# Non-monogenic Division Fields and Endomorphisms of Abelian Varieties

Hanson Smith

University of Connecticut

# Table of contents

1. Background
2. Division Fields
3. Results for Division Fields of Elliptic Curves
4. Results for Abelian Varieties of Dimension $> 1$

# Background

# Monogeneity

One of the primary interests of number theory is understanding the roots of monic polynomials in $\mathbb{Z}[x]$. When and how can the roots of one polynomial be expressed by the roots of another polynomial?

# Monogeneity

One of the primary interests of number theory is understanding the roots of monic polynomials in $\mathbb{Z}[x]$. When and how can the roots of one polynomial be expressed by the roots of another polynomial?

Let $K/\mathbb{Q}$ be a number field of degree $n$ with ring of integers $\mathcal{O}_K$. We say $K$ *is monogenic* or $\mathcal{O}_K$ *admits a power integral basis* if $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in K$.

# Monogeneity

One of the primary interests of number theory is understanding the roots of monic polynomials in $\mathbb{Z}[x]$. When and how can the roots of one polynomial be expressed by the roots of another polynomial?

Let $K/\mathbb{Q}$ be a number field of degree $n$ with ring of integers $\mathcal{O}_K$. We say *$K$ is monogenic* or *$\mathcal{O}_K$ admits a power integral basis* if $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in K$. More explicitly, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is an $\mathbb{Z}$-basis for the $\mathbb{Z}$-module $\mathcal{O}_K$.

# Our First Friends

Take $\mathbb{Q}(\sqrt{d})$, with $d$ square-free.

# Our First Friends

Take $\mathbb{Q}(\sqrt{d})$, with $d$ square-free. The ring of integers of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \bmod 4$ and $\mathbb{Z}[\sqrt{d}]$ otherwise.

# Our First Friends

Take $\mathbb{Q}(\sqrt{d})$, with $d$ square-free. The ring of integers of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \bmod 4$ and $\mathbb{Z}[\sqrt{d}]$ otherwise. In both cases $\mathbb{Q}(\sqrt{d})$ is monogenic.

# Our First Friends

Take $\mathbb{Q}(\sqrt{d})$, with $d$ square-free. The ring of integers of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \bmod 4$ and $\mathbb{Z}[\sqrt{d}]$ otherwise. In both cases $\mathbb{Q}(\sqrt{d})$ is monogenic.

Let $\zeta_n$ be a primitive $n^{\text{th}}$ root of unity and consider the $n^{\text{th}}$ cyclotomic field $\mathbb{Q}(\zeta_n)$.

# Our First Friends

Take $\mathbb{Q}(\sqrt{d})$, with $d$ square-free. The ring of integers of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \bmod 4$ and $\mathbb{Z}[\sqrt{d}]$ otherwise. In both cases $\mathbb{Q}(\sqrt{d})$ is monogenic.

Let $\zeta_n$ be a primitive $n^{\text{th}}$ root of unity and consider the $n^{\text{th}}$ cyclotomic field $\mathbb{Q}(\zeta_n)$. It is a bit more difficult than in the quadratic case, but one can show that the ring of integers of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$.

# Our First Friends

Take $\mathbb{Q}(\sqrt{d})$, with $d$ square-free. The ring of integers of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \bmod 4$ and $\mathbb{Z}[\sqrt{d}]$ otherwise. In both cases $\mathbb{Q}(\sqrt{d})$ is monogenic.

Let $\zeta_n$ be a primitive $n^{\text{th}}$ root of unity and consider the $n^{\text{th}}$ cyclotomic field $\mathbb{Q}(\zeta_n)$. It is a bit more difficult than in the quadratic case, but one can show that the ring of integers of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$.

The maximal real subfield of the $n^{\text{th}}$ cyclotomic field is $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

# Our First Friends

Take $\mathbb{Q}(\sqrt{d})$, with $d$ square-free. The ring of integers of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \bmod 4$ and $\mathbb{Z}[\sqrt{d}]$ otherwise. In both cases $\mathbb{Q}(\sqrt{d})$ is monogenic.

Let $\zeta_n$ be a primitive $n^{\text{th}}$ root of unity and consider the $n^{\text{th}}$ cyclotomic field $\mathbb{Q}(\zeta_n)$. It is a bit more difficult than in the quadratic case, but one can show that the ring of integers of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$.

The maximal real subfield of the $n^{\text{th}}$ cyclotomic field is $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. These number fields are also monogenic with $\zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n)$ providing a generator.

# "All that glistens is not gold."

Does this always happen? When one is learning (or discovering) algebraic number theory, they might be tempted to think every extension of $\mathbb{Q}$ is monogenic.

# “All that glistens is not gold.”

Does this always happen? When one is learning (or discovering) algebraic number theory, they might be tempted to think every extension of $\mathbb{Q}$ is monogenic. It works for the first few families of number fields we encounter, so maybe we expect it always happens.

# “All that glistens is not gold.”

Does this always happen? When one is learning (or discovering) algebraic number theory, they might be tempted to think every extension of $\mathbb{Q}$ is monogenic. It works for the first few families of number fields we encounter, so maybe we expect it always happens.

*Expectation is the root of all heartache.*

- William Shakespeare

# Dedekind-Kummer Factorization

**Theorem (Dedekind building on work of Kummer)**

*Let $f(x)$ be a monic, irreducible polynomial in $\mathbb{Z}[x]$ with $\alpha$ denoting a root. If $p \in \mathbb{Z}$ is a prime that does not divide $[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]]$, then the factorization of $p$ in $\mathcal{O}_{\mathbb{Q}(\alpha)}$ mirrors the factorization of $f(x)$ in $\mathbb{F}_p[x]$.*

# Dedekind-Kummer Factorization

**Theorem (Dedekind building on work of Kummer)**

*Let $f(x)$ be a monic, irreducible polynomial in $\mathbb{Z}[x]$ with $\alpha$ denoting a root. If $p \in \mathbb{Z}$ is a prime that does not divide $[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]]$, then the factorization of $p$ in $\mathcal{O}_{\mathbb{Q}(\alpha)}$ mirrors the factorization of $f(x)$ in $\mathbb{F}_p[x]$. That is,*

$$f(x) \equiv f_1(x)^{e_1} \cdots f_r(x)^{e_r} \bmod p \quad \textit{and} \quad p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

# Dedekind-Kummer Factorization

**Theorem (Dedekind building on work of Kummer)**

*Let $f(x)$ be a monic, irreducible polynomial in $\mathbb{Z}[x]$ with $\alpha$ denoting a root. If $p \in \mathbb{Z}$ is a prime that does not divide $[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]]$, then the factorization of $p$ in $\mathcal{O}_{\mathbb{Q}(\alpha)}$ mirrors the factorization of $f(x)$ in $\mathbb{F}_p[x]$. That is,*

$$f(x) \equiv f_1(x)^{e_1} \cdots f_r(x)^{e_r} \bmod p \quad \textit{and} \quad p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

For example, consider $\mathbb{Q}(\alpha)$ where $\alpha$ is a root of $x^3 - x^2 - 2x - 8$.

# Dedekind-Kummer Factorization

**Theorem (Dedekind building on work of Kummer)**

*Let $f(x)$ be a monic, irreducible polynomial in $\mathbb{Z}[x]$ with $\alpha$ denoting a root. If $p \in \mathbb{Z}$ is a prime that does not divide $[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]]$, then the factorization of $p$ in $\mathcal{O}_{\mathbb{Q}(\alpha)}$ mirrors the factorization of $f(x)$ in $\mathbb{F}_p[x]$. That is,*

$$f(x) \equiv f_1(x)^{e_1} \cdots f_r(x)^{e_r} \bmod p \quad \textit{and} \quad p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

For example, consider $\mathbb{Q}(\alpha)$ where $\alpha$ is a root of $x^3 - x^2 - 2x - 8$. Dedekind computed the factorization $(2) = \mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_2''$.

# Dedekind-Kummer Factorization

**Theorem (Dedekind building on work of Kummer)**

*Let $f(x)$ be a monic, irreducible polynomial in $\mathbb{Z}[x]$ with $\alpha$ denoting a root. If $p \in \mathbb{Z}$ is a prime that does not divide $[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]]$, then the factorization of $p$ in $\mathcal{O}_{\mathbb{Q}(\alpha)}$ mirrors the factorization of $f(x)$ in $\mathbb{F}_p[x]$. That is,*

$$f(x) \equiv f_1(x)^{e_1} \cdots f_r(x)^{e_r} \bmod p \quad \textit{and} \quad p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

For example, consider $\mathbb{Q}(\alpha)$ where $\alpha$ is a root of $x^3 - x^2 - 2x - 8$. Dedekind computed the factorization $(2) = \mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_2''$.

Thus, if this field is monogenic, there is a cubic polynomial that generates and has **three** distinct linear factors in $\mathbb{F}_2[x]$.

# Dedekind-Kummer Factorization

**Theorem (Dedekind building on work of Kummer)**

*Let $f(x)$ be a monic, irreducible polynomial in $\mathbb{Z}[x]$ with $\alpha$ denoting a root. If $p \in \mathbb{Z}$ is a prime that does not divide $[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]]$, then the factorization of $p$ in $\mathcal{O}_{\mathbb{Q}(\alpha)}$ mirrors the factorization of $f(x)$ in $\mathbb{F}_p[x]$. That is,*

$$f(x) \equiv f_1(x)^{e_1} \cdots f_r(x)^{e_r} \bmod p \quad \textit{and} \quad p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

For example, consider $\mathbb{Q}(\alpha)$ where $\alpha$ is a root of $x^3 - x^2 - 2x - 8$. Dedekind computed the factorization $(2) = \mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_2''$.

Thus, if this field is monogenic, there is a cubic polynomial that generates and has **three** distinct linear factors in $\mathbb{F}_2[x]$. In this case we say 2 is a *common index divisor.*

# Division Fields

# Cyclotomic Fields $\mathbb{Q}(\mathbb{G}_m[n])$ and Division Fields $\mathbb{Q}(A[n])$

Recall that the $n^{\text{th}}$ $\mathbb{G}_m$ division field (the $n^{\text{th}}$ cyclotomic field) is monogenic. In analogy with $\mathbb{G}_m$, we can ask about the division fields of other abelian groups, like elliptic curve and other abelian varieties.

# Cyclotomic Fields $\mathbb{Q}(\mathbb{G}_m[n])$ and Division Fields $\mathbb{Q}(A[n])$

Recall that the $n^{\text{th}}$ $\mathbb{G}_m$ division field (the $n^{\text{th}}$ cyclotomic field) is monogenic. In analogy with $\mathbb{G}_m$, we can ask about the division fields of other abelian groups, like elliptic curve and other abelian varieties.

Motivating question: When is $\mathbb{Q}(A[n])$ monogenic?

# Cyclotomic Fields $\mathbb{Q}(\mathbb{G}_m[n])$ and Division Fields $\mathbb{Q}(A[n])$

Recall that the $n^{\text{th}}$ $\mathbb{G}_m$ division field (the $n^{\text{th}}$ cyclotomic field) is monogenic. In analogy with $\mathbb{G}_m$, we can ask about the division fields of other abelian groups, like elliptic curve and other abelian varieties.

Motivating question: When is $\mathbb{Q}(A[n])$ monogenic?

Slightly more approachable, but still difficult question: When is $\mathbb{Q}(E[n])$ monogenic?

# Cyclotomic Fields $\mathbb{Q}(\mathbb{G}_m[n])$ and Division Fields $\mathbb{Q}(A[n])$

Recall that the $n^{\text{th}}$ $\mathbb{G}_m$ division field (the $n^{\text{th}}$ cyclotomic field) is monogenic. In analogy with $\mathbb{G}_m$, we can ask about the division fields of other abelian groups, like elliptic curve and other abelian varieties.

Motivating question: When is $\mathbb{Q}(A[n])$ monogenic?

Slightly more approachable, but still difficult question: When is $\mathbb{Q}(E[n])$ monogenic?

Gonzáles-Jiménez and Lozano-Robledo show that $\mathbb{Q}(E[n])$ coincides with $\mathbb{Q}(\zeta_n)$ sometimes. In particular when $n = 2, 3, 4$, and 5 this can happen.

# Splitting in $\mathbb{Q}(E[n])$

Let $a_p$ be the trace of Frobenius at $p$, let $b_p$ be the index $[\mathcal{O}_K : \mathrm{End}_{\mathbb{F}_p}(E)]$, and write $\Delta_{\mathrm{End}}$ for the discriminant of $\mathrm{End}_{\mathbb{F}_p}(E)$.

# Splitting in $\mathbb{Q}(E[n])$

Let $a_p$ be the trace of Frobenius at $p$, let $b_p$ be the index $[\mathcal{O}_K : \mathrm{End}_{\mathbb{F}_p}(E)]$, and write $\Delta_{\mathrm{End}}$ for the discriminant of $\mathrm{End}_{\mathbb{F}_p}(E)$. Consider the matrix

$$\sigma_p = \begin{bmatrix} \frac{a_p + b_p\delta_{\mathrm{End}}}{2} & b_p \\ \frac{b_p(\Delta_{\mathrm{End}} - \delta_{\mathrm{End}})}{4} & \frac{a_p - b_p\delta_{\mathrm{End}}}{2} \end{bmatrix}, \tag{1}$$

where $\delta_{\mathrm{End}} = 0, 1$ according to whether $\Delta_{\mathrm{End}} \equiv 0, 1$ modulo 4.

# Splitting in $\mathbb{Q}(E[n])$

Let $a_p$ be the trace of Frobenius at $p$, let $b_p$ be the index $[\mathcal{O}_K : \mathrm{End}_{\mathbb{F}_p}(E)]$, and write $\Delta_{\mathrm{End}}$ for the discriminant of $\mathrm{End}_{\mathbb{F}_p}(E)$. Consider the matrix

$$\sigma_p = \begin{bmatrix} \frac{a_p + b_p\delta_{\mathrm{End}}}{2} & b_p \\ \frac{b_p(\Delta_{\mathrm{End}} - \delta_{\mathrm{End}})}{4} & \frac{a_p - b_p\delta_{\mathrm{End}}}{2} \end{bmatrix}, \tag{1}$$

where $\delta_{\mathrm{End}} = 0, 1$ according to whether $\Delta_{\mathrm{End}} \equiv 0, 1$ modulo 4.

[Duke and Tóth, 2002]: Suppose $n$ is prime to $p$. When reduced modulo $n$, the matrix $\sigma_p$ yields a global representation of the Frobenius class over $p$ in $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$. In particular, the order of $\sigma_p$ modulo $n$ is the residue class degree of $p$ in $\mathbb{Q}(E[n])$.

# Results for Division Fields of Elliptic Curves

# Main Result A

There are a lot of division fields $\mathbb{Q}(E[n])$ that are not monogenic!

# Main Result A

There are a lot of division fields $\mathbb{Q}(E[n])$ that are not monogenic!

**Algorithm/theorem statement for $p = 2$ (Smith)**

*If $E$ is an elliptic curve over $\mathbb{Q}$ whose reduction at the prime 2 has trace of Frobenius $a_2$ and such that, for one of the $n$ listed on the following slide, the Galois representation*

$$\rho_{E,n} : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

*is surjective. Then $\mathbb{Q}(E[n])$ is not monogenic. Moreover, 2 is a common index divisor of $\mathbb{Q}(E[n])$.*

# Results for $p = 2$

| $a_2$ | $\sigma_2$ | non-monogenic $n$ |
|---|---|---|
| 0 | $\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$ | 3, 5, 9, 11, 15, 17, 21, 27, 33, 43, 51, 57, 63, 85, 91, 93, 105, 117, 129, 171, 195, 255, 257, 273, 315, 331, 341, 381, 455, 513, 585, 657, 683, 771, 819, 993 |
| 1 | $\begin{bmatrix} 1 & 1 \\ -2 & 0 \end{bmatrix}$ | 11 |
| -1 | $\begin{bmatrix} 0 & 1 \\ -2 & -1 \end{bmatrix}$ | 11, 23 |
| 2 | $\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ | 5, 13, 15, 17, 41, 51, 65, 85, 91, 105, 117, 145, 195, 205, 255, 257, 273, 315, 455, 565, 585, 771, 819 |
| $-2$ | $\begin{bmatrix} -1 & 1 \\ -1 & -1 \end{bmatrix}$ | 5, 13, 15, 17, 41, 51, 65, 85, 91, 105, 117, 145, 195, 205, 255, 257, 273, 315, 455, 565, 585, 771, 819 |

## Main Result B

There are a lot of division fields $\mathbb{Q}(E[n])$ that are not monogenic!

# Main Result B

There are a lot of division fields $\mathbb{Q}(E[n])$ that are not monogenic!

**Theorem (Smith)**

*Let $E/\mathbb{Q}$ be an elliptic curve without CM, then for infinitely many $n > 1$ the division field $\mathbb{Q}(E[n])$ is not monogenic.*

# Results for Abelian Varieties of Dimension $> 1$

# ...Or How to Sound Like You Understood a Talk

If you do something for elliptic curves, you can always ask the question, “Can I do this for abelian varieties?”

# Difficulties

The construction of the Frobenius in [Duke and Tóth, 2002] was very important for our work with elliptic curves. They use Deuring lifting for their construction. For an arbitrary abelian variety such a canonical lift does not necessarily exist.

# Difficulties

The construction of the Frobenius in [Duke and Tóth, 2002] was very important for our work with elliptic curves. They use Deuring lifting for their construction. For an arbitrary abelian variety such a canonical lift does not necessarily exist. Canonical lifts exist if we restrict to ordinary or almost ordinary abelian varieties, but we are interested in low $p$-rank too.

# Difficulties

Instead, we opted to generalize the approach taken by [Centeleghe, 2016] This approach relies on the fact that if $A$ is an abelian variety over a field $k$ with CM by a Gorenstein ring (i.e., if $\mathrm{End}_k(A)$ is a Gorenstein ring), then the Tate module $T_l(A)$ is free of rank one over $\mathrm{End}_k(A) \otimes \mathbb{Z}_l$.

# Difficulties

Instead, we opted to generalize the approach taken by [Centeleghe, 2016] This approach relies on the fact that if $A$ is an abelian variety over a field $k$ with CM by a Gorenstein ring (i.e., if $\mathrm{End}_k(A)$ is a Gorenstein ring), then the Tate module $T_l(A)$ is free of rank one over $\mathrm{End}_k(A) \otimes \mathbb{Z}_l$. This is great! Now we **just** need to write down a basis for the relevant orders in an arbitrary CM field of degree $2g$, where the dimension $g$ is greater than 1.

# Difficulties

Instead, we opted to generalize the approach taken by [Centeleghe, 2016] This approach relies on the fact that if $A$ is an abelian variety over a field $k$ with CM by a Gorenstein ring (i.e., if $\mathrm{End}_k(A)$ is a Gorenstein ring), then the Tate module $T_l(A)$ is free of rank one over $\mathrm{End}_k(A) \otimes \mathbb{Z}_l$. This is great! Now we **just** need to write down a basis for the relevant orders in an arbitrary CM field of degree $2g$, where the dimension $g$ is greater than 1. Even if we restrict to $g = 2$ and to maximal orders, this last step is difficult and results in an overwhelming number of cases.

# Difficulties

Instead, we opted to generalize the approach taken by [Centeleghe, 2016] This approach relies on the fact that if $A$ is an abelian variety over a field $k$ with CM by a Gorenstein ring (i.e., if $\mathrm{End}_k(A)$ is a Gorenstein ring), then the Tate module $T_l(A)$ is free of rank one over $\mathrm{End}_k(A) \otimes \mathbb{Z}_l$. This is great! Now we **just** need to write down a basis for the relevant orders in an arbitrary CM field of degree $2g$, where the dimension $g$ is greater than 1. Even if we restrict to $g = 2$ and to maximal orders, this last step is difficult and results in an overwhelming number of cases. Thus we focus on the minimal case.

# The Minimal Endomorphism Ring

Suppose $|k| = p^m = q$. $\mathrm{End}_k(A)$ must contain **Frobenius** $\pi$ and its dual **verschiebung** $v$. In fact, all orders of $\mathrm{End}_k(A) \otimes \mathbb{Q}$ containing $\pi$ and $v$ are endomorphism rings. Thus the smallest possible endomorphism ring is $\mathbb{Z}[\pi, v]$.

# The Minimal Endomorphism Ring

Suppose $|k| = p^m = q$. $\mathrm{End}_k(A)$ must contain **Frobenius** $\pi$ and its dual **verschiebung** $v$. In fact, all orders of $\mathrm{End}_k(A) \otimes \mathbb{Q}$ containing $\pi$ and $v$ are endomorphism rings. Thus the smallest possible endomorphism ring is $\mathbb{Z}[\pi, v]$.

The characteristic polynomial of $\pi$ and $v$ is a *Weil q-polynomial*. We restrict to abelian varieties with irreducible Weil $q$-polynomials so that $\mathbb{Z}[\pi, v]$ is Gorenstein.

# The Matrix Representing Frobenius

Let $A/k$ be an abelian variety with $\mathrm{End}_k(A) \cong \mathbb{Z}[\pi, v]$.

# The Matrix Representing Frobenius

Let $A/k$ be an abelian variety with $\mathrm{End}_k(A) \cong \mathbb{Z}[\pi, v]$. First note that $\{1, \pi, \ldots, \pi^g, v, \ldots, v^{g-1}\}$ forms a $\mathbb{Z}$-basis for $\mathbb{Z}[\pi, v]$.

Write

$$f(x) = x^{2g} + a_{2g-1}x^{2g-1} + \cdots + a_1 x + a_0$$

for the Weil $q$-polynomial of $A$. The following matrix yields the action of $\pi$ on $\mathbb{Z}[\pi, v]$, and hence on $T_l(A)$.

# The Matrix Representing Frobenius

$$
\sigma_{\mathfrak{p}} = \begin{array}{cc}
\begin{array}{ccccccccccc} 1 & \pi & \pi^2 & \pi^{g-2} & \pi^{g-1} & \pi^g & v & v^2 & v^3 & & v^{g-1} \end{array} & \\
\begin{bmatrix}
0 & 0 & 0 & \dots & 0 & -qa_{g+1} & q & 0 & 0 & \dots & 0 \\
1 & 0 & 0 & \dots & 0 & -a_g & 0 & 0 & 0 & \dots & 0 \\
0 & 1 & 0 & \dots & 0 & -a_{g+1} & 0 & 0 & 0 & \dots & 0 \\
\vdots & \vdots & \ddots & \dots & \vdots & -a_{g+i-1} & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & \dots & 1 & 0 & -a_{2g-2} & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & \dots & 0 & 1 & -a_{2g-1} & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & \dots & 0 & 0 & -qa_2 & 0 & q & 0 & \dots & 0 \\
0 & 0 & \dots & 0 & 0 & -qa_3 & 0 & 0 & q & \dots & 0 \\
0 & 0 & \dots & 0 & 0 & -qa_{i+1} & \vdots & \vdots & & \ddots & 0 \\
0 & 0 & \dots & 0 & 0 & -qa_{g-1} & 0 & 0 & 0 & \dots & q \\
0 & 0 & \dots & 0 & 0 & -q & 0 & 0 & 0 & \dots & 0
\end{bmatrix} &
\begin{array}{c} 1 \\ \pi \\ \pi^2 \\ \pi^i \\ \pi^{g-1} \\ \pi^g \\ v \\ v^2 \\ v^i \\ v^{g-2} \\ v^{g-1} \end{array}
\end{array}
$$

# Non-monogenic Division Fields of Abelian Surfaces

**Algorithm/theorem statement for $p = 2$ (Smith)**

*Let $A/\mathbb{F}_p$ be an abelian surface and write the Weil polynomial of $A$ as*

$$x^4 + a_3x^3 + a_2x^2 + pa_3x + p^2.$$

*Suppose the Weil polynomial is irreducible,* $\mathrm{End}_k(A)$ *is minimal, and*

$$\rho_{\hat{A},n} : \mathrm{Gal}(\mathbb{Q}(\hat{A}[n])/\mathbb{Q}) \to \mathrm{GSp}_4(\mathbb{Z}/n\mathbb{Z})$$

*is surjective for some $\hat{A}$ that reduces to $A$ modulo $p$. The following tables show the $n < 500$ for which the prime 2 is a common index divisor of $\mathbb{Q}(\hat{A}[n])$ over $\mathbb{Q}$.*

# Non-monogenic Division Fields of Abelian Surfaces

| $a_3$ | $a_2$ | $p$-rank | non-monogenic $n$ |
|---|---|---|---|
| -3 | 5 | 2 | 3, 19, 31, 57, 61, 93, 171, 183 |
| -2 | 2 | 0 | 5, 7, 9, 13, 15, 21, 35, 37, 39, 45, 51, 61, 63, 65, 85, 91, 105, 109, 111, 117, 119, 133, 135, 153, 171, 185, 189, 195, 205, 219, 221, 241, 247, 255, 259, 273, 285, 305, 315, 325, 327, 333, 351, 357, 365, 377, 399, 455, 481, 485 |
| -2 | 3 | 2 | 7, 47 |
| -1 | -1 | 2 | 5, 9, 11, 15, 23, 37, 43, 45, 67, 111, 127, 135, 151, 185, 203, 301, 333 |
| -1 | 0 | 1 | 47 |
| -1 | 1 | 2 | 3, 9, 103, 127 |
| -1 | 3 | 2 | 5, 15, 59 |
| 0 | -3 | 2 | 3, 5, 9, 11, 15, 23, 29, 33, 37, 45, 53, 87, 111, 135, 137, 185, 203, 233, 281, 301, 333 |
| 0 | -2 | 0 | 3, 5, 7, 9, 11, 13, 15, 19, 21, 27, 33, 35, 39, 43, 45, 51, 57, 63, 65, 67, 73, 77, 81, 85, 91, 93, 99, 105, 109, 111, 117, 119, 129, 133, 135, 151, 153, 171, 185, 189, 195, 201, 217, 219, 221, 231, 241, 247, 255, 259, 273, 279, 285, 301, 315, 327, 331, 333, 337, 341, 351, 357, 365, 381, 387, 399, 441, 453, 455, 481, 485 |

**Table 1:** $n < 500$ where 2 is a common index divisor in $\mathbb{Q}(\hat{A}[n])$

# Non-monogenic Division Fields of Abelian Surfaces

| $a_3$ | $a_2$ | $p$-rank | non-monogenic $n$ |
|---|---|---|---|
| 0 | -1 | 2 | 3, 17, 19, 23, 31, 57, 61, 93, 171, 183, 229 |
| 0 | 1 | 2 | 3, 9, 17, 19, 23, 47, 57, 61, 69, 93, 171, 183, 229 |
| 0 | 2 | 0 | 3, 5, 7, 9, 13, 15, 19, 21, 27, 31, 35, 39, 45, 49, 51, 57, 63, 65, 73, 77, 85, 89, 91, 93, 99, 105, 109, 111, 117, 119, 127, 133, 135, 151, 153, 161, 171, 185, 189, 195, 217, 219, 221, 231, 241, 247, 255, 259, 273, 279, 285, 301, 315, 327, 331, 333, 337, 341, 351, 357, 365, 381, 387, 399, 441, 453, 455, 481, 485 |
| 1 | -1 | 2 | 5, 7, 9, 11, 15, 37, 43, 45, 67, 79, 111, 135, 185, 203, 301, 333 |
| 1 | 0 | 1 | 47 |
| 1 | 1 | 2 | 3, 9 |
| 1 | 3 | 2 | 5, 15, 59 |
| 2 | 2 | 0 | 5, 7, 9, 13, 15, 21, 35, 37, 39, 45, 51, 61, 63, 65, 85, 91, 105, 109, 111, 117, 119, 133, 135, 153, 171, 185, 189, 195, 205, 219, 221, 241, 247, 255, 259, 273, 285, 305, 315, 325, 327, 333, 351, 357, 365, 377, 399, 455, 481, 485 |
| 2 | 3 | 2 | 7, 47 |
| 3 | 5 | 2 | 3, 19, 31, 57, 61, 93, 171, 183 |

**Table 2:** $n < 500$ where 2 is a common index divisor in $\mathbb{Q}(\hat{A}[n])$

**Algorithm/theorem statement for $p = 2$ (Smith)**

*Let $A/\mathbb{F}_p$ be an abelian threefold and write the Weil polynomial of $A$ as*

$$x^6 + a_5x^5 + a_4x^4 + a_3x^3 + pa_5x^2 + p^2a_4x + p^3.$$

*Suppose the Weil polynomial is irreducible,* $\mathrm{End}_k(A)$ *is minimal, and*

$$\rho_{\hat{A},n} : \mathrm{Gal}(\mathbb{Q}(\hat{A}[n])/\mathbb{Q}) \to \mathrm{GSp}_6(\mathbb{Z}/n\mathbb{Z})$$

*is surjective for some $\hat{A}$ that reduces to $A$ modulo $p$. The following tables show the $n < 200$ for which the prime 2 is a common index divisor of $\mathbb{Q}(\hat{A}[n])$ over $\mathbb{Q}$.*

# Non-monogenic Division Fields of Abelian Threefolds

| $a_5$ | $a_4$ | $a_3$ | $p$-rank | non-monogenic $n$ | $a_5$ | $a_4$ | $a_3$ | $p$-rank | non-monogenic $n$ |
|---|---|---|---|---|---|---|---|---|---|
| -4 | 9 | -15 | 3 | 7, 11, 23, 29, 43, 71, 87, 113, 127 | 0 | 1 | -3 | 3 | 3, 9 |
| -3 | 2 | 1 | 3 | 7, 11, 29, 43, 71, 87, 113, 127 | 0 | 1 | -1 | 3 | |
| -3 | 6 | -9 | 3 | 3, 9, 27, 153 | 0 | 1 | 3 | 3 | 3, 9 |
| -2 | 0 | 3 | 3 | 107, 149 | 0 | 2 | -2 | 0 | |
| -2 | 1 | 0 | 2 | 3, 5, 11, 55, 83 | 0 | 2 | -1 | 3 | 7 |
| -2 | 3 | -5 | 3 | 3, 9, 27, 59, 63 | 1 | -1 | -5 | 3 | 3, 9 |
| -2 | 3 | -3 | 3 | 5, 83, 131 | 1 | -1 | -4 | 2 | 3, 7, 49 |
| -2 | 5 | -7 | 3 | 3, 7 | 1 | 0 | -3 | 3 | 7, 77, 103 |
| -1 | -1 | 5 | 3 | 3, 9 | 1 | 0 | 1 | 3 | 3 |
| -1 | 0 | -1 | 3 | 3 | 1 | 1 | 0 | 2 | 3, 7 |
| 0 | 0 | -3 | 3 | 3, 7, 9, 13, 15, 21, 27, 29, 31, 35, 39, 45, 63, 65, 87, 91, 93, 105, 117, 123, 141, 151, 195 | 2 | 4 | 6 | 0 | 3 |
| 0 | 0 | -2 | 0 | 3, 7, 11, 15, 23, 29, 37, 45, 67, 71, 79 | 2 | 5 | 7 | 3 | 3, 7 |
| 0 | 0 | -1 | 3 | 3, 5, 7, 15, 19, 21, 25, 35, 45, 63, 71, 75, 95, 97, 105, 123, 133 | 3 | 2 | -1 | 3 | 7, 11, 23, 29, 43, 71, 87, 113, 127 |
| 0 | 0 | 1 | 3 | 3, 5, 7, 15, 19, 21, 25, 35, 45, 47, 49, 63, 75, 95, 97, 105, 123, 133 | 3 | 5 | 7 | 3 | 7 |
| 0 | 0 | 2 | 0 | 3, 7, 11, 15, 23, 29, 37, 45, 67 | 3 | 6 | 9 | 3 | 3, 9, 27, 153 |
| 0 | 0 | 3 | 3 | 3, 7, 9, 13, 15, 21, 27, 29, 31, 35, 39, 45, 47, 63, 65, 71, 87, 91, 93, 105, 117, 123, 141, 151, 195 | 4 | 9 | 15 | 3 | 7, 11, 29, 43, 71, 87, 113, 127 |

# Thank You!

Centeleghe, T. G. (2016).

**Integral Tate modules and splitting of primes in torsion fields of elliptic curves.**

*Int. J. Number Theory*, 12(1):237–248.

Centeleghe, T. G. and Stix, J. (2015).

**Categories of abelian varieties over finite fields, I: Abelian varieties over $\mathbb{F}_p$.**

*Algebra Number Theory*, 9(1):225–265.

Duke, W. and Tóth, A. (2002).

**The splitting of primes in division fields of elliptic curves.**

*Experiment. Math.*, 11(4):555–565 (2003).

Smith, H. (2021).

**Non-monogenic division fields of elliptic curves.**

*J. Number Theory*, 228:174–187.

Waterhouse, W. C. (1969).

**Abelian varieties over finite fields.**

*Ann. Sci. École Norm. Sup. (4)*, 2:521–560.

# An Example with an Ordinary Elliptic Curve

Suppose $E$ is an elliptic curve with $a_2 = 1$. The characteristic polynomial of Frobenius is $x^2 - x + 2$ and this has discriminant $-7$. Letting $\pi$ denote the Frobenius endomorphism of $E$ over $\mathbb{F}_2$, we have $\mathrm{End}_{\mathbb{F}_2}(E) \cong \mathbb{Z}[\pi] = \mathcal{O}_{\mathbb{Q}(\pi)}$.

Combining all this information, we see Duke and Tóth's matrix representing $\pi$ is

$$\sigma_2 = \begin{bmatrix} 8/2 & (-7 \cdot 8)/4 \\ 1 & -6/2 \end{bmatrix} = \begin{bmatrix} 4 & -14 \\ 1 & -3 \end{bmatrix}.$$

Denote the order of $\sigma_2$ modulo $n$ by $\mathrm{ord}\,(\sigma_2, n)$. This is the residue class degree of 2 in $\mathbb{Q}(E[n])$.

# An Example with an Ordinary Elliptic Curve

Generically, we expect the degree of $\mathbb{Q}(E[n])$ over $\mathbb{Q}$ to be $|\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})|$. Thus 2 will split into $\frac{|\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})|}{\operatorname{ord}(\sigma_2,n)}$ primes in $\mathbb{Q}(E[n])$.

The number of irreducible polynomials of degree $m$ in $\mathbb{F}_p[x]$ is $\dfrac{1}{m}\sum_{d|m} p^d \mu\left(\dfrac{m}{d}\right)$. With Dedekind's factorization theorem in mind, we compare $\frac{|\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})|}{\operatorname{ord}(\sigma_2,n)}$ and $\frac{1}{\operatorname{ord}(\sigma_2,n)} \sum\limits_{d|\operatorname{ord}(\sigma_2,n)} 2^d \mu\left(\frac{\operatorname{ord}(\sigma_2,n)}{d}\right)$.

If the number of irreducible polynomial of degree $\operatorname{ord}(\sigma_2, n)$ in $\mathbb{F}_2[x]$ is less than $\dfrac{|\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})|}{\operatorname{ord}(\sigma_2, n)}$, then 2 must divide the index of any monogenic order in $\mathcal{O}_{\mathbb{Q}(E[n])}$. We find that $\sigma_2$ has order 10 modulo 11, so that 2 splits into 1320 primes in $\mathbb{Q}(E[11])$. There are only 99 irreducible polynomials of degree 10 in $\mathbb{F}_2[x]$. Thus 2 is a common index divisor of $\mathbb{Q}(E[11])$ over $\mathbb{Q}$.