Canadian Mathematical Bulletin
doi:10.4153/CMB-2011-045-x

Endomorphisms of Two Dimensional Jacobians and Related Finite Algebras

William Butske

Abstract. Zarhin proves that if C is the curve $y^2 = f(x)$ where $\mathrm{Gal}_{\mathbb{Q}}(f(x)) = S_n$ or A_n, then $\mathrm{End}_{\overline{\mathbb{Q}}}(J) = \mathbb{Z}$. In seeking to examine his result in the genus $g = 2$ case supposing other Galois groups, we calculate $\mathrm{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2$ for a genus 2 curve where $f(x)$ is irreducible. In particular, we show that unless the Galois group is S_5 or A_5, the Galois group does not determine $\mathrm{End}_{\overline{\mathbb{Q}}}(J)$.

1 Background

Let C be a genus g curve defined over $\mathbb{Q}$. We denote by J the Jacobian of the curve C. J is an abelian variety of dimension g defined over $\mathbb{Q}$. While both C and J are defined over $\mathbb{Q}$, we will consider them over $\overline{\mathbb{Q}}$. As a result we will have an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the set of $\overline{\mathbb{Q}}$ points of C and hence on the set of $\overline{\mathbb{Q}}$ points of J. If f is a polynomial over $\mathbb{Q}$, then we denote by $\mathrm{Gal}_{\mathbb{Q}}(f(x))$, the Galois group of f over $\mathbb{Q}$.

Let $\mathrm{End}_{\overline{\mathbb{Q}}}(J)$, denote the ring of endomorphisms of J defined over $\overline{\mathbb{Q}}$. In his paper [6], Zarhin gives, for hyperelliptic curves, a simple criterion for determining when $\mathrm{End}_{\overline{\mathbb{Q}}}(J)$ is *trivial i.e.*, when $\mathrm{End}_{\overline{\mathbb{Q}}}(J) = \mathbb{Z}$.

Theorem 1.1 (Zarhin) *Let C be the curve defined by the equation $y^2 = f(x)$, where $\deg(f) = n \geq 5$ and $f(x)$ is square-free in $\mathbb{Q}[x]$. If $\mathrm{Gal}_{\mathbb{Q}}(f(x)) = S_n$ or A_n, then $\mathrm{End}_{\overline{\mathbb{Q}}}(J) = \mathbb{Z}$.*

So at least in the above case, $\mathrm{Gal}_{\mathbb{Q}}(f(x))$ determines $\mathrm{End}_{\overline{\mathbb{Q}}}(J)$.

Suppose now that $f(x)$ is irreducible of degree 5, then $\mathrm{Gal}_{\mathbb{Q}}(f(x))$ is one of the following groups: S_5, A_5, F_{20} (the Frobenius group of order 20), D_5, or $\mathbb{Z}/5\mathbb{Z}$. We seek to determine to what extent Zarhin's result extends to these cases. For instance, is knowing $\mathrm{Gal}_{\mathbb{Q}}(f(x)) = F_{20}$ enough to determine $\mathrm{End}_{\overline{\mathbb{Q}}}(J)$? To answer this question we will determine $\mathrm{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2$ for a genus 2 curve with a $\mathbb{Q}$-rational Weierstrass point (the existence of such a point is equivalent to the condition that $\deg(f) = 5$ ([2]). Our main result is that the Galois group does not determine $\mathrm{End}_{\overline{\mathbb{Q}}}(J)$.

Received by the editors January 4, 2009; revised June 29, 2009.
Published electronically March 18, 2011.
AMS subject classification: **11G10**, 20C20.

2 Representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $\mathrm{End}_{\overline{\mathbb{Q}}}(J)$

Let $J[2]$ denote the points of order two on the Jacobian. $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts linearly on $J[2]$, as does $\mathrm{End}_{\overline{\mathbb{Q}}}(J)$. In other words we have representations $\overline{\rho}_2$ and $\overline{\phi}_2$ as follows:

$$\begin{tikzcd} & & \mathrm{End}_{\overline{\mathbb{Q}}}(J) \arrow[d, "\overline{\phi}_2"] \\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[r, "\overline{\rho}_2"] & \mathrm{Aut}(J[2]) \arrow[r, hook] & \mathrm{End}_{\overline{\mathbb{Q}}}(J[2]), \end{tikzcd}$$

where $\overline{\rho}_2$ and $\overline{\phi}_2$ are nothing more than the restriction maps. Furthermore, we have that $J[2] \cong (\mathbb{F}_2)^{2g}$. Thus, in the case of a genus two curve, we have the homomorphisms:

$$\begin{tikzcd} & & \mathrm{End}_{\overline{\mathbb{Q}}}(J) \arrow[d, "\overline{\phi}_2"] \\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[r, "\overline{\rho}_2"] & \mathrm{GL}_4(\mathbb{F}_2) \arrow[r, hook] & \mathrm{Mat}_4(\mathbb{F}_2). \end{tikzcd}$$

2.1 Images of $\overline{\rho}_2$ and $\overline{\phi}_2$

One has an explicit basis for $J[2]$ in terms of ramification points, as mentioned in Mori [3], and from this basis one can show that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $J[2]$ via the surjection $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}_{\mathbb{Q}}(f(x))$. In other words, $\mathrm{Im}(\overline{\rho}_2) \cong \mathrm{Gal}_{\mathbb{Q}}(f(x))$. Now an endomorphism that kills $J[2]$ factors as $[2]\colon J(C) \to J(C)$ followed by an endomorphism of $J(C)$, so the kernel of $\overline{\phi}_2$ is $2\,\mathrm{End}_{\overline{\mathbb{Q}}}(J)$, *i.e.*, $\mathrm{Im}(\overline{\phi}_2) \cong \mathrm{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2$.

3 G-Normal Algebras

Notice now that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $\mathrm{End}_{\overline{\mathbb{Q}}}(J)$ via conjugation, and furthermore, the maps $\overline{\rho}_2$ and $\overline{\phi}_2$ respect this action. Thus, if $h \in \mathrm{Im}(\overline{\phi}_2) \cong \mathrm{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2$ and $g \in \mathrm{Im}(\overline{\rho}_2) \cong \mathrm{Gal}_{\mathbb{Q}}(f(x))$, then $ghg^{-1} \in \mathrm{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2$.

Definition 3.1 Let $G \to GL_n(F)$ be a faithful representation of a group G. Let A be an F-subalgebra of $Mat_n(F)$. We say that A is *G-normal* if for all elements $g \in G$ and $h \in A$ we have that $ghg^{-1} \in A$. (This notion appears in an equivalent form in Zarhin [7].)

In terms of this definition, we have that $\mathrm{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2$ is a $\mathrm{Gal}_{\mathbb{Q}}(f(x))$-normal subalgebra of $\mathrm{Mat}_4(\mathbb{F}_2)$ when C is a genus two curve. In [7], Zarhin proves that if we take our representation of $\mathrm{Gal}_{\mathbb{Q}}(f(x))$ arising from Mori, then the only subalgebra that is $\mathrm{Gal}_{\mathbb{Q}}(f(x))$-normal for $\mathrm{Gal}_{\mathbb{Q}}(f(x)) \cong S_5$ or A_5 is $\mathbb{F}_2$. Zarhin's theorem then follows as a corollary when combined with the Mumford–Albert classification of $\mathrm{End}^0_{\overline{\mathbb{Q}}}(J)$ ([4]). We will show that when $\mathrm{Gal}_{\mathbb{Q}}(f(x)) \cong F_{20}, D_5$, or $\mathbb{Z}/5\mathbb{Z}$, the set of

$\mathrm{Gal}_{\mathbb{Q}}(f(x))$-normal algebras is given by $\{\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_{16}\}$, and moreover, all such algebras occur as $\mathrm{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2$ for some curve C.

Remark 3.2 One should be careful here and note that the definition of G-normal algebra is made with respect to a particular representation. It is possible for an algebra to be normal with respect to one faithful representation and not normal with respect to another.

The fact that $\mathrm{End}_{\overline{\mathbb{Q}}}(J)$ is normal with respect to the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ informs a philosophy about the image of the ℓ-adic representations ρ_ℓ and ϕ_ℓ that one obtains from considering the inverse limit over n of the representations ρ_{ℓ^n} and ϕ_{ℓ^n} respectively. Note that $\rho_\ell\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_{2g}(\mathbb{Z}_\ell)$ and $\phi_\ell\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Mat_{2g}(\mathbb{Z}_\ell)$. The philosophy is that a "big" $\mathrm{End}_{\overline{\mathbb{Q}}}(J)$, hence a "big" $\mathrm{Im}(\phi_\ell)$, forces a "small" $\mathrm{Im}(\rho_\ell)$ and vice-versa. This philosophy is stated more precisely as "big monodromy" if and only if $\mathrm{End}_{\overline{\mathbb{Q}}}(J) = \mathbb{Z}$ and has been proven in the case of genus 1 by Serre [5] and in genus 2 by Zarhin [6].

In our case we are examining $\ell = 2$ and the first term of our inductive limit, $J[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g}$. Applying our philosophy, we expect that the bigger the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the harder it is for $\mathrm{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2$ to be normal with respect to this image. In other words, "big" image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ implies "small" $\mathrm{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2$, so if the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is as big as possible (*i.e.,* S_n or A_n), then $\mathrm{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2$ should be small as possible, *i.e.,* $\mathbb{F}_2$.

Indeed, this is what Zarhin did for curves of the form $y^2 = f(x)$. One might then be led to the conclusion that as we reduce the size of the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *i.e.,* the size of $\mathrm{Gal}_{\mathbb{Q}}(f(x))$, we can increase the size of $\mathrm{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2$. We state this bit of philosophy as a generalization of the idea of "big monodromy"

Big Monodromy *Let $H \subsetneq G$ be transitive subgroups of S_n other than S_n and A_n. Then the set of G-normal algebras is properly contained in the set of H-normal algebras.*

Our main result then comes as a bit of a surprise. Namely, the proper containments $\mathbb{Z}/5\mathbb{Z} \subsetneq D_5 \subsetneq F_{20}$ do not imply proper containments F_{20}-normal algebras $\subsetneq$ D_5-normal algebras $\subsetneq \mathbb{Z}/5\mathbb{Z}$-normal algebras. In fact, these latter three sets are equal.

4 $\mathrm{Gal}_{\mathbb{Q}}(f(x))$-Normal Subalgebras of $\mathrm{Mat}_4(\mathbb{F}_2)$

A naive method of determining the G-normal subalgebras of any $Mat_n(\mathbb{F}_p)$ would be to list all subspaces of $Mat_n(\mathbb{F}_p)$, use these spaces to generate algebras and then check if the resulting algebras remained G-normal. This method very quickly becomes too costly for practical implementation. In the case of $\mathrm{Mat}_4(\mathbb{F}_2)$, there are 134732283882872625911 subspaces to check.

We can considerably narrow the number of subspaces to be checked by examining the $\mathrm{Gal}_{\mathbb{Q}}(f(x))$-module structure of $\mathrm{Mat}_4(\mathbb{F}_2)$ more closely. In particular, all possibilities for $\mathrm{Gal}_{\mathbb{Q}}(f(x))$ contain the cyclic subgroup $\mathbb{Z}/5\mathbb{Z}$, thus the set of $\mathbb{Z}/5\mathbb{Z}$-normal subspaces is sufficient to determine all $\mathrm{Gal}_{\mathbb{Q}}(f(x))$-normal subspaces. Give $\mathrm{Mat}_4(\mathbb{F}_2)$ the structure of an $F_2[t]$-module by having t act on $\mathrm{Mat}_4(\mathbb{F}_2)$ via conjugation by a generator of $\mathbb{Z}/5\mathbb{Z}$. This allows us to use modules over PIDs to determine all the $\mathrm{Gal}_{\mathbb{Q}}(f(x))$-normal subspaces of $\mathrm{Mat}_4(\mathbb{F}_2)$.

4.1 $\mathbb{F}_2[t]$-Module Structure of $\mathrm{Mat}_4(\mathbb{F}_2)$

Using the standard basis e_{ij} for $\mathrm{Mat}_4(\mathbb{F}_2)$, one computes that the matrix that represents the action of t is given by

$$T = \begin{bmatrix}
0&1&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
1&1&1&0&0&1&0&0&0&1&0&0&0&1&0&0\\
1&0&1&1&0&0&1&0&0&0&1&0&0&0&1&0\\
1&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1\\
1&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&1&0&1&0&0&0&0&0&0&0&0&0\\
0&0&1&0&1&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&1&1&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&1&0&1&0&0&0&0&0\\
0&0&0&0&0&0&1&0&1&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&1&1&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&1&0&1&0\\
0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0
\end{bmatrix}.$$

Then via *GAP4* [1],

$$\mathrm{char}_{\mathbb{F}_2}(T,t) = (t-1)^4(t^4+t^3+t^2+t+1)^3$$

and

$$\min_{\mathbb{F}_2}(T,t) = t^5 - 1$$

Thus we have the $\mathbb{F}_2[t]$-module decomposition of $\mathrm{Mat}_4(\mathbb{F}_2)$:

$$\mathrm{Mat}_4(\mathbb{F}_2) \cong \bigoplus_{i=1}^{4} \mathbb{F}_2[t]/(t+1) \bigoplus_{i=1}^{3} \mathbb{F}_2[t]/(t^4+t^3+t^2+t+1) \tag{4.1}$$

Given our decomposition (4.1), we note that if W is an $\mathbb{F}_2[t]$-submodule of $\mathrm{Mat}_4(\mathbb{F}_2)$, then $W \cong W_1 \oplus W_2$, where $W_1 \subseteq \bigoplus_{i=1}^4 \mathbb{F}_2[t]/(t+1)$ is an $\mathbb{F}_2[t]/(t+1) \cong \mathbb{F}_2$-submodule and

$$W_2 \subseteq \bigoplus_{i=1}^{3} \mathbb{F}_2[t]/(t^4+t^3+t^2+t+1)$$

is an

$$\mathbb{F}_2[t]/(t^4+t^3+t^2+t+1) \cong \mathbb{F}_{2^4}\text{-submodule.}$$

Thus, to enumerate all $\mathbb{F}_2[t]$-submodules, it suffices to enumerate all $\mathbb{F}_2$-subspaces of $(F_2)^4$ and all $\mathbb{F}_{2^4}$ subspaces of $(\mathbb{F}_{2^4})^3$. Denote by $(\frac{k}{n,q})$ the number of k-dimensional $\mathbb{F}_q$-subspaces of $(\mathbb{F}_q)^n$. Then we have

$$\begin{aligned}
\left| \mathbb{F}_2[t] - \text{submodules of } \bigoplus_{i=1}^{4} \mathbb{F}_2[t]/(t+1) \right| &= 1 + \left(\tfrac{1}{4,2}\right) + \left(\tfrac{2}{4,2}\right) + \left(\tfrac{3}{4,2}\right) + 1 \\
&= 1 + 15 + 35 + 15 + 1 \\
&= 67
\end{aligned}$$

https://doi.org/10.4153/CMB-2011-045-x Published online by Cambridge University Press

$$\begin{aligned}\left|\mathbb{F}_2[t]-\text{submodules of }\bigoplus_{i=1}^{4}\mathbb{F}_2[t]/(t^4+t^3+t^2+t+1)\right| &= 1+\binom{1}{3,2^4}+\binom{2}{3,2^4}+1\\ &= 1+237+237+1\\ &= 476\end{aligned}$$

We can further restrict the number of subspaces needed in $\bigoplus_{i=1}^{4}\mathbb{F}_2[t]/(t+1)$ by noting that we require the identity matrix to be one of our subspaces since $id \in \mathrm{End}_{\overline{\mathbb{Q}}}(J)\otimes_{\mathbb{Z}}\mathbb{F}_2$.

By counting the number of $\mathbb{F}_2$-subspaces of $(\mathbb{F}_2)^4$ that contain the identity element, we need only consider 16 of the 67 $\mathbb{F}_2$-subspaces of $(\mathbb{F}_2)^4$. Thus we have reduced our initial test of 134732283882873635911 subspaces to only having to check $16\cdot 476 = 7616$ subspaces.

5 Description of Algorithm

In this section, we describe an algorithm for determining the $\mathbb{F}_2[t]$-subalgebras of $\mathrm{Mat}_4(\mathbb{F}_2)$. We write $\mathrm{Mat}_4(\mathbb{F}_2)$ as the row space $(\mathbb{F}_2)^{16}$, taking as basis the standard basis $\{e_{ij}\}$ of $\mathrm{Mat}_4(\mathbb{F}_2)$. For example, the identity matrix id corresponds to the row vector

$$(1,0,0,0,0,1,0,0,0,0,1,0,0,0,0,1) = e_{11}+e_{22}+e_{33}+e_{44}.$$

Step 1: Obtain an explicit realization of decomposition (4.1).

Viewing $\mathrm{Mat}_4(\mathbb{F}_2)$ as a 16-dimensional $\mathbb{F}_2$-vector space we computed the 16×16 matrix T associated with the action of $\mathbb{Z}/5\mathbb{Z}$ on $\mathrm{Mat}_4(\mathbb{F}_2)$, *i.e.,* the matrix associated with conjugation by the generator of $\mathbb{Z}/5\mathbb{Z}$ (to do this, we used our explicit representation of $\mathbb{Z}/5\mathbb{Z}$ in $\mathrm{Mat}_4(\mathbb{F}_2)$).

Remark 5.1 Let G be a finite group, and let V be any finite dimensional G-vector space over F where $\mathrm{char}(F)$ does not divide the order of G. Consider the linear transformation $\phi\colon V \to V$ given by $v \mapsto \sum_{g\in G} gv$. The image of ϕ is then fixed elementwise by G. Conversely, if $v \in V$ is fixed by G, then $v = \sum_{g\in G} gv$. In other words, $V^G = \mathrm{Im}(\phi)$.

The remark tells us that the columns of the matrix $T^4+T^3+T^2+T+1$ span the subspace of elements fixed by T, *i.e.,* by conjugation. We then reduce these to a basis, $\{v_1,v_2,v_3,v_4\}$, of $\mathrm{Mat}_4(\mathbb{F}_2)^{\mathbb{Z}/5\mathbb{Z}}$. Upon examining this basis, one sees $\{v_1,v_2,v_3,v_4\} = \{e_{11},e_{22},e_{33},e_{44}\}$, as one might expect. In particular, the identity element is in $\mathrm{Mat}_4(\mathbb{F}_2)^{\mathbb{Z}/5\mathbb{Z}}$. We then have a basis for the $\bigoplus_{i=1}^{4}\mathbb{F}_2[t]/(t+1)$ part of $\mathrm{Mat}_4(\mathbb{F}_2)$. We seek to extend $\{v_1,v_2,v_3,v_4\}$ to a basis for all of $\mathrm{Mat}_4(\mathbb{F}_2)$.

We could do this by randomly picking a vector out of the complement of the span of $\{v_1,v_2,v_3,v_4\}$ and testing if this vector yields an invariant subspace, but we do slightly better in noting that

$$\mathrm{Mat}_4(\mathbb{F}_2) = \mathrm{Ker}(\phi)\bigoplus\mathrm{Im}(\phi) = \mathrm{Ker}(\phi)\bigoplus\mathrm{Mat}_4(\mathbb{F}_2)^{\mathbb{Z}/5\mathbb{Z}}$$

https://doi.org/10.4153/CMB-2011-045-x Published online by Cambridge University Press

and then calculating a basis for $\mathrm{Ker}(\phi)$. In our implementation, the vector

$$v_5 := [0,0,0,0,0,0,0,0,1,0,0,0,1,1,0,0]$$

generates an irreducible $\mathbb{Z}/5\mathbb{Z}$-subspace of in the complement of $\mathrm{Mat}_4(\mathbb{F}_2)^{\mathbb{Z}/5\mathbb{Z}}$, which we denote $\langle v_5\rangle$. We then have an explicit basis for

$$V' := \bigoplus_{i=1}^{4} \mathbb{F}_2[t]/(t+1) \bigoplus, \mathbb{F}_2[t]/(t^4+t^3+t^2+t+1)$$

which we wish to extend to $\mathrm{Mat}_4(\mathbb{F}_2)$. We then take a random element in the complement of V' and check to see if it yields an irreducible submodule. We repeat this until we have a basis of

$$\bigoplus_{i=1}^{4} \mathbb{F}_2[t]/(t+1) \bigoplus_{i=0}^{3} \mathbb{F}_2[t]/(t^4+t^3+t^2+t+1).$$

The decomposition we arrive at is given by

$$\mathrm{Mat}_4(\mathbb{F}_2) \cong \bigoplus_{i=1}^{4} e_{ii} \bigoplus \langle v_5\rangle \bigoplus \langle v_6\rangle \bigoplus \langle v_7\rangle,$$

where

$$v_5 := [0,0,0,0,0,0,0,0,1,0,0,0,1,1,0,0],$$
$$v_6 := [0,1,1,0,0,0,0,0,1,0,0,0,0,0,0,0],$$
$$v_7 := [1,1,0,0,0,0,0,1,1,0,1,1,0,0,0,0].$$

We then calculate a list of all $\mathbb{F}_{2^4}$-subspaces of $(\mathbb{F}_{2^4})^3$ and convert this to a list of bases for all invariant subspaces of the 12 dimensional part, $\bigoplus_{i=0}^{3} \mathbb{F}_2[t]/(t^4+t^3+t^2+t+1)$, of $\mathrm{Mat}_4(\mathbb{F}_2)$ using the explicit basis we obtained above.

Step 2: Enumerate the subspaces containing the identity in terms of Step 1.

We combine the above list of with the list of all subspaces of $\mathrm{Mat}_4(\mathbb{F}_2)^{\mathbb{Z}/5\mathbb{Z}}$ containing the identity to get the list of all subspaces of $\mathrm{Mat}_4(\mathbb{F}_2)$ which are $\mathbb{Z}/5\mathbb{Z}$-invariant.

Step 3: Determine which of the $\mathbb{F}_2[t]$-submodules are in fact $\mathbb{F}_2[t]$-subalgebras.

Using the list of Step 2, we generate all possible $\mathbb{F}_2[t]$-subalgebras of $\mathrm{Mat}_4(\mathbb{F}_2)$ by using all $\mathbb{F}_2[t]$-subspaces as generating sets. We then check which of these resulting algebras are $\mathbb{Z}/5\mathbb{Z}$-invariant.

Step 4: Check the list from Step 3 for F_{20} and D_5 normalcy.

Given our list of all $\mathbb{Z}/5\mathbb{Z}$-normal subalgebras from Step 3, we check to see which are also F_{20} and D_5-normal.

https://doi.org/10.4153/CMB-2011-045-x Published online by Cambridge University Press

6 Results of the Algorithm

Examining the output of the algorithm as implemented above in *GAP*4, we have that there are precisely five $\mathbb{F}_2$-subalgebras of $\mathrm{Mat}_4(\mathbb{F}_2)$ that are $\mathbb{Z}/5\mathbb{Z}$-normal, up to choice of basis. They are given as follows where by $F\langle x, y\rangle$ we denote the F algebra generated by x and y

$$A_1 := \mathbb{F}_2 \left\langle \begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{bmatrix} \right\rangle$$

$$A_2 := \mathbb{F}_2 \left\langle \begin{bmatrix} 1&0&1&1\\ 1&0&1&0\\ 0&1&0&1\\ 1&1&0&1 \end{bmatrix}, \begin{bmatrix} 0&0&1&1\\ 1&1&1&0\\ 0&1&1&1\\ 1&1&0&0 \end{bmatrix} \right\rangle$$

$$A_3 := \mathbb{F}_2 \left\langle \begin{bmatrix} 1&1&0&0\\ 0&1&1&0\\ 0&0&1&1\\ 1&1&1&0 \end{bmatrix}, \begin{bmatrix} 0&1&1&0\\ 0&0&1&1\\ 1&1&1&0\\ 0&1&1&1 \end{bmatrix}, \begin{bmatrix} 0&0&0&1\\ 1&1&1&1\\ 1&0&0&0\\ 0&1&0&0 \end{bmatrix}, \begin{bmatrix} 0&0&1&0\\ 0&0&0&1\\ 1&1&1&1\\ 1&0&0&0 \end{bmatrix} \right\rangle$$

$$A_4 := \mathbb{F}_2 \left\langle \begin{bmatrix} 0&0&1&1\\ 0&1&1&0\\ 1&1&0&0\\ 0&1&1&1 \end{bmatrix}, \begin{bmatrix} 1&1&0&0\\ 0&1&1&0\\ 0&0&1&1\\ 1&1&1&0 \end{bmatrix}, \begin{bmatrix} 0&1&0&1\\ 0&1&0&1\\ 0&0&1&0\\ 0&0&0&0 \end{bmatrix}, \begin{bmatrix} 0&0&0&0\\ 1&0&0&0\\ 1&0&1&1\\ 1&0&1&1 \end{bmatrix}, \begin{bmatrix} 0&0&0&1\\ 0&1&1&1\\ 0&0&1&1\\ 1&1&1&1 \end{bmatrix} \right\rangle$$

$$A_5 := \mathrm{Mat}_4(\mathbb{F}_2)$$

We sum up our results in the following theorem, which is the main result of this work.

Theorem 6.1 (Main Result) *The algebras A_i, for $i = 1 \dots 5$, are the only F_{20}, D_5, and $\mathbb{Z}/5\mathbb{Z}$-normal subalgebras of $Mat_4(\mathbb{F}_2)$; moreover, they are all simultaneously F_{20}, D_5 and $\mathbb{Z}/5\mathbb{Z}$-normal.*

Proof Only the fact that all the algebras are in addition F_{20} and D_5-normal needs to be checked, but this can be done by hand, or by examining the output of Step 4 of the algorithm. ■

Corollary 6.2 *Let C be the curve of genus 2 defined by $y^2 = f(x)$, where $f(x) \in \mathbb{Q}[x]$ is of degree 5, square free, and irreducible. Then $\mathrm{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2$ is, up to choice of basis of $J[2]$, one of A_1, A_2 or A_3.*

Proof If $\mathrm{Gal}_{\mathbb{Q}}(f(x)) = S_5$ or A_5, apply Zarhin, otherwise $\mathrm{Gal}_{\mathbb{Q}}(f(x))$ is one of F_{20}, D_5, or $\mathbb{Z}/5\mathbb{Z}$ and we can apply Theorem 6.1. A_1, A_2, A_3, A_4, and A_5 are of dimensions 1, 2, 4, 8, and 16 respectively, while $\mathrm{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2$ is of dimension less than or equal to 4 since $\mathrm{rank}_{\mathbb{Z}}(\mathrm{End}_{\overline{\mathbb{Q}}}(J)) \le 4$ [4]. ■

7 A_i as $\mathrm{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2$

Furthermore, we show that that A_1, A_2, and A_3 occur as $\mathrm{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2$ as follows. First a family of polynomials that give the prescribed Galois group is constructed. Then one uses MAGMA to determine $\mathrm{End}_{\overline{\mathbb{Q}}}(J)$ and subsequently $\mathrm{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2$.

Remark 7.1 This method of searching is an extremely naive fishing expedition, since Mori proved in [3] that a *generic* hyperelliptic curve of arbitrary genus has the property that $\mathrm{End}_{\overline{\mathbb{Q}}}(J) = \mathbb{Z}$. Thus one expects such a search to generically fail, and it is perhaps surprising that this method yielded some results.

Example 7.2 For the polynomial $f(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$ we have via MAGMA that $\operatorname{End}_{\overline{\mathbb{Q}}}(J) = \mathbb{Z}$. Thus $\operatorname{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2 = A_1$.

Example 7.3 The algebra A_2 occurs for $f(x) = x^5 - x^4 - x^3 - x^2 + x + 1$ as MAGMA gives us that

$$\operatorname{End}_{\overline{\mathbb{Q}}}(J) = \mathbb{Z}\left\langle \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} \right\rangle,$$

which, upon tensoring with $\mathbb{F}_2$, is conjugate to A_2. Note also that the characteristic polynomial of the above matrix is $x^2 - x - 1$ that has roots $\frac{1 \pm 5}{2}$. Thus $\operatorname{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(\sqrt{5})$.

Example 7.4 Lastly, A_3 occurs for the $f(x) = x^5 + 2$. We can see this in two ways. First, MAGMA gives us that

$$\operatorname{End}_{\overline{\mathbb{Q}}}(J) = \mathbb{Z}\left\langle \begin{bmatrix} 0 & 1 & 0 & 1 \\ 2 & 1 & 1 & 0 \\ 1 & -2 & 0 & 1 \\ -3 & -1 & -1 & 0 \end{bmatrix} \right\rangle.$$

Then one can tensor with $\mathbb{F}_2$ and check conjugate conjugacy to A_3. Alternately, we can see from the above matrix representation of $\operatorname{End}_{\overline{\mathbb{Q}}}(J)$ that $\operatorname{End}_{\overline{\mathbb{Q}}}(J) = \mathbb{Z}[\zeta_5]$, where ζ_5 is a primitive root of unity. The ζ_5 comes from the fact that $(x, y) \mapsto (x\zeta_5, y)$ is an automorphism of the curve defined by $y^2 = x^5 + 2$. Now note that $\mathbb{Z}[\zeta_5]$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\zeta_5)$, and thus the ideal (2) factors in $\mathbb{Z}[\zeta_5]$ as a product of primes $(2)\mathbb{Z}[\zeta_5] = \mathfrak{P}_1^{\alpha_1} \dots \mathfrak{P}_r^{\alpha_r}$. Since $\mathbb{Q}(\zeta_5)$ is Galois over $\mathbb{Q}$, $(2)\mathbb{Z}[\zeta_5] = (\mathfrak{P}_1 \dots \mathfrak{P}_r)^e$ and $ref = \phi(5) = 4$. Furthermore, since 2 does not divide 5, (2) splits into the product of $\phi(5)/f$ prime ideals, where f is the order of $2 \pmod 5$. Since $f = 4$, (2) does not split in $\mathbb{Z}[\zeta_5]$. Thus $\operatorname{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2 = \mathbb{Z}[\zeta_5] \otimes_{\mathbb{Z}} \mathbb{F}_2 = \mathbb{Z}[\zeta_5]/(2)$ has dimension $f = 4$ over $\mathbb{Z}/(2)\mathbb{Z} = \mathbb{F}_2$. Since $\operatorname{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2$ is $\operatorname{Gal}_{\mathbb{Q}}(f(x))$-normal and A_3 is the only algebra fitting this description, $\operatorname{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2 = A_3$.

While this shows that all of the algebras A_i do in fact occur, it sidesteps the question nearest to the idea of Zarhin's result. Namely, given the Galois group, how much information can we get about $\operatorname{End}_{\overline{\mathbb{Q}}}(J)$? The following table gives a partial answer in the genus 2 case.

$\operatorname{Gal}_{\mathbb{Q}}(f(x))$	A_1	A_2	A_3
F_{20}	$x^5 + x^4 + 2x^3 + 4x^2 + x + 1$	$x^5 - 10x^2 + 20x - 24$	$x^5 + 2$
D_5	$x^5 + 11x + 44$	$x^5 - x^3 - 2x^2 - 2x - 1$	
$\mathbb{Z}/5\mathbb{Z}$	$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$		

For instance, in the case that $\operatorname{Gal}_{\mathbb{Q}}(f(x)) = F_{20}$, all of the A_i can occur and the idea of determining $\operatorname{End}_{\overline{\mathbb{Q}}}(J)$ from $\operatorname{Gal}_{\mathbb{Q}}(f(x))$ fails.

Remark 7.5 The author conjectures that the table can be filled in, *i.e.*, attempting to determine $\mathrm{End}_{\overline{\mathbb{Q}}}(J)$ via $\mathrm{Gal}_{\mathbb{Q}}(f(x))$ always fails in the genus 2 case. More precisely, the author conjectures that for the Galois groups $G = F_{20}, D_5, \mathbb{Z}/5\mathbb{Z}$, there exist polynomials $f_{G,i}(x)$ such that $Gal_{\mathbb{Q}}(f_{G,i}) = G$ and $\mathrm{End}_{\overline{\mathbb{Q}}}(J) \otimes_{\mathbb{Z}} \mathbb{F}_2 = A_i$ for $i = 1, 2, 3$.

8 A_i Intrinsically

We have the following lattice of algebras in $\mathrm{Mat}_4(\mathbb{F}_2)$

$$\begin{tikzcd}
A_4 \arrow[d, dash] \\
A_3 \arrow[d, dash] \\
A_2 = \mathbb{F}_4 \arrow[d, dash] \\
A_1 = \mathbb{F}_2.
\end{tikzcd}$$

Note that A_3 is not a field as it contains zero divisors. However, as the reviewer pointed out, we do have a containment in $\mathrm{Mat}_4(\mathbb{F}_2)$ as follows:

$$\begin{tikzcd}
& A_4 \arrow[dl, dash] \arrow[dr, dash] & \\
A_3 \arrow[dr, dash] & & \mathbb{F}_{16} \arrow[dl, dash] \\
& A_2 = \mathbb{F}_4 \arrow[d, dash] & \\
& A_1 = \mathbb{F}_2, &
\end{tikzcd}$$

where we can take the field $\mathbb{F}_{16}$ to be the algebra generated by the element

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

Now, $\mathrm{Gal}(\mathbb{F}_{16}/\mathbb{F}_2) = \mathbb{Z}/4\mathbb{Z}$, thus we can realize the semidirect product $F_{20} = \mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ as $F_{20} = \mathbb{Z}/5\mathbb{Z} \rtimes \mathrm{Gal}(\mathbb{F}_{16}/\mathbb{F}_2)$ and furthermore A_4 is the centralizer of A_2 in $\mathrm{Mat}_4(\mathbb{F}_2)$.

References

[1] The GAP Group, *GAP—Groups, Algorithms, and Programming, Version 4.4.* http://www.gap-system.org, 2004.

[2] P. Lockhart, *On the discriminant of a hyperelliptic curve.* Trans. Amer. Math. Soc. **342**(1994), no. 2, 729–752. doi:10.2307/2154650
[3] S. Mori, *The endomorphism rings of some Abelian varieties.* Japan. J. Math. (N.S.) **2**(1976), no. 1, 109–130.
[4] D. Mumford, *Abelian varieties.* Tata Institute of Fundamental Research Studies in Mathematics, 5, Oxford University Press, London, 1970.
[5] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves.* Revised reprint of the 1968 original. Research Notes in Mathematics, 7, A K Peters, Wellesley, MA, 1998.
[6] Y. G. Zarhin, *Abelian varieties, ℓ-adic representations and* SL_2. Izv. Akad. Nauk SSSR Ser. Mat. **43**(1979), no. 2, 294–308.
[7] ———, *Hyperelliptic Jacobians without complex multiplication.* Math. Res. Lett. **7**(2000), no. 1, 123–132.

Department of Mathematics, Rose-Hulman Institute of Technology, Terre Haute, IN 47907, U.S.A.
e-mail: butske@rose-hulman.edu