

COMPOSITIO MATHEMATICA

SAMUEL P. WHITE

Sporadic cycles on CM abelian varieties

Compositio Mathematica, tome 88, n° 2 (1993), p. 123-142

http://www.numdam.org/item?id=CM_1993__88_2_123_0

© Foundation Compositio Mathematica, 1993, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (<http://http://www.compositio.nl/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

Sporadic cycles on CM abelian varieties

SAMUEL P. WHITE

University of Texas, Austin, TX 78712, U.S.A.

Received 4 July 1990; accepted 20 July 1992

1. Introduction

Let A be an abelian variety of dimension d with complex multiplication by a CM-field K of degree $2d$. The Mumford-Tate group M_A is a subgroup of K^* thought of as a torus over \mathbb{Q} . Consider the following two conditions

- (i) $\dim(M_A) = d + 1$,
- (ii) The ring of Hodge cycles on A is generated by classes of divisors.

In a paper by Pohlmann ([2], Theorem 1) there is an explicit criterion on the sets $g\bar{S}$, $g \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ (where (K, \bar{S}) is the CM-type of A) for which the divisor classes in $H^{1,1}(A, \mathbb{C}) \cap H^2(A, \mathbb{Q})$ do not generate the Hodge ring on A . The criterion of Pohlmann immediately shows that (i) implies (ii). Between 1977 and 1978, K. Ribet asked whether (i) and (ii) were equivalent. H. W. Lenstra, Jr., quickly showed that the conditions were indeed equivalent under the supplementary hypothesis that K is abelian over \mathbb{Q} (see Theorem 3). The purpose of this article is to construct an explicit example giving a negative answer to the general question; namely there exists a CM abelian variety not satisfying (i) but satisfying (ii).

We start with some definitions. A *CM-field* K is a totally complex field of degree two over a totally real field K_0 . We assume K is of degree $2d$ and that K is a (maximal) subfield of $\text{End}(A) \otimes \mathbb{Q}$ for some CM abelian variety A of degree d . Let L be the Galois closure of K and put $G = \text{Gal}(L/\mathbb{Q})$, $H = \text{Gal}(L/K)$. The group G has a natural left action on the field K which identifies the embeddings of K with G/H and the distinguished involution c induced by complex conjugation acts on G/H . A *CM-type* is a pair (K, \bar{S}) , where $\bar{S} = \{\sigma_1, \dots, \sigma_d\} \subset G/H$ is a choice of representatives for the action of c . Define $\Psi: K \rightarrow \mathbb{C}^d$ by $\Psi(x) = (\sigma_1 x, \dots, \sigma_d x)$. An abelian variety A defined over \mathbb{C} is of CM-type (K, \bar{S}) if $A \cong \mathbb{C}^n/\Psi(L)$ for some lattice L in K (rank $2d$ over \mathbb{Q}) and if the action of K on A is induced by Ψ .

Let A be any abelian variety of CM-type (K, \bar{S}) . From Pohlmann's paper ([2],

Theorem 1) on algebraic cycles, subsets $\Delta \subset G/H$ such that

- (a) $\Delta - c\Delta \neq 0$,
- (b) $\forall g |\Delta \cap g\bar{S}| = p$

correspond to one dimensional \mathbb{C} -vector spaces (“lines”) in

$$H^{p,p}(A, \mathbb{C}) \cap H^{2p}(A, \mathbb{Q}) \otimes \mathbb{C} \subseteq H^{p,p}(A, \mathbb{C})$$

which are not generated by cup products from $H^{1,1}(A, \mathbb{C}) \cap H^2(A, \mathbb{Q}) \otimes \mathbb{C}$. We call such subsets *sporadic*. Clearly condition (ii) for any abelian variety A of CM-type (K, \bar{S}) is equivalent to the absence of any sporadic Δ . We prove the following theorem.

THEOREM 1. *There exists a CM-type (K, \bar{S}) with no sporadic subsets Δ whose Mumford-Tate group has rank less than $d + 1$.*

In fact we construct a specific counterexample with K Galois with Galois group $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times D_5$. The construction is reduced to finding a zero divisor of $\mathbb{Q}[G]$ with the correct properties. We review the cohomology theory of A and define the Mumford-Tate group, showing the rank is the rank of an easily computed submodule of the group ring $\mathbb{Q}[G]$.

2. The cohomology

This section reviews without proof some of the basic facts about the cohomology of abelian varieties. Let $V = \mathbb{C}^d$ and assume $A \cong V/\Lambda$ where Λ is a rank $2d$ \mathbb{Z} -lattice in \mathbb{C}^d . Elementary topology tells us that $H_1(A, \mathbb{Z}) = \Lambda$ and it is not hard to verify that

$$H^1(A, \mathbb{Q}) = \text{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Q})$$

and

$$H^1(A, \mathbb{C}) = \text{Hom}_{\mathbb{R}}(V, \mathbb{C})$$

respectively. The equality $V = \Lambda \otimes \mathbb{R}$ extends maps $\phi: \Lambda \rightarrow \mathbb{Q}$ uniquely to \mathbb{R} -linear maps $\phi: V \rightarrow \mathbb{C}$. This defines an injection of $H^1(A, \mathbb{Q})$ into $H^1(A, \mathbb{C})$. Define $U = \text{Hom}_{\mathbb{C}}(V, \mathbb{C})$, then there is a natural decomposition

$$H^1(A, \mathbb{C}) = \text{Hom}_{\mathbb{R}}(V, \mathbb{C}) = U \oplus \bar{U} \tag{1}$$

where \bar{U} are the complex conjugate maps, e.g. $\bar{\phi} \in \bar{U}$ if $\bar{\phi}(\lambda \mathbf{x}) = \bar{\lambda} \bar{\phi}(\mathbf{x})$ for all $\mathbf{x} \in V$, $\lambda \in \mathbb{C}$.

The higher cohomology groups are generated by wedge products of the first cohomology group. Thus

$$H^n(A, \mathbb{Q}) = \bigwedge^n H^1(A, \mathbb{Q})$$

and

$$H^n(A, \mathbb{C}) = \bigwedge^n H^1(A, \oplus).$$

Again there is a natural inclusion $H^n(A, \mathbb{Q})$ into $H^n(A, \mathbb{C})$. The image elements by this inclusion are called *rational cycles*. The decomposition $H^1(A, \mathbb{C}) = U \oplus \bar{U}$ induces a decomposition

$$H^n(A, \mathbb{C}) = \bigoplus_{p+q=n} H^{p,q}$$

where $H^{p,q} = \wedge^p U \otimes \wedge^q \bar{U}$. Define,

$$H^{p,q}(A, \mathbb{Q}) = H^{p,q}(A, \mathbb{C}) \cap H^{p+q}(A, \mathbb{Q}).$$

In particular, elements of $H^{p,p}(A, \mathbb{Q})$ are commonly called *Hodge cycles*. If X is codimension p subvariety of A , then X corresponds naturally to a cycle in $H^{p,p}(A, \mathbb{Q})$. These cycles are called *algebraic cycles*. The Hodge conjecture states that the algebraic cycles span $H^{p,p}(A, \mathbb{Q})$. Of course for $p = 1$, it is well known that $H^{1,1}(A, \mathbb{Q})$ is spanned by the image of divisors. It is the case $p > 1$ which is of interest.

The cohomology groups $H^n(A, \mathbb{Q})$ and $H^n(A, \mathbb{C})$ have a natural cup product structure induced by the wedge product, $\alpha \cap \beta = \alpha \wedge \beta$. For example, the group $\bigoplus_{p=1}^d H^{p,p}(A, \mathbb{Q})$ combined with this cup product structure is commonly known as the *Hodge ring*. Under cup products $H^{1,1}$ generates $H^{p,p}$. The question is: when does $H^{1,1}(A, \mathbb{Q})$ generate $H^{p,p}(A, \mathbb{Q})$? We may not be able to answer this question in general but we do get an obvious definition. A Hodge cycle in $H^{p,p}$ is *sporadic* if it is not generated from $H^{1,1}(A, \mathbb{Q})$. If we assume A is of CM-type (K, \bar{S}) then Pohlmann ([2], Theorem 1) proves sporadic subsets with p elements exist if and only if sporadic cycles in $H^{p,p}$ exist. So sporadic subsets for CM abelian varieties can be characterized in terms of their CM-type (K, \bar{S}) . As a side remark, since cup products of algebraic cycles correspond to intersections of algebraic varieties, if A has no sporadic cycles then the Hodge conjecture holds for A .

3. The Mumford-Tate group

Let $W = H_1(A, \mathbb{Q})$ and $W^* = \text{Hom}(W, \mathbb{Q}) \cong H^1(A, \mathbb{Q})$. The space $W_{\mathbb{C}} = W \otimes \mathbb{C}$ decomposes into

$$W_{\mathbb{C}} = V \oplus \bar{V}$$

where $\lambda \cdot x = \bar{\lambda}x$ for $\lambda \in \mathbb{C}$ and $x \in \bar{V}$. Define $t \in V$ to have bidegree $(-1, 0)$ and $t \in \bar{V}$ to have bidegree $(0, -1)$. Given any \mathbb{Q} -vector space of the form

$$D = W^{\otimes m} \otimes W^{*\otimes n} \quad (m, n \geq 0)$$

this definition induces a natural bidegree structure on

$$D_{\mathbb{C}} = W_{\mathbb{C}}^{\otimes m} \otimes W_{\mathbb{C}}^{*\otimes n}.$$

Let $D_{\mathbb{C}}^{r,s} \subseteq D_{\mathbb{C}}$ consist of elements of bidegree (r, s) and define

$$D^{r,s} = D \cap D_{\mathbb{C}}^{r,s}.$$

Any element $\alpha \in GL(W)$ induces an action on D . We say α is a *Hodge invariant* if there exists $\lambda \in \mathbb{Q}^*$ such that for every D and nonempty $D^{p,p}$ ($p \in \mathbb{Z}$)

$$\alpha z = \lambda^{-p} z \quad \forall z \in D^{p,p}.$$

The subgroup of Hodge invariants in $GL(W)$ is the *Mumford-Tate group* M_A .

If A is polarizable (admits an embedding into projective space), then by Deligne ([1], Proposition 3.4) M_A is an algebraic group over \mathbb{Q} . In this case, we can characterize the Mumford-Tate group by its action on the (p, p) part of the cohomology of the powers A^n of A . We give details below.

To be polarizable means there exists a bilinear form

$$E: V \otimes V \rightarrow \mathbb{R}$$

satisfying

- (a) $E(x, y) = -E(y, x)$,
- (b) $E(ix, y) = -E(x, iy)$,
- (c) $E(x, y) \in \mathbb{Z}$ if $x, y \in \Lambda$,
- (d) E is non-degenerate, i.e. $\det E \neq 0$.

The \mathbb{Q} -module W is canonically isomorphic to the submodule $\Lambda \otimes \mathbb{Q}$ in V and

thus E defines an alternating form

$$E: W \otimes W \rightarrow \mathbb{Q}.$$

This alternating form extends naturally to a non-degenerate skew Hermitian form

$$S: W_{\mathbb{C}} \otimes W_{\mathbb{C}} \rightarrow \mathbb{C}$$

by using the relation

$$S(x \otimes \alpha, y \otimes \beta) = \alpha \bar{\beta} E(x, y)$$

for $x \otimes \alpha, y \otimes \beta \in W \otimes \mathbb{C} = W_{\mathbb{C}}$. (The form $iS|_V$ is the usual hermitian form H on V). It is simple to verify that

$$S(V, \bar{V}) = 0$$

so the isomorphism

$$W \rightarrow W^*$$

induced by E preserves the bidegree structure. In other words, algebraic elements of bidegree (p, p) (note that $2p = n - m$) in

$$D = W^{\otimes m} \otimes W^{*\otimes n}$$

correspond “naturally” by E to algebraic elements of bidegree $(p + m, p + m)$ in

$$D = W^{*\otimes m+n}.$$

But $W^{*\otimes n}$ embeds naturally into $H^n(A^n, \mathbb{Q})$. Conversely every cohomology group $H^r(A^n, \mathbb{Q})$ embeds into $\bigoplus_{i=1}^n W^{*\otimes r}$. Thus the spaces D can be substituted by the cohomology groups $H^r(A^n, \mathbb{Q})$ when calculating M_A . An element α in $GL(W)$ is a Hodge invariant if and only if there exists $\lambda \in \mathbb{Q}^*$ such that for every $n > 0$,

$$\alpha x = \lambda^{-p} x \quad \text{whenever } x \in H^{p,p}(A^n, \mathbb{Q}).$$

Hence, M_A is the algebraic subgroup of $GL(W)$ that acts as scalars on the Hodge ring of the powers of A .

Now assume A is of CM-type (K, \bar{S}) . Then K^* has natural action on $W \cong \Lambda \otimes \mathbb{Q}$ giving an injection of K^* into $GL(W)$. Furthermore the CM-type (K, \bar{S}) induces a natural polarization

$$E(x, y) = \text{Tr}_{K/\mathbb{Q}} \beta x \bar{y}$$

where β is any totally imaginary element of K . We will describe M_A explicitly. For example, the description will imply that $M_A \subseteq K_{\mathbb{Q}}^*$ where $K_{\mathbb{Q}}^* = \{x \mid x \in K^*, x\bar{x} \in \mathbb{Q}\}$, with equality only if M_A is maximal. In particular M_A is an algebraic subgroup of K^* , i.e. a torus.

Let S be the inverse image of \bar{S} in G . Assume that the pair (K, \bar{S}) is simple, which means we have the equality

$$H = \{g \in G \mid Sg = S\}.$$

It is an exercise to show that (K, \bar{S}) is simple if and only if every sporadic Δ (see Definition in Section 1) satisfies

$$|\Delta| > 2.$$

Of course this means that any CM-type satisfying the conditions of Theorem 1 is simple.

Let $T = S^{-1}$ (the set of inverses of elements of S), and set

$$H' = \{g \in G \mid Tg = T\} = \{g \in G \mid gS = S\}.$$

Let F be the fixed field of H' and \bar{T} the image of T in G/H' . Then F is a CM field, and (F, \bar{T}) is a CM-type, called the dual type (i.e. dual to (K, \bar{S})). The groups K^* and F^* can be thought of as tori over \mathbb{Q} . If we let T_K and T_F denote these algebraic groups, we can define an algebraic morphism $N_{\bar{T}}: T_F \rightarrow T_K$ by the formula

$$N_{\bar{T}}(x) = \prod_{\sigma \in \bar{T}} \sigma x.$$

THEOREM 2. *The image of $N_{\bar{T}}$ is the Mumford-Tate group of A .*

Proof. Too involved to prove here. See Deligne ([1], Example 3.7) for a computation of M_A in terms of cocharacters. □

In this paper we are only interested in the rank of M_A . Since computing the rank of the image of $N_{\bar{T}}$ directly is difficult, we compute the rank of the pull-back $N_{\bar{T}}^*$ on the duals instead.

The character groups X_K and X_F on T_K and T_F are just the free abelian

groups on the embeddings of K and F respectively (see Serre [4]). In terms of characters, $N_{\bar{T}}$ induces a map $N_{\bar{T}}^*: X_K \rightarrow X_F$ given by the formula

$$g \rightarrow g \sum_{\sigma \in \bar{T}} \sigma.$$

Its image will have the same rank as M_A . We observe that the left $\mathbb{Q}[G]$ -submodule generated by the image of $N_{\bar{T}}^*$ in $X_K \otimes \mathbb{Q}$ is isomorphic to the submodule generated by T in $\mathbb{Q}[G]$ (we identify T with the formal sum of its elements as we do with all subsets of G). Thus the latter module's rank is the same as the rank of the Mumford-Tate group. Likewise the left $\mathbb{Q}[G]$ -submodule generated by S , or equivalently the right $\mathbb{Q}[G]$ -submodule generated by T , has the same rank as the rank of the Mumford-Tate group of the dual CM-type (F, \bar{T}) .

These are the submodules we use when computing the rank of the Mumford-Tate group. They are particularly tractable because they are submodules of a group ring. For example, this characterization makes it easy to prove the following result.

LEMMA 1. *The rank of the Mumford-Tate group of a CM-type and its dual is the same.*

Proof. Let M be the left $\mathbb{Q}[G]$ -submodule generated by T and N the right $\mathbb{Q}[G]$ -submodule generated by T . We show that $\text{rank}(M) = \text{rank}(N)$. The rank of M and N do not change if we tensor with any algebraically closed field, say \mathbb{C} for example. But $\mathbb{Q}[G] \otimes \mathbb{C} = \mathbb{C}[G] = \bigoplus V_i$ where each $V_i \cong M(n_i)$ is a matrix algebra over \mathbb{C} . Thus $T = \sum T_i$ with each $T_i \in V_i$. The rank of the left (right) $\mathbb{C}[G]$ -submodule generated by T is the sum of the ranks of the left (right) $\mathbb{C}[G]$ -submodules generated by T_i in V_i . But T_i lies inside a $M(n_i)$, so by simple linear algebra the left and right $\mathbb{Q}[G]$ -submodules generated by T_i have the same rank. Therefore $\text{rank}(M) = \text{rank}(N)$. □

In the future we use the left $\mathbb{Q}[G]$ -submodule M generated by S when computing the rank of the Mumford-Tate group. We have the following nice condition for when M is maximal. Let

$$M_0 = \{x \mid x \in \mathbb{Q}[G], x + cx = qt_G, q \in \mathbb{Q}\}$$

where $t_G = \sum_{g \in G} g$ is the trace element and define

$$\bar{M}_0 = \{x \mid x \in M_0, xh = x \forall h \in H\}.$$

Then $M \subseteq \bar{M}_0$ and M is of maximal rank, i.e. $\text{rank } M = \dim A + 1$, if and only if $M = \bar{M}_0$.

4. The case K Galois

Since we are trying to create a counterexample, a special case will do as well as the general case. Specifically assume K is Galois, or equivalently that H is trivial and $S = \bar{S}$, $M_0 = \bar{M}_0$.

We factor $\mathbb{Q}[G]$ as

$$\mathbb{Q}[G] = \mathbb{Q}[G]^+ \oplus \mathbb{Q}[G]^-$$

where

$$\mathbb{Q}[G]^+ = (1+c)\mathbb{Q}[G], \quad \mathbb{Q}[G]^- = (1-c)\mathbb{Q}[G].$$

Note that the component of Δ and S in $\mathbb{Q}[G]^-$ are $\Delta - c\Delta$ and $S - cS$ respectively. Thus the two conditions for a sporadic Δ can be reinterpreted in the ring $\mathbb{Q}[G]^-$ as

- (a) $\Delta - c\Delta \neq 0$,
- (b) $(S - cS) \cdot (\Delta^{-1} - c\Delta^{-1}) = 0$ in $\mathbb{Q}[G]^-$.

We have converted the question of the existence of sporadic cycles into a question about the existence of certain zero divisors in a group ring. Any element of $\mathbb{Q}[G]^-$ whose coefficients are all ± 1 can be put in the form $S - cS$. Similarly, any element whose coefficients are $0, \pm 1$ can be put in the form $\Delta^{-1} - c\Delta^{-1}$. If the product of the two is zero then the elements correspond to a CM-type for which there exists a sporadic cycle. If no such $\Delta^{-1} - c\Delta^{-1}$ exists for a specific choice of $S - cS$ then the ring of Hodge cycles of any associated abelian variety A is generated by the classes of divisors.

However, if we consider higher powers A^n of A , a sporadic cycle on A^n would correspond to a right annihilator of $S - cS$ in $\mathbb{Q}[G]^-$ whose coefficients are $0, \pm 1, \dots, \pm n$. Thus if $S - cS$ is not a G -module generator of $\mathbb{Q}[G]^-$ or equivalently has a right annihilator then there exists a high enough power A^n such that A^n has a sporadic cycle.

This is particularly helpful because of the following lemma.

LEMMA 2. *Let (K, S) be a Galois CM-type with Galois group G and central involution c . The rank of the corresponding Mumford-Tate group is maximal if and only if $S - cS$ is a G -module generator of $\mathbb{Q}[G]^-$.*

Proof. Simple algebra shows that the condition $M = M_0 (= \bar{M}_0)$ is equivalent to the condition $\mathbb{Q}[G]^- (S - cS) = \mathbb{Q}[G]^-$. □

In particular if $\text{rank}(M_A) < d + 1$ then for some $n > 0$, there is a sporadic cycle on A^n . Our objective is to show $n = 1$ is not sufficient.

We need no longer concern ourselves with the theory of abelian varieties. Instead we can concentrate on the calculation of zero divisors in group rings. For instance, Lenstra’s result is a direct consequence of the following fact.

LEMMA 3. *If G is abelian, every submodule N of $\mathbb{Q}[G]^-$ has a nonzero element β whose coefficients are $0, \pm 1$.*

Proof. Since G is abelian

$$\mathbb{Q}[G]^- \otimes \mathbb{C} = \sum_{\substack{\chi \in \hat{G} \\ \chi(c) \neq 1}} \mathbb{C} \cdot e_\chi$$

where $e_\chi = \sum_{g \in G} \chi(g)g$. Because N is defined over \mathbb{Q} ,

$$\mathbb{C}e_\chi \subset N \otimes \mathbb{C} \Rightarrow \mathbb{C}e_{\chi'} \subset N \otimes \mathbb{C} \quad \text{if } \chi' \text{ conjugate to } \chi.$$

Let H be the kernel of χ . Let σ generate the cyclic group G/H and assume $\sigma^m = c$, $\sigma^{2m} = 1$. Then χ generates the character group of G/H and χ and χ' are conjugate $\Leftrightarrow (t, 2m) = 1$. Let

$$\hat{\beta} = \prod_{\substack{p|2m \\ p \text{ odd}}} (1 - c\sigma^{2m/p}).$$

Then if an odd χ' is not conjugate to χ then either $\chi'(\hat{\beta}) = 0$ or $\chi'(H) = 0$. In either case $\chi'(\hat{\beta}H) = 0$ which implies that if we let $\beta = \hat{\beta}H$,

$$\beta \in \sum_{\chi' \sim \chi} \mathbb{C}e_{\chi'} \subseteq N \otimes \mathbb{C}.$$

Furthermore, β has the appropriate coefficients since the order of a typical product $\sigma^{2n/p_1} \dots \sigma^{2n/p_t}$ is exactly $p_1 \dots p_t$, different for each product. This proves the lemma. □

THEOREM 3 (Lenstra). *Let (K, \bar{S}) be any simple CM-type, where K is a field with abelian Galois group. If A is any abelian variety of CM type (K, \bar{S}) then $\text{rank}(M) = \dim(A) + 1$ if and only if the ring of Hodge cycles on A is generated by classes of images of divisors.*

Proof. We need check only the case when $\text{rank}(M) < \dim(A) + 1$. By Lemma 2 this is equivalent to $S - cS$ not generating $\mathbb{Q}[G]^-$. If N is the nontrivial submodule generated by the right annihilators of $S - cS$ then by Lemma 3, there exists an element in N whose coefficients are $0, \pm 1$. This can be rewritten in the form $\Delta^{-1} - c\Delta^{-1}$ which gives us a “line” Δ containing a sporadic cycle on A . □

5. A group ring statement of our result

When G is not abelian, $\mathbb{Q}[G]^-$ may have submodules which do not contain an element with coefficients $0, \pm 1$. Our counterexample requires that there exist a group G and a CM-type S such that $S - cS$ does not generate $\mathbb{Q}[G]^-$ and such that no nonzero right annihilator of $S - cS$ has coefficients $0, \pm 1$. We simplify matters by assuming G is of the form $\mathbb{Z}/2\mathbb{Z} \times G_0$ where the $\mathbb{Z}/2\mathbb{Z}$ component corresponds to complex conjugation, i.e. $\mathbb{Z}/2\mathbb{Z} = \{1, c\}$. Note $\mathbb{Q}[G]^- \cong \mathbb{Q}[G_0]$ and our previous group ring conditions for a sporadic Δ are actually statements about the group ring $\mathbb{Q}[G_0]$. We summarize the equivalence between the Hodge ring statements and the group ring statements in the following proposition.

PROPOSITION 1. *Let K be a Galois complex multiplication field with Galois group $G = \mathbb{Z}/2\mathbb{Z} \times G_0$ where G_0 is the Galois group of the totally real subfield. Write every element of G as $c^i\sigma$ where $i = 0, 1$ and $\sigma \in G_0$. Define a map from subsets $U \subseteq G$ to $\mathbb{Q}[G_0]$ by*

$$\Phi: U \rightarrow \sum_{c^i\sigma \in U} (-1)^i \sigma.$$

The map Φ gives a bijection between CM-types S and elements $\alpha = \sum_{g \in G_0} a_g g$, $a_g \in \{\pm 1\}$. Let α be the image of any simple CM-type S . Then the following three conditions are equivalent.

1. *The divisor classes do not generate the Hodge ring of any abelian variety of CM-type (K, S) .*
2. *There exists a sporadic Δ .*
3. *There exists (nonzero) $\beta \in \mathbb{Q}[G_0]$ whose coefficients are ± 1 or 0 such that $\alpha \cdot \beta = 0$.*

In particular let $G_0 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times D_5$ where D_5 is the dihedral group of order 10. We will prove

THEOREM 4. *There exists a CM-type S such that $\mathbb{Q}[G_0]\alpha \neq \mathbb{Q}[G_0]$ and such that no (nonzero) β whose coefficients are ± 1 or 0 will satisfy $\alpha \cdot \beta = 0$.*

Since Theorem 4 involves only statements about S and the group ring $\mathbb{Q}[G_0]$, we will prove the theorem without any references to the field K . Later we will construct a complex multiplication field with Galois group

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times D_5$$

(the first component being complex conjugation). Obviously if such a field exists then Theorem 4 implies Theorem 1.

6. The general approach

Let G_0 be a non-abelian group. By the general theory of simple rings

$$\mathbb{Q}[G_0] = \bigoplus V_i \quad (V_i \text{ is a simple ring}).$$

For each i , V_i is a division ring or a matrix algebra over a division ring. Let $\alpha \in \mathbb{Q}[G_0]$, then

$$\alpha = \sum \alpha_i \quad \alpha_i \in V_i.$$

If $\alpha \cdot \beta = 0$ then $\beta = \sum \beta_i$ and $\alpha_i \cdot \beta_i = 0$ for each i . If $\beta_i \neq 0$ this means α_i is either zero or a matrix of less than full rank. Thus if we choose our α_i so that α_i is of full rank except for restricted subset of i , we can restrict the possibilities for the right $\mathbb{Q}[G_0]$ -module N of right annihilators of α . For example, with little difficulty we can guarantee that the right annihilators have no elements whose coefficients are all 0 or ± 1 . The problem is that α is not necessarily of the right form. To fix this we use the following general technique.

Remove the denominators in a_g from $\alpha = \sum a_g g$. Multiply the result by two and add or subtract the trace element $t_G = \sum_{g \in G_0} g$ to guarantee that all the coefficients are odd. If done correctly, this should not change the right annihilators of α . Let p be a prime. Create a larger group $\mathbb{Z}/p\mathbb{Z} \times G_0$. Then assuming $\mathbb{Z}/p\mathbb{Z} = \langle \tau \mid \tau^p = 1 \rangle$,

$$\begin{aligned} \mathbb{Q}[\mathbb{Z}/p\mathbb{Z} \times G_0] &= \tau^+ \mathbb{Q}[G_0] \oplus \tau^- \mathbb{Q}[\tau][G_0] \\ &\cong \mathbb{Q}[G_0] \oplus \mathbb{Q}[\omega_p][G_0] \end{aligned}$$

where $\tau^+ = 1 + \tau + \dots + \tau^{p-1}$ and $\tau^- = p - \tau^+$. We can create a new α' out of the old α as follows. Choose $\gamma_i \in \mathbb{Q}[G_0]$, $i = 0, \dots, p-1$, which satisfy the following two conditions.

1. $\alpha = \sum \gamma_i$,
2. the coefficients of each γ_i consist of entirely $+1$'s or -1 's.

If p is large enough, there will be ample choices for γ_i . Let $\alpha' = \sum_{i=0}^{p-1} \gamma_i \tau^i$. The projection of α' into $\tau^+ \mathbb{Q}[G_0]$ is equal to α and if we are lucky the projection of α' into $\tau^- \mathbb{Q}[\tau][G_0]$ will generate all of that ring. The odds are in our favour since “most” elements in any simple ring generate the ring. If that is the case then α' will have exactly the same zero divisors as α but will now be of the right form. This gives us our counterexample. This is not exactly the approach we follow but it is good to keep it in mind.

7. The decomposition of the group ring

Unfortunately the next three sections are somewhat technical. In order to construct a counterexample we must decompose $\mathbb{Q}[G_0]$ explicitly and verify by direct computation that “ α ” (see Propositions 2, 3 and 4 and Section 9) satisfies the properties wanted. Since G_0 is the semi-direct (and direct) product of cyclic subgroups, the decomposition is induced from the decompositions and (tensor) products of the cyclic factors. Over \mathbb{Q} some complexity is introduced by the repeated $\mathbb{Z}/5\mathbb{Z}$ factors (one inside D_5). The algebra $\mathbb{Q}[\mathbb{Z}/5\mathbb{Z}]$ is isomorphic to $\mathbb{Q} \oplus \mathbb{Q}[\omega]$ (ω is the fifth root of unity) but $\mathbb{Q}[\omega]$ is the splitting field for any further $\mathbb{Q}[\mathbb{Z}/5\mathbb{Z}]$ factors.

We assume $G_0 = \mathbb{Z}/2\mathbb{Z} \times H$ with $H = \mathbb{Z}/5\mathbb{Z} \times D_5$. Let σ generate the $\mathbb{Z}/2\mathbb{Z}$ component. Immediately,

$$\mathbb{Q}[G_0] = (\sigma + 1)\mathbb{Q}[H] \oplus (\sigma - 1)\mathbb{Q}[H]$$

so we are reduced to studying the decomposition of $\mathbb{Q}[H]$.

Let $F_5 = \mathbb{Z}/5\mathbb{Z} = \langle \tau \mid \tau^5 = 1 \rangle$ and $D_5 = \langle \rho, \gamma \mid \rho^2 = 1, \gamma^5 = 1, \rho\gamma\rho = \gamma^{-1} \rangle$. Decomposing $\mathbb{Q}[F_5]$ we have

$$\mathbb{Q}[F_5] = \tau_+ \mathbb{Q}[\tau] \oplus \tau_- \mathbb{Q}[\tau]. \tag{2}$$

where $\tau_+ = \sum_{i=0}^4 \tau^i/5$ and $\tau_- = 1 - \tau_+$ are the orthogonal idempotents. Note, $\tau_+ \mathbb{Q}[\tau] \cong \mathbb{Q}$ and if we map τ onto ω (a primitive 5th root of unity) $\tau_- \mathbb{Q}[\tau] \cong \mathbb{Q}[\omega]$. Define $x^+ = \tau_+ x$ and $x^- = \tau_- x$ for each $x \in \mathbb{Q}[H]$ and extend this notation to subsets of $\mathbb{Q}[H]$ (for example, $\mathbb{Q}^+ = \tau_+ \mathbb{Q}$ and $\mathbb{Q}^- = \tau_- \mathbb{Q}$). Then using (2) we have as a direct sum of rings,

$$\begin{aligned} \mathbb{Q}[H] &= \tau_+ \mathbb{Q}[\tau][D_5] \oplus \tau_- \mathbb{Q}[\tau][D_5] \\ &= \mathbb{Q}^+[D_5] \oplus \mathbb{Q}^-[\tau][D_5] \\ &\cong \mathbb{Q}[D_5] \oplus \mathbb{Q}[\omega][D_5]. \end{aligned} \tag{3}$$

Our intention is to decompose each factor into its simple ring components. For convenience we collect the symbols needed.

$$\begin{aligned} \tau_+ &= \sum_{n=0}^4 \tau^n/5, \tau_- = 1 - \tau_+ \quad \text{and} \quad x^+ = \tau_+ x, x^- = \tau_- x \quad \text{for } x \in \mathbb{Q}[H] \\ \gamma_i &= \sum_{n=0}^4 \tau^{ni} \gamma^n, \gamma_i^* = \sum_{n=1}^4 \tau^{ni} \gamma^n \quad (\text{i.e. } 1 + \gamma_i^* = \gamma_i) \\ \rho_+ &= 1 + \rho, \rho_- = 1 - \rho. \end{aligned}$$

Let V be spanned by the \mathbb{Q} -basis

$$\rho^i \gamma^j (1 - \gamma) \quad (i = 0, 1, j = 0, \dots, 3).$$

Then the first summand decomposes as

$$\mathbb{Q}[D_5] = \rho_+ \gamma_0 \mathbb{Q} \oplus \rho_- \gamma_0 \mathbb{Q} \oplus V. \tag{4}$$

The summands $\rho_+ \gamma_0 \mathbb{Q}$ and $\rho_- \gamma_0 \mathbb{Q}$ are one dimensional and V is a matrix algebra over $\mathbb{Q}[\gamma + \gamma^{-1}] \cong \mathbb{Q}[\sqrt{5}]$. For instance, V will decompose (non-uniquely) into a direct sum of the two irreducible left $\mathbb{Q}[H]$ -modules $V\rho_+$ and $V\rho_-$.

Tensoring (4) with $\mathbb{Q}^-[\tau]$,

$$\mathbb{Q}^-[\tau][D_5] = \rho_+ \gamma_0 \mathbb{Q}^-[\tau] \oplus \rho_- \gamma_0 \mathbb{Q}^-[\tau] \oplus \mathbb{Q}^-[\tau]V. \tag{5}$$

As before $\rho_+ \gamma_0 \mathbb{Q}^-[\tau]$ and $\rho_- \gamma_0 \mathbb{Q}^-[\tau]$ are one dimensional irreducible factors over $\mathbb{Q}^-[\tau] \cong \mathbb{Q}[\omega]$. However, V is now the direct sum of two matrix algebras F_1 and F_2 over $\mathbb{Q}^-[\tau]$. The algebras F_1 and F_2 decompose further as left $\mathbb{Q}[H]$ -modules but the decomposition is not unique. Set $K = \mathbb{Q}^-[\tau]$. One such decomposition is

$$F_1 = E_1 \oplus E_{-1}$$

$$F_2 = E_2 \oplus E_{-2}$$

where

$$E_1 = \gamma_1^- K \oplus \rho \gamma_1^- K \cong K^2$$

$$E_{-1} = \gamma_{-1}^- K \oplus \rho \gamma_{-1}^- K \cong K^2$$

$$E_2 = \gamma_2^- K \oplus \rho \gamma_2^- K \cong K^2$$

$$E_{-2} = \gamma_{-2}^- K \oplus \rho \gamma_{-2}^- K \cong K^2.$$

It is this decomposition which allows us to create our counterexample.

Even though the decomposition as $\mathbb{Q}[H]$ -modules is not unique, the ring $\mathbb{Q}[H]$ factors into unique simple ring components. It is worthwhile to give this decomposition.

PROPOSITION 2

$$\mathbb{Q}[H] = \tau_+(\rho_+ \gamma_0 \mathbb{Q} \oplus \rho_- \gamma_0 \mathbb{Q} \oplus V) \oplus \rho_+ \gamma_0^- K \oplus \rho_- \gamma_0^- K \oplus F_1 \oplus F_2$$

is the unique decomposition of $\mathbb{Q}[H]$ as simple rings.

Proof. This follows from (4) and (5). □

8. The creation of $\hat{\alpha}$

We construct an element $\hat{\alpha} \in \mathbb{Q}[H]$ whose coefficients are all ± 1 and whose right annihilators are sums of elements from $\tau_+ \rho_- V$ and F_1 . In the next section, we enlarge the group to G_0 and eliminate the contribution coming from $\tau_+ \rho_- V$. The remaining (nonzero) right annihilators in F_1 will have at least one coefficient not equal to 0, ± 1 . The $\hat{\alpha}$ derived here was obtained by trial and error. Since the process was somewhat laborious we give only the final result.

To start we represent every element of F_i ($i = 1, 2$) as a 2×2 matrix over K and find the zero divisors. Let $e_1 = \gamma_i^-, e_2 = \rho\gamma_i^-$ be a basis of E_i . Since $\gamma_i^- e_1 = 5e_1$ and $\gamma_i^- e_2 = \rho\gamma_i^- \gamma_i^- = 0$, the element γ_i^- corresponds to the matrix

$$\begin{bmatrix} 5 & 0 \\ 0 & 0 \end{bmatrix}.$$

Likewise $\rho\gamma_i^-, \gamma_i^-, \rho\gamma_i^-$ correspond to the matrices

$$\begin{bmatrix} 0 & 0 \\ 5 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 5 \end{bmatrix}, \begin{bmatrix} 0 & 5 \\ 0 & 0 \end{bmatrix}$$

respectively. This gives an isomorphism between $M_2(K)$ and F_i .

We are more interested in F_1 so set $i = 1$. Elements in $M_2(K)$ with right annihilators (the extra factor of 5 is for clarity of notation only) are the matrices

$$A(a, b, \phi, \zeta) = 5 \begin{bmatrix} \phi a & \phi b \\ \zeta a & \zeta b \end{bmatrix} \quad (\phi, \zeta \in K).$$

They correspond to $x(a, b, \phi, \zeta)$ in F_1 where

$$x(a, b, \phi, \zeta) = \phi(a\gamma_1^- + b\rho\gamma_1^-) + \zeta(a\rho\gamma_1^- + b\gamma_1^-). \tag{6}$$

The right annihilators of $A(a, b, \phi, \zeta)$ in $M_2(K)$ are

$$5 \begin{bmatrix} \phi' b & \zeta' b \\ -\phi' a & -\zeta' a \end{bmatrix} \quad (\phi', \zeta' \in K)$$

which correspond to $y(a, b, \phi', \zeta')$ in F_1 where

$$y(a, b, \phi', \zeta') = \phi'(b\gamma_1^- - a\rho\gamma_1^-) + \zeta'(b\rho\gamma_1^- - a\gamma_1^-). \tag{7}$$

Thus we have shown

LEMMA 4. *If $x \cdot y = 0$ in F_1 then $x = x(a, b, \phi, \zeta)$ and $y = y(a, b, \phi', \zeta')$ for some $a, b, \phi, \zeta, \phi', \zeta' \in K$.*

For the correct choice of a and b , the right annihilators have at least one coefficient not equal to zero or ± 1 . We start with a technical lemma.

LEMMA 5. *Let r, s be nonzero numbers such that $r \neq \pm s, r \neq \pm 2s, s \neq \pm 2r$ then $\{\delta_1 r + \delta_2 s \mid \delta_1, \delta_2 \in \{0, \pm 1\}\}$ has nine distinct elements.*

Proof. Easy computation. □

PROPOSITION 3. *Assume r and s are as in the lemma. If we set $y(-s, r, \phi, \zeta) = \sum_{g \in H} \rho_g g$ and assume $y(-s, r, \phi, \zeta) \neq 0$ then there exists g such that $\rho_g \notin \{0, \pm 1\}$.*

Proof. Assume $y(-s, r, \phi, \zeta)$ has coefficients in $\{0, \pm 1\}$. By (7)

$$y(-s, r, \phi, \zeta) = \phi(r\gamma_1^- + s\rho\gamma_1^-) + \zeta(r\rho\gamma_1^- + s\gamma_1^-).$$

But $\phi \in \mathbb{Q}^-[\tau] = K$ so $\phi\gamma_1^- = \phi\gamma_1$, likewise for the other terms so

$$y(-s, r, \phi, \zeta) = r\phi\gamma_1 + s\zeta\gamma_{-1} + \rho[s\phi\gamma_1 + r\zeta\gamma_{-1}].$$

Let

$$r\phi\gamma_1 + s\zeta\gamma_{-1} = \sum_{j=0, k=0}^4 c_{jk} \tau^j \gamma^k \tag{8}$$

$$s\phi\gamma_1 + r\zeta\gamma_{-1} = \sum_{j=0, k=0}^4 d_{jk} \tau^j \gamma^k \tag{9}$$

where by assumption $c_{jk}, d_{jk} \in \{0, \pm 1\}$. Take r times (8) and subtract s times (9),

$$(r^2 - s^2)\phi\gamma_1 = \sum_{j=0, k=0}^4 (rc_{jk} - sd_{jk})\tau^j \gamma^k.$$

Using

$$\gamma_1 = 1 + \tau\gamma + \dots + \tau^4\gamma^4, \quad \phi = \sum \phi_a \tau^a \quad \text{and} \quad \tau^5 = 1$$

an algebraic computation shows that $rc_{jk} - sd_{jk} = rc_{l0} - sd_{l0}$ where $l \equiv j - k \pmod{5}$. By Lemma 5, $c_{jk} = c_{l0}, d_{jk} = d_{l0}$. Multiplying (8) by s and subtracting

(9) times r and using the same reasoning we can show $c_{jk} = c_{m0}$, $d_{jk} = d_{m0}$ where $m \in F_5$, $m \equiv j + k \pmod{5}$. So $\forall j, k$ $c_{10} = c_{m0}$ and $d_{10} = d_{m0}$. It follows that $c_{00} = c_{j0}$ and $d_{00} = d_{j0}$ $j = 1, \dots, 4$. But $\sum_{j=0}^4 c_{j0} \tau^j \in \mathbb{Q}^-[\tau]$ so $\sum_{j=0}^4 c_{j0} = 0$ and so $c_{j0} = 0 \forall j$. Likewise $d_{j0} = 0 \forall j$. Thus (8) and (9) imply $r\phi \cdot 1 + s\zeta \cdot 1$ and $s\phi \cdot 1 + r\zeta \cdot 1$ are zero and therefore ϕ and ζ are zero. Contradiction. \square

Having done the ground work, we begin the creation of $\hat{\alpha}$. Note for future reference that

$$\gamma_i^- + \tau_+ \gamma_0 = \gamma_i, \quad \sum_{i=0}^4 \gamma_i^- = 5^- \quad (5^- = \tau_- 5), \quad \gamma_{5-i} = \gamma_{-i}. \quad (10)$$

We start with

$$\begin{aligned} x(a, b, 1, 1) &= a\gamma_1^- + b\rho\gamma_{-1}^- + a\rho\gamma_1^- + b\gamma_{-1}^- \\ &= (1 + \rho)(a\gamma_1^- + b\gamma_{-1}^-). \end{aligned}$$

in F_1 . It is a left zero divisor in F_1 whose right annihilators in F_1 are the set $\{y(a, b, \phi, \zeta) \mid \phi, \zeta \in K\}$. The objective is to add in elements from the other factors of $\mathbb{Q}[H]$ so that the sum has ± 1 as coefficients. If done correctly the contributions from most of the other factors will be invertible. In the following we pick and choose our elements and compute partial sums, much like putting together a puzzle made out of oddly shaped building blocks. The hope is that the last piece will fit in correctly. The initial few choices will be designed to keep the relative ratios (the ratio of one coefficient to another) in the set $\{0, \pm 1, \pm 2, \infty\}$.

The first elements are from $\rho_+ \gamma_0^- K$ and F_2 . Define

$$\begin{aligned} x_n &= x(a, b, 1, 1) + n(1 + \rho)(\gamma_0^- + \gamma_2^- + \gamma_{-2}^-) \\ &= (1 + \rho)(5^- + (a - n)\gamma_1^- + (b - n)\gamma_{-1}^-). \end{aligned}$$

If we assume $a = 5x + n$ and $b = 5y + n$ then

$$x_n = 5(1 + \rho)[n^- + x\gamma_1^- + y\gamma_{-1}^-].$$

Set $n = 1$, $x = 1$, $y = -1$. Then $a = 6$, $b = -4$. Define

$$\bar{\alpha} = \frac{x_1}{5} = (1 + \rho)(1^- + \gamma_1^- - \gamma_{-1}^-).$$

Now we assemble the rest of $\hat{\alpha}$. No group elements must be left out (see Ω_1), the bar in γ_i^- must be removed (see Ω_2), and every coefficient must be made ± 1 (see Ω_3).

Let

$$\Omega_1 = -(1-\rho)\gamma_0^- + (1-\rho)\gamma_2^- + (1-\rho)\gamma_{-2}^-$$

$$\Omega_2 = (1+\rho)\tau_+ + (1-\rho)\tau_+\gamma_0$$

$$\Omega_3 = -(1+\rho)5\tau_+ = -(1+\rho)(1+\tau+\tau^2+\tau^3+\tau^4).$$

Then

$$\begin{aligned} \bar{\alpha} + \Omega_1 &= (1-\gamma_0 + \gamma_1 - \gamma_{-1} + \gamma_2 + \gamma_{-2})^- + \rho(1 + \gamma_0 + \gamma_1 - \gamma_{-1} - \gamma_2 - \gamma_{-2})^- \\ &= 1 - \gamma_0 + \gamma_1 - \gamma_{-1} + \gamma_2 + \gamma_{-2} + \rho(1 + \gamma_0 + \gamma_1 - \gamma_{-1} - \gamma_2 - \gamma_{-2}) - \Omega_2 \text{ (see (10))} \\ &= 2 - \gamma_0^* + \gamma_1^* - \gamma_{-1}^* + \gamma_2^* + \gamma_{-2}^* + \rho(0 + \gamma_0^* + \gamma_1^* - \gamma_{-1}^* - \gamma_2^* - \gamma_{-2}^*) - \Omega_2 \\ &= 1 - \tau - \tau^2 - \tau^3 - \tau^4 - \gamma_0^* + \gamma_1^* - \gamma_{-1}^* + \gamma_2^* + \gamma_{-2}^* \\ &\quad + \rho(-1 - \tau - \tau^2 - \tau^3 - \tau^4 + \gamma_0^* + \gamma_1^* - \gamma_{-1}^* - \gamma_2^* - \gamma_{-2}^*) - \Omega_3 - \Omega_2. \end{aligned}$$

If we set $\hat{\alpha} = \bar{\alpha} + \Omega_1 + \Omega_2 + \Omega_3$, then the coefficients of $\hat{\alpha}$ are indeed all ± 1 so $\hat{\alpha}$ is the image by Φ of a complex multiplication type (see Proposition 1).

Now,

$$\begin{aligned} \hat{\alpha} &= \frac{x(6, -4, 1, 1)}{5} + \frac{(1+\rho)[\gamma_0^- + \gamma_2^- + \gamma_{-2}^-]}{5} - (1-\rho)\gamma_0^- + (1-\rho)\gamma_2^- + (1-\rho)\gamma_{-2}^- \\ &\quad + (1+\rho)\tau_+ + (1-\rho)\tau_+\gamma_0 - 5(1+\rho)\tau_+ \\ &= \frac{x(6, -4, 1, 1)}{5} + \frac{(1+\rho)}{5} \gamma_0^- - (1-\rho)\gamma_0^- + \left[\frac{6}{5}\gamma_2^- - \frac{4}{3}\rho\gamma_{-2}^- + \frac{6}{5}\gamma_{-2}^- - \frac{4}{3}\rho\gamma_{-2}^-\right] \\ &\quad - 4(1+\rho)\tau_+ \left(1 - \frac{\gamma_0}{5}\right) - \frac{4}{5}(1+\rho)\tau_+\gamma_0 + (1-\rho)\tau_+\gamma_0. \end{aligned}$$

But $\frac{6}{5}\gamma_2^- - \frac{4}{3}\rho\gamma_{-2}^- + \frac{6}{5}\gamma_{-2}^- - \frac{4}{3}\rho\gamma_{-2}^-$ corresponds to the matrix $\begin{bmatrix} 6 & -4 \\ -4 & 6 \end{bmatrix}$ which is invertible in F_2 . Therefore,

PROPOSITION 4. *The element $\hat{\alpha}$ decomposes into the sum of the following*

component elements, listed in the order of Proposition 2.

$$\begin{aligned}
& -\frac{4}{5}(1+\rho)\tau_+\gamma_0 \in \tau_+\rho_+\gamma_0\mathbb{Q} \\
& (1-\rho)\tau_+\gamma_0 \in \tau_+\rho_-\gamma_0\mathbb{Q} \\
& -4\rho_+\tau_+(1-\gamma_0/5) \in \tau_+V \\
& \frac{1}{5}(1+\rho)\gamma_0^- \in \rho_+\gamma_0^-K \\
& (1-\rho)\gamma_0^- \in \rho_-\gamma_0^-K \\
& \frac{x(6, -4, 1, 1)}{5} \in F_1 \\
& \frac{6}{5}\gamma_2^- - \frac{4}{5}\rho\gamma_2^- + \frac{6}{5}\gamma_2^- - \frac{4}{5}\rho\gamma_2^- \in F_2
\end{aligned}$$

The only component elements that are not invertible are $x(6, -4, 1, 1)/5$ and $-4\rho_+\tau_+(1-\gamma_0/5)$.

Proof. Clearly all the components are nonzero. The only subalgebras not isomorphic to fields or division algebras are τ_+V , F_1 , and F_2 . We have verified $\hat{\alpha}|_{F_2}$ is invertible and $\hat{\alpha}|_{F_1}$ is not invertible by construction. If $-4\rho_+\tau_+(1-\gamma_0/5) \in \tau_+V$ were invertible then we would not need the next section. Unfortunately this element is annihilated by $\rho_-\tau_+V$. \square

So by Propositions 2, 3 and 4 and Lemma 4, the right annihilators of $\hat{\alpha}$ generate the right $\mathbb{Q}[H]$ -module

$$\{y(6, -4, \phi, \zeta) \mid \phi, \zeta \in K\} \oplus (1-\rho)\tau_+V.$$

9. Eliminating the factor $(1-\rho)\tau_+V$

Set

$$\begin{aligned}
\alpha &= \hat{\alpha} + \sigma(1+\tau+\tau^2+\tau^3+\tau^4)\{1+\gamma+\gamma^2-\gamma^3-\gamma^4+\rho(1+\gamma+\gamma^2+\gamma^3+\gamma^4)\} \\
&= \hat{\alpha} + \sigma\{3(1+\rho)\tau_+\gamma_0 - 2(1-\rho)\tau_+\gamma_0 + 5\tau_+[(1-\gamma_0/5)+\gamma+\gamma^2-\gamma^3-\gamma^4]\}.
\end{aligned}$$

Unlike $\hat{\alpha}$, almost any reasonable try seems to produce a good α . Simple computation shows that the α given above, like $\hat{\alpha}$, has all coefficients ± 1 and is therefore the image of a CM-type. Furthermore the projections of α to $(1\pm\sigma)\mathbb{Q}[H]$ are the elements

$$\frac{1}{2}(\hat{\alpha} \pm \{3(1+\rho)\tau_+\gamma_0 - 2(1-\rho)\tau_+\gamma_0 + 5\tau_+[(1-\gamma_0/5)+\gamma+\gamma^2-\gamma^3-\gamma^4]\}). \quad (11)$$

A little more computation using (11) and Propositions 2 and 4 shows that α generates every simple ring subfactor of $(1 + \sigma)\mathbb{Q}[H]$ and $(1 - \sigma)\mathbb{Q}[H]$ except for $(1 \pm \sigma)F_1$ and possibly $(1 \pm \sigma)\tau_+ V$. Clearly our first goal is to show that α does indeed generate the factors $(1 \pm \sigma)\tau_+ V$.

Case 1: The component of α in $(1 + \sigma)\tau_+ V$. This is

$$\begin{aligned} & \left(\frac{1 + \sigma}{2}\right) \{-4(1 + \rho)\tau_+(1 - \gamma_0/5) + 5\tau_+[(1 - \gamma_0/5) + \gamma + \gamma^2 - \gamma^3 - \gamma^4]\} \\ &= \frac{1 + \sigma}{2} \cdot \tau_+[(1 - \gamma_0/5) + 5(\gamma + \gamma^2 - \gamma^3 - \gamma^4) - 4\rho(1 - \gamma_0/5)]. \end{aligned}$$

Define an automorphism $(\bar{\cdot})$ analogous to complex conjugation by extending the maps $\bar{\gamma} = \gamma^{-1}$ and $\bar{1} = 1$ to all of $\mathbb{Q}[\gamma]$. This gives us the obvious definition of an “absolute value”, $|z|^2 = z \cdot \bar{z}$ for $z \in \mathbb{Q}[\gamma]$. Note that $1 - \gamma_0/5$ has absolute value $1 - \gamma_0/5$ and is the identity in the field $(1 - \gamma_0/5)\mathbb{Q}[\gamma] (\cong \mathbb{Q}[\omega])$.

LEMMA 6. An element $(a + b\rho)$ $a, b \in (1 - \gamma_0/5)\mathbb{Q}[\gamma]$ is a zero divisor if and only if

$$\left| \frac{b}{a} \right| = 1 - \gamma_0/5.$$

Proof. $(a + b\rho) \cdot (c + d\rho) = 0$ implies that $ac + b\bar{d}$ and $ad + b\bar{c}$ must be zero (remember $z\rho = \rho\bar{z}$). The result follows from some simple algebra. \square

Applying Lemma 6, α generates $(1 + \sigma)\tau_+ V$ if

$$\frac{-4(1 - \gamma_0/5)}{(1 - \gamma_0/5) + 5(\gamma + \gamma^2 - \gamma^3 - \gamma^4)}$$

does not have “absolute value” $(1 - \gamma_0/5)$. This is a simple numerical computation which we leave to the reader.

Case 2: The component of α in $(1 - \sigma)\tau_+ V$. This is similar to Case 1 and omitted here. Therefore α generates every irreducible component of $\mathbb{Q}[G_0]$ except for $(1 \pm \sigma)F_1$.

The projections of α into $(1 \pm \sigma)F_1$ generate the left $\mathbb{Q}[G_0]$ submodules

$$(1 \pm \sigma)\{x(6, -4, \phi, \zeta) \mid \phi, \zeta \in K\}.$$

Thus the right annihilators of α are of the form

$$(1 \pm \sigma)y(6, -4, \phi, \zeta) \quad (\phi, \zeta \in K)$$

or equivalently of the form

$$y(6, -4, \phi_1, \zeta_1) + \sigma y(6, -4, \phi_2, \zeta_2) \quad (\phi_i, \zeta_i \in K).$$

By Proposition 3, these elements will never have coefficients consisting entirely of $\pm 1, 0$. This proves Theorem 4.

10. The creation of the corresponding CM field

We still need to show that there is a Galois totally complex field whose Galois group is $\mathbb{Z}/2 \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times D_5$ with the first $\mathbb{Z}/2\mathbb{Z}$ component being complex conjugation. If a totally real field whose Galois group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times D_5$ exists then adding in any imaginary quadratic extension over \mathbb{Q} will give us the totally complex field. However, this reduces to showing the existence of a totally real D_5 since it is easy to create real quadratic and quintic extensions disjoint from the D_5 extension. Gene Smith, UC Berkeley, in his thesis ([5]) computes the general polynomial parametrizing all such D_5 extensions. One simple example of such a D_5 extension is the splitting field for

$$z^5 - 10z^4 - 70z^3 - 25z^2 + 190z + 12.$$

Its real roots are approximately $-0.02730, 1.41005, -2.57914, -3.55684$, and 14.78866 and the real quadratic subfield is $\mathbb{Q}[\sqrt{5}]$.

Once we have the field, we use the α we created in the previous section to construct a CM-type S . Then as in Section 2.1 we create the map Ψ from K to \mathbb{C}^{100} by taking the direct sum over all the embeddings in S . Taking the quotient of \mathbb{C}^{100} by the image of any lattice in K will give us an abelian variety which has no sporadic cycles but whose Mumford-Tate group has order $85 < 101$.

References

- [1] P. Deligne: Hodge cycles on abelian varieties (notes by J. S. Milne). *Lecture Notes in Mathematics* 900 (1982), 9–100.
- [2] H. Pohlmann: Algebraic cycles on abelian varieties of complex multiplication type. *Ann. Math.* 88 (1968), 161–180.
- [3] K. Ribet: Hodge classes on certain types of abelian varieties. *Am. J. Math.* 105 (1983), 523–535.
- [4] J. Serre: *Abelian l -adic Representations and Elliptic Curves*. McGill University lecture notes, with William Kuyk and John Labute, 1968.
- [5] G. Smith: *Generic Cyclic Polynomials and Some Applications*. Ph.D. thesis, 1990.