-module.

In order to obtain an explicit description of circular words, we reformulate this decomposition in terms of Galois actions. Let G be a Galois group $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$, $\Delta = \mathrm{Gal}(\tilde{K}/K)$, $\tilde{P} = \mathcal{B} \cap \mathcal{O}_{\tilde{K}}$ and σ be a generator of the decomposition group of a prime ideal $\tilde{P}$ in $\tilde{K}$. Then, the decomposition of $\mathcal{O}_K \otimes_{\mathbb{Z}} \bar{\mathbb{F}}_p$ can be written as follows:

$$\mathcal{O}_K/p\mathcal{O}_K \otimes_{\mathbb{Z}} \bar{\mathbb{F}}_p \cong \bigoplus_{i=1}^{m} F_{P_i} \otimes_{\mathbb{F}_p} \bar{\mathbb{F}}_p \cong$$

$$\bigoplus_{i=1}^{m} \left(\bigoplus_{\alpha \in \mathrm{Hom}(F_{P_i},\bar{\mathbb{F}}_p)} \bar{\mathbb{F}}_p \right) \cong \prod_{\alpha \in \mathrm{Hom}(K,\bar{\mathbb{Q}})} \bar{\mathbb{F}}_p,$$

where F_{P_i} is the residue field of a prime ideal P_i. The last isomorphism is derived from the fact that the embeddings $F_{P_i} \to \bar{\mathbb{F}}_p$ have one-to-one correspondences with the embeddings $K \to \bar{\mathbb{Q}}$ (because p is unramified).

Let us fix a prime ideal $\tilde{P} = \tilde{P}_i$ and an isomorphism $\mathcal{O}_{\tilde{K}}/\tilde{P} \cong \mathbb{F}_q \subset \bar{\mathbb{F}}_p$. Then, each $\alpha \in G$ induces an embedding $\mathbb{F}_q$ into $\bar{\mathbb{F}}_p$ by sending $(a \bmod \tilde{P}) \mapsto (\alpha(a) \bmod \tilde{P})$. Then, we have the following decomposition of $\mathbb{D}(A[p])$ into $2g$ one-dimensional eigenspaces:

$$\mathbb{D}(A[p]) = \bigoplus_{\alpha \in G \setminus \Delta} \mathrm{V}_\alpha,$$

where α runs through all conjugate classes of G by the action of Δ on the right and:

$$\mathrm{V}_\alpha = \{v \in \mathbb{D}(A[p]) \,|\, a(v) = (\alpha(a) \bmod \tilde{P})v \qquad \text{for any } a \in \mathcal{O}_K\}.$$

All V_α are isomorphic to each other, so it follows that $\dim_{\bar{\mathbb{F}}_p} V_\alpha = 1$ for each $\alpha \in G \setminus \Delta$.

The action of $\mathcal{O}_K$ on $\mathbb{D}(A[p])$ is imposed by a fixed isomorphism $\mathcal{O}_K \cong \mathrm{End}(A)$. The Frobenius Fr on $\mathbb{D}(A[p])$ is p-linear and commutes with the $\mathcal{O}_K$-action. Hence, for each irreducible component V_α of $\mathbb{D}(A[p])$, an irreducible component V_β exists

such that $\mathrm{Fr}(V_\alpha) \subset V_\beta$. Moreover, β corresponds to the class of $\sigma\alpha$ in $G\backslash\Delta$ (because $\sigma(a) \equiv a^p \bmod \tilde{P}$). Thus,

$$\mathrm{Fr} : \mathrm{V}_\alpha \to \mathrm{V}_{\sigma\alpha}.$$

Let us denote the fiber product $(\mathcal{A} \bmod \mathcal{B}) \times \bar{\mathbb{F}}_p$ by A. The set S of the isomorphism classes of irreducible factors of $\mathbb{D}(A[p])$ as an $\mathcal{O}_K \otimes_{\mathbb{Z}} \bar{\mathbb{F}}_p$-module can be identified with the set $\mathrm{Hom}(K, \bar{\mathbb{Q}})$ by identifying the isomorphism classes of irreducible representations of $\mathcal{O}_K \otimes_{\mathbb{Z}} \bar{\mathbb{F}}_p$ in $\bar{\mathbb{F}}_p$ and the set S. An exact sequence of group schemes exists:

$$0 \to A[\mathrm{Ver}] \to A[p] \xrightarrow{\mathrm{Ver}} A[\mathrm{Fr}] \to 0,$$

which yields an exact sequence of the Dieudonné modules:

$$0 \to \mathbb{D}(A[\mathrm{Ver}]) \to \mathbb{D}(A[p]) \xrightarrow{\mathcal{F}} \mathbb{D}(A[\mathrm{Fr}]) \to 0.$$

Due to this exact sequence, the set S is a disjoint union of S^0 and S^1, where S^0 and S^1 are the classes of irreducible representations that occur in $\mathbb{D}(A[\mathrm{Ver}])$ and $\mathbb{D}(A[\mathrm{Fr}])$, respectively.

Let S^1 be a CM type of $\mathcal{A}$ and S^0 be the conjugation of the CM type. Based on these data, we can draw a graph of a circular word for BT_1 of an abelian variety A over $\bar{\mathbb{F}}_p$. The vertices of Γ are the classes G/Δ and there is an arrow between a class $[\alpha] \in G/\Delta$ and $[\sigma\alpha]$, where σ is a generator of the decomposition group. The arrow $[\alpha] \to [\sigma\alpha]$ is labeled by $\mathcal{V}$ if $[\alpha] \in S^1$; otherwise, $[\sigma\alpha] \to [\alpha]$ is labeled by $\mathcal{F}$.

5. Algorithm description

5.1. **Algorithm.** For convenience, we introduce a notion for characterizing the decomposition of a prime number p in a CM field K.

Definition 5.1. *A pair of non-negative integers (α, β) is called the **decomposition type** of p if*

$$p\mathcal{O}_K = \mathcal{P}_1 \dots \mathcal{P}_\alpha$$

and

$$p\mathcal{O}_{K_0} = \mathcal{Q}_1 \dots \mathcal{Q}_\beta,$$

where K_0 a totally real subfield of K and $\mathcal{P}_i \subset \mathcal{O}_K, \mathcal{Q}_j \subset \mathcal{O}_{K_0}$ are prime ideals (not necessarily distinct).

Next, for a given Galois group $G = \mathrm{Gal}(\tilde{K}/\mathbb{Q})$ and decomposition type (α, β) of prime p, we describe an algorithm that provides all possible non-isomorphic decompositions of the group scheme $\mathrm{A}[p]$. According to the results given in the previous section, it is sufficient to describe the actions of $\mathcal{F}$ and $\mathcal{V}$ on the proper subspaces of the module $\mathbb{D}(A[p])$.

Using pseudocode, the algorithm below can be written as follows.

Algorithm 1

```
G = Gal(K̃/ℚ)
ιList ← GetInvolutions(G)
for all ι ∈ ιList do
    DeltaList ← GetDeltaSubgroups(G, ι)
    for all Δ ∈ DeltaList do
        H0 ← GetH0Subgroup(G, ι, Δ)
        CMTypesList ← GetCMTypes(G, ι, Δ)
        for all S¹ ∈ CMTypesList do
            for all σ ∈ G do
                α ← |Δ \ G/⟨σ⟩|
                β ← |H0 \ G/⟨σ⟩|
                Words ← GetWords(G, ι, Δ, S¹, σ)
                Print:  (α, β) ⟶ Words
            end for
        end for
    end for
end for
```

The algorithm is implemented in the GAP computer algebra system and it can be found in [14].

The algorithm begins with the selection of an involution ι from the center of G. The element ι induces a complex conjugation of the CM field K. Then, according to the main theorem in Galois theory, the field K corresponds to a subgroup $\Delta \subset G$ of order $|G|/(2g)$ that does not contain ι. Moreover, Δ is a normal subgroup in G if and only if $\Delta = \langle 1 \rangle$, i.e., when $K/\mathbb{Q}$ is Galois.

Denote H_0 as a subgroup of G corresponding to the subfield $K_0 \subset K$. The subgroup H_0 is the smallest subgroup that contains ι and Δ. Next, we select a primitive CM-type S^1 from all the CM-types that arise from a given G, ι, and

Δ. The pair (K, S^1) corresponds to the unique simple abelian variety A over K, and vice versa. Finally, we need to choose a prime ideal $\tilde{\mathcal{P}} \subset \mathcal{O}_{\tilde{K}}$ in order to establish correspondences between the decomposition types of $p = \tilde{\mathcal{P}} \cap \mathbb{Z}$ in K and decompositions of the group scheme A$[p]$. In this case, it is sufficient to fix the decomposition group $\mathcal{D}$ of the ideal $\tilde{\mathcal{P}}$, which is a cyclic subgroup of G.

5.2. **Main Result.** We applied the algorithm in order to explicitly obtain a full table of all the possible decompositions of the scheme A$[p]$ with the given decomposition type (α, β) of prime p in a CM field K for dimensions $g = 1, 2, 3, 4, 5$.

It is known that for any $g > 0$, there are only a finite number of possible Galois groups $G = \mathrm{Gal}(\tilde{K}/\mathbb{Q})$ such that $\tilde{K}$ is a Galois closure of a CM field K of dimension $2g$ over $\mathbb{Q}$. A previous study [2] provided complete lists of these groups for $g \leq 7$. Therefore, we applied the algorithm to each group in the list to obtain the set of all possible decompositions of the scheme A$[p]$ corresponding to the decompositions of prime p that can arise for a simple abelian variety of a given dimension. We recall that the algorithm returns the decompositions of A$[p]$ as sets of circular words, so in order to obtain the final result, we employed the table at the end of Section 3.

A list of all the Galois groups arising for $\tilde{K}$ with K of dimension g is presented in the following table. For the sake of brevity, we denote the groups as given in the GAP computer algebra system. Thus, each group of order n is written as $G_{n,m}$, where m is the second index of the group in the GAP Small Groups Library.

$\dim \mathcal{A}$	$\lvert G\rvert$	groups list
2	2	$G_{2,1}$
4	4	$G_{4,1}$
	8	$G_{8,3}$
6	6	$G_{6,2}$
	12	$G_{12,4}$
	24	$G_{24,13}$
	48	$G_{48,48}$
8	8	$G_{8,1}$; $G_{8,2}$; $G_{8,3}$; $G_{8,4}$; $G_{8,5}$
	16	$G_{16,3}$; $G_{16,6}$; $G_{16,7}$; $G_{16,8}$; $G_{16,11}$; $G_{16,13}$
	24	$G_{24,3}$; $G_{24,13}$
	32	$G_{32,6}$; $G_{32,7}$; $G_{32,11}$; $G_{32,27}$; $G_{32,43}$; $G_{32,49}$
	48	$G_{48,29}$; $G_{48,48}$
	64	$G_{64,32}$; $G_{64,34}$; $G_{64,134}$; $G_{64,138}$
	96	$G_{96,204}$
	128	$G_{128,928}$
	192	$G_{192,201}$; $G_{192,1493}$
	384	$G_{384,5602}$
10	10	$G_{10,2}$
	20	$G_{20,4}$
	40	$G_{40,12}$
	120	$G_{120,35}$
	160	$G_{160,235}$
	240	$G_{240,189}$
	320	$G_{320,1636}$
	640	$G_{640,21536}$
	1920	$G_{1920,240997}$

	3840	$G_{2,1} \times G_{1920,240996}$

Let us examine the algorithm in more detail based on the following example. Let $g = 5$ and $G = \mathrm{Gal}(\tilde{K}/\mathbb{Q}) = G_{40,12}$. With accuracy up to an isomorphism, we can assume that G is generated by the permutations $(2,7)(3,4,8,9)$ and $(1,4,3,8)$ as a subgroup of order 40 of the symmetric group S_{10}.

The only non-trivial involution at the center of G is the permutation $\iota = (2,7)$.

Only 10 subgroups of G are suitable to serve as Δ. However, up to an automorphism of G that preserves ι, there is only one such subgroup. Therefore, we consider the subgroup $\langle\delta\rangle$ as Δ, where $\delta = (3,4,8,9)$ has order 4 in G. Thus, the H_0 subgroup is generated by the elements ι and δ.

The quotient $\Delta \setminus G$ comprises the following.

$$\{\Delta, \Delta(2,7), \Delta(1,3)(4,8), \Delta(1,3)(2,7)(4,8), \Delta(1,4,9,3), \Delta(1,4,9,3)(2,7),$$
$$\Delta(1,8,9,4,3), \Delta(1,8,9,4,3)(2,7), \Delta(1,9,8,3), \Delta(1,9,8,3)(2,7)\}$$

We can construct 32 CM-types from the elements of this set, but only 16 of them are not pairwise conjugated. In addition, there is one primitive CM-type in this set and we do not need to examine it. Furthermore, if we consider only the CM-types that are not translated into each other by the automorphisms of G, then only 5 different CM-types need to be considered, as follows:

(A) $S^1 = \{\Delta, \Delta(1,3)(4,8), \Delta(1,4,9,3), \Delta(1,8,9,4,3), \Delta(1,9,8,3)(2,7)\}$;
(B) $S^1 = \{\Delta, \Delta(1,3)(4,8), \Delta(1,4,9,3), \Delta(1,8,9,4,3)(2,7), \Delta(1,9,8,3)(2,7)\}$;
(C) $S^1 = \{\Delta, \Delta(1,3)(4,8), \Delta(1,4,9,3)(2,7), \Delta(1,8,9,4,3), \Delta(1,9,8,3)(2,7)\}$;
(D) $S^1 = \{\Delta, \Delta(1,3)(4,8), \Delta(1,4,9,3)(2,7), \Delta(1,8,9,4,3)(2,7), \Delta(1,9,8,3)(2,7)\}$;
(E) $S^1 = \{\Delta, \Delta(1,3)(2,7)(4,8), \Delta(1,4,9,3)(2,7), \Delta(1,8,9,4,3)(2,7), \Delta(1,9,8,3)(2,7)\}$.

Finally, with G, $\Delta \setminus G$, and S^1, we constructed the correspondence

$$(\alpha, \beta) \to {}^*\textit{set of circular words}^*$$

for each element $\sigma \in G$ using the explicit formulae in the algorithm and at the end of Section 4. The following table was obtained.

ideal decomposition	circular words
$\mathcal{P}$	$[\mathcal{FFFFFVVVVV}]$
	$[\mathcal{FFVVFVVFFV}]$
	$[\mathcal{FFFVFVVVFV}]$
$\mathcal{P}\mathcal{P}^c$	$[\mathcal{FFFFV}], [\mathcal{VVVVF}]$
	$[\mathcal{FFFVV}], [\mathcal{VVVFF}]$
	$[\mathcal{FFVFV}], [\mathcal{VVFVF}]$
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2$	$[\mathcal{FV}], [\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}]$
	$[\mathcal{FFFV}], [\mathcal{VVVF}], [\mathcal{FV}]$
	$[\mathcal{FFVV}], [\mathcal{FFVV}], [\mathcal{FV}]$
	$[\mathcal{FV}], [\mathcal{FV}], [\mathcal{FV}], [\mathcal{FV}], [\mathcal{FV}]$
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c$	$[\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}]$
	$[\mathcal{FFFV}], [\mathcal{VVVF}], [\mathcal{F}], [\mathcal{V}]$
	$[\mathcal{FFVV}], [\mathcal{FFVV}], [\mathcal{F}], [\mathcal{V}]$
	$[\mathcal{FV}], [\mathcal{FV}], [\mathcal{FV}], [\mathcal{FV}], [\mathcal{F}], [\mathcal{V}]$

$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3$	$[\mathcal{FV}], [\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}]$
	$[\mathcal{FV}], [\mathcal{FV}], [\mathcal{FV}], [\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}]$
	$[\mathcal{FV}], [\mathcal{FV}], [\mathcal{FV}], [\mathcal{FV}], [\mathcal{FV}]$
$\mathcal{P}_1\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4\mathcal{P}_5$	$[\mathcal{FV}], [\mathcal{FV}], [\mathcal{FV}], [\mathcal{FV}], [\mathcal{FV}]$
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3\mathcal{P}_3^c$	$[\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}]$
	$[\mathcal{FV}], [\mathcal{FV}], [\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}]$
	$[\mathcal{FV}], [\mathcal{FV}], [\mathcal{FV}], [\mathcal{FV}], [\mathcal{F}], [\mathcal{V}]$
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3\mathcal{P}_3^c\mathcal{P}_4\mathcal{P}_4^c\mathcal{P}_5\mathcal{P}_5^c$	$[\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}], [\mathcal{F}], [\mathcal{V}]$

Thus, by applying the algorithm to all of the Galois groups from the list above and by replacing the sets of circular words with the quasi-polarized BT_1-group schemes, we obtained the following correspondences between the decomposition types of the prime p and decompositions of the scheme $\mathrm{A}[p]$.

5.2.1. *Replication of the results given by* [13] *for* $g = 1, 2, 3$.

ideal decomposition	group scheme decomposition	p-rank	a-number
Dimension 1			
$\mathcal{P}$	$\mathrm{I}_{1,1}$	0	1
$\mathcal{P}\mathcal{P}^c$	$\mu_p \times \mathbb{Z}/p\mathbb{Z}$	1	0
Dimension 2			
$\mathcal{P}$	$\mathrm{I}_{2,1}$	0	1
$\mathcal{P}\mathcal{P}^c$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2$	2	0
	$\mathrm{I}_{1,1}^2$	0	2
$\mathcal{P}_1\mathcal{P}_2$	$\mathrm{I}_{1,1}^2$	0	2
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{1,1}$	1	1
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2$	2	0
Dimension 3			
$\mathcal{P}$	$\mathrm{I}_{3,1}$	0	1
	$\mathrm{I}_{1,1}^3$	0	3
$\mathcal{P}\mathcal{P}^c$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^3$	3	0
	$\mathrm{I}_{3,2}$	0	2
$\mathcal{P}_1\mathcal{P}_2$	$\mathrm{I}_{1,1} \times \mathrm{I}_{2,1}$	0	2
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{1,1}$	2	1
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{2,1}$	1	1
	$\mathrm{I}_{1,1}^3$	0	3
$\mathcal{P}_1\mathcal{P}_2\mathcal{P}_3$	$\mathrm{I}_{1,1}^3$	0	3
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^3$	3	0
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{1,1}^2$	1	2
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_3$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{1,1}^2$	1	2
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{1,1}$	2	1
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3\mathcal{P}_3^c$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^3$	3	0

5.2.2. *A new result for* $g = 4$.

ideal decomposition	group scheme decomposition	p-rank	a-number
$\mathcal{P}$	$\mathrm{I}_{4,1}$	0	1
	$\mathrm{I}_{4,3}$	0	3
$\mathcal{P}\mathcal{P}^c$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^4$	4	0
	$\mathrm{I}_{4,2}$, $\mathrm{I}_{2,1}^2$	0	2
	$\mathrm{I}_{1,1}^4$	0	4
$\mathcal{P}_1\mathcal{P}_2$	$\mathrm{I}_{1,1} \times \mathrm{I}_{3,1}$, $\mathrm{I}_{2,1}^2$	0	2
	$\mathrm{I}_{1,1}^4$	0	4
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^3 \times \mathrm{I}_{1,1}$	3	1
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{2,1}$	2	1
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{3,1}$	1	1
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{1,1}^3$	1	3
	$\mathrm{I}_{1,1} \times \mathrm{I}_{3,2}$, $\mathrm{I}_{1,1}^2 \times \mathrm{I}_{2,1}$	0	3
$\mathcal{P}_1\mathcal{P}_2\mathcal{P}_3$	$\mathrm{I}_{1,1}^2 \times \mathrm{I}_{2,1}$	0	3
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^4$	4	0
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{1,1}^2$	2	2
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{3,2}$	1	2
	$\mathrm{I}_{1,1}^4$	0	4
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_3$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{1,1}^2$	2	2
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{1,1} \times \mathrm{I}_{2,1}$	1	2
	$\mathrm{I}_{1,1}^4$	0	4
$\mathcal{P}_1\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4$	$\mathrm{I}_{1,1}^4$	0	4
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^3 \times \mathrm{I}_{1,1}$	3	1
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{2,1}$	2	1
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{1,1}^3$	1	3
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{1,1}^3$	1	3
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3\mathcal{P}_3^c$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^4$	4	0
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{1,1}^2$	2	2
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3\mathcal{P}_4$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{1,1}^2$	2	2
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3\mathcal{P}_3^c\mathcal{P}_4$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^3 \times \mathrm{I}_{1,1}$	3	1
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3\mathcal{P}_3^c\mathcal{P}_4\mathcal{P}_4^c$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^4$	4	0

5.2.3. *A new result for $g = 5$.*

ideal decomposition	group scheme decomposition	p-rank	a-number
$\mathcal{P}$	$\mathrm{I}_{5,1}$	0	1
	$\mathrm{I}_{5,3}$, $\mathrm{J}_{5,3}$	0	3
	$\mathrm{I}_{1,1}^5$	0	5
$\mathcal{P}\mathcal{P}^c$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^5$	5	0
	$\mathrm{I}_{5,2}$, $\mathrm{J}_{5,2}$	0	2
	$\mathrm{I}_{5,4}$	0	4
$\mathcal{P}_1\mathcal{P}_2$	$\mathrm{I}_{1,1} \times \mathrm{I}_{4,1}$, $\mathrm{I}_{2,1} \times \mathrm{I}_{3,1}$	0	2
	$\mathrm{I}_{1,1} \times \mathrm{I}_{4,3}$, $\mathrm{I}_{1,1}^3 \times \mathrm{I}_{2,1}$	0	4
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^4 \times \mathrm{I}_{1,1}$	4	1
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^3 \times \mathrm{I}_{2,1}$	3	1
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{3,1}$	2	1
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{1,1}^3$	2	3

	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{4,1}$	1	1
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{4,3}$	1	3
	$\mathrm{I}_{1,1} \times \mathrm{I}_{4,2}$, $\mathrm{I}_{3,2} \times \mathrm{I}_{2,1}$, $\mathrm{I}_{1,1}^2 \times \mathrm{I}_{3,1}$, $\mathrm{I}_{1,1} \times \mathrm{I}_{2,1}^2$	0	3
	$\mathrm{I}_{1,1}^5$	0	5
$\mathcal{P}_1\mathcal{P}_2\mathcal{P}_3$	$\mathrm{I}_{1,1}^2 \times \mathrm{I}_{3,1}$, $\mathrm{I}_{1,1} \times \mathrm{I}_{2,1}^2$	0	3
	$\mathrm{I}_{1,1}^5$	0	5
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^5$	5	0
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^3 \times \mathrm{I}_{1,1}^2$	3	2
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{3,2}$	2	2
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{4,2}$, $(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{2,1}^2$	1	2
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{1,1}^4$	1	4
	$\mathrm{I}_{1,1}^2 \times \mathrm{I}_{3,2}$	0	4
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_3$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^3 \times \mathrm{I}_{1,1}^2$	3	2
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{1,1} \times \mathrm{I}_{2,1}$	2	2
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{1,1} \times \mathrm{I}_{3,1}$, $(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{2,1}^2$	1	2
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{1,1}^4$	1	4
	$\mathrm{I}_{1,1}^2 \times \mathrm{I}_{3,2}$, $\mathrm{I}_{1,1}^3 \times \mathrm{I}_{2,1}$	0	4
$\mathcal{P}_1\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4$	$\mathrm{I}_{1,1}^3 \times \mathrm{I}_{2,1}$	0	4
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^4 \times \mathrm{I}_{1,1}$	4	1
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^3 \times \mathrm{I}_{2,1}$	3	1
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{3,1}$	2	1
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{1,1}^3$	2	3
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{1,1} \times \mathrm{I}_{3,2}$, $(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{1,1}^2 \times \mathrm{I}_{2,1}$	1	3
	$\mathrm{I}_{1,1}^5$	0	5
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{1,1}^3$	2	3
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{1,1}^2 \times \mathrm{I}_{2,1}$	1	3
	$\mathrm{I}_{1,1}^5$	0	5
$\mathcal{P}_1\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4\mathcal{P}_5$	$\mathrm{I}_{1,1}^5$	0	5
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3\mathcal{P}_3^c$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^5$	5	0
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^3 \times \mathrm{I}_{1,1}^2$	3	2
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{3,2}$	2	2
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{1,1}^4$	1	4
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3\mathcal{P}_4$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^3 \times \mathrm{I}_{1,1}^2$	3	2
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{1,1} \times \mathrm{I}_{2,1}$	2	2
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{1,1}^4$	1	4
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4\mathcal{P}_5$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z}) \times \mathrm{I}_{1,1}^4$	1	4
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3\mathcal{P}_3^c\mathcal{P}_4$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^4 \times \mathrm{I}_{1,1}$	4	1
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^3 \times \mathrm{I}_{2,1}$	3	1
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{1,1}^3$	2	3
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3\mathcal{P}_4\mathcal{P}_5$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^2 \times \mathrm{I}_{1,1}^3$	2	3
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3\mathcal{P}_3^c\mathcal{P}_4\mathcal{P}_4^c$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^5$	5	0
	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^3 \times \mathrm{I}_{1,1}^2$	3	2
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3\mathcal{P}_3^c\mathcal{P}_4\mathcal{P}_5$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^3 \times \mathrm{I}_{1,1}^2$	3	2
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3\mathcal{P}_3^c\mathcal{P}_4\mathcal{P}_4^c\mathcal{P}_5$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^4 \times \mathrm{I}_{1,1}$	4	1
$\mathcal{P}_1\mathcal{P}_1^c\mathcal{P}_2\mathcal{P}_2^c\mathcal{P}_3\mathcal{P}_3^c\mathcal{P}_4\mathcal{P}_4^c\mathcal{P}_5\mathcal{P}_5^c$	$(\mu_p \times \mathbb{Z}/p\mathbb{Z})^5$	5	0

References

[1] C. Blake. *A Deuring criterion for Abelian varieties.* Bulletin of the London Mathematical Society, 46(6):1256–1263, 2014.

[2] B. Dodson. *The structure of Galois groups of CM-fields.* Trans. Am. Math. Soc., 283:1–32, 1984.

[3] T. Ekedahl. *On supersingular curves and Abelian varieties.* Math. Scand., 60:151–178, 1987.

[4] Eyal Z. Goren. *On certain reduction problems concerning Abelian surfaces.* Manuscr. Math., 94(1):33–43, 1997.

[5] H. Kraft. *Kommutative Algebraische p-Gruppen (mit Anwendungen auf p-divisible Gruppen und abelsche Varietäten).* Sonderforsch. Bereich Bonn. 1975.

[6] S. Lang. *Elliptic Functions.* 1987.

[7] J. Milne. *Complex multiplication.* 2006.

[8] P. Moree. *The formal series Witt transform.* Discrete Mathematics, 295(1–3):143–160, 2005.

[9] F. Oort. *Simple p-kernels of p-divisible groups.* Adv. Math., 198(1):275–310, 2005.

[10] R. Pink. *Finite Group Schemes.* 2004/05. http://www.math.ethz.ch/ pink/FiniteGroupSchemes.html.

[11] R. Pries. *A short guide to p-torsion of Abelian varieties in characteristic p.* 2006/09. http://arxiv.org/abs/math/0609658v1.

[12] K.-I. Sugiyama. *On a generalization of Deuring's results* Finite Fields and their Applications, 26:69–85, 2014.

[13] A. Zaytsev. *Generalization of Deuring reduction theorem.* Journal of Algebra, 2012.

[14] Source code of the program[1]: *https://github.com/asmirnov1005/crtav.*

E-mail address: asmirnov1005@gmail.com, al.zaytsev@skoltech.ru

Skolkovo Institute of Science and Technology, Nobelya Ulitsa 3. Moscow, Russia

[1] Tested in GAP v4.8.6.