Addition law structure of elliptic curves

David Kohel

Institut de Mathématiques de Luminy
Université de la Méditerranée
163, avenue de Luminy, Case 907
13288 Marseille Cedex 9
France

Abstract

The study of alternative models for elliptic curves has found recent interest from cryptographic applications, once it was recognized that such models provide more efficiently computable algorithms for the group law than the standard Weierstrass model. Examples of such models arise via symmetries induced by a rational torsion structure. We analyze the module structure of the space of sections of the addition morphisms, determine explicit dimension formulas for the spaces of sections and their eigenspaces under the action of torsion groups, and apply this to specific models of elliptic curves with parametrized torsion subgroups.

1. Introduction

Let k be a field and A an abelian variety over k with a given projective embedding $\iota : A \to \mathbb{P}^r$, determined by the complete linear system associated to an invertible sheaf $\mathscr{L} = \mathcal{O}_A(1) := \iota^*\mathcal{O}_{\mathbb{P}^r}(1)$. We denote the addition morphism on A by:

$$\mu : A \times A \to A.$$

An *addition law* is an $(r+1)$-tuple $\mathfrak{s} = (p_0, \ldots, p_r)$ of bihomogenous elements p_j of

$$k[X_0, \ldots, X_r]/I \otimes_k k[X_0, \ldots, X_r]/I,$$

where I is the defining ideal of A, such that the rational map

$$((x_0 : \ldots, x_r), (y_0 : \cdots : y_r)) \longmapsto (p_0(x,y) : \cdots : p_r(x,y))$$

defines μ on an open subset U of $A \times A$. The complement of U is called the *exceptional set* of $\mathfrak{s}$. Lange and Ruppert [17] give a characterization of addition laws, as sections of an invertible sheaf, from which it follows that the exceptional set of any nonzero addition law is the support of a divisor, which we refer to as the *exceptional divisor*. An addition law is said to have bidegree (m, n) if the polynomials $p_j(x, y)$ are homogeneous of degree m and n in x_i and y_j,

respectively. The set of addition laws of bidegree (m, n), together with the zero map, form a k-vector space.

A set S of addition laws is said to be *geometrically complete* if the intersection of the exceptional sets of all $\mathfrak{s}$ in S is empty, and *arithmetically complete* if this intersection contains no k-rational point. The original use of the term *complete* for geometrically complete in the literature [6, 17, 18] has more recently been supplanted by its use for arithmetically complete, in literature with a view to computational and cryptographic application. The intersection of the exceptional sets for $\mathfrak{s}$ in S clearly equals the intersection of the exceptional sets for all $\mathfrak{s}$ in its k-linear span.

The structure of addition laws depends intrinsically not just on A, but also on the embedding $\iota : A \to \mathbb{P}^r$, determined by global sections $s_0, \ldots, s_r$ in $\Gamma(A, \mathscr{L})$, for the sheaf $\mathscr{L} = \mathcal{O}_A(1)$. We assume, moreover, that ι is a projectively normal embedding (see Birkenhake-Lange [5, Chap. 7, §3]), and in particular, that the global sections span $\Gamma(A, \mathscr{L})$. We recall that an invertible sheaf is said to be *symmetric* if $[-1]^*\mathscr{L} \cong \mathscr{L}$. Lange and Ruppert [17] determine the structure of addition laws, and in particular prove the following main theorem.

Theorem 1 (Lange-Ruppert). *Let $\iota : A \to \mathbb{P}^r$ be a projectively normal embedding of A, and $\mathscr{L} = \mathcal{O}_A(1)$. The set of addition laws of bidegrees $(2, 3)$ and $(3, 2)$ on A are geometrically complete. If $\mathscr{L}$ is symmetric, then the set of addition laws of bidegree $(2, 2)$ are geometrically complete, and otherwise empty.*

Remark. Lange and Ruppert assume the hypothesis that ι is defined with respect to the complete linear system of an invertible sheaf $\mathscr{L} \cong \mathscr{M}^m$ where $\mathscr{M}$ is ample and $m \geq 3$. Their hypothesis implies the projective normality of ι and the latter is sufficient for their proof. In the case of an elliptic curve, projective normality is equivalent to the surjectivity of $\Gamma(\mathbb{P}^r, \mathcal{O}(1))$ on $\Gamma(E, \mathscr{L})$.

In the case of elliptic curves, Bosma and Lenstra [6] give a precise description of the exceptional divisors of addition laws of bidegree $(2, 2)$ when A is an elliptic curve embedded as a Weierstrass model. Using this analysis, they prove that two addition laws are sufficient for a complete system. However, their description of the structure of addition laws applies more generally to other projective embeddings of an elliptic curve. We carry out this analysis to determine the dimensions of spaces of addition laws in families with rational torsion subgroups and study the module decomposition of these spaces with respect to the action of torsion.

In view of Theorem 1, the simplest possible structure of an addition law we might hope for is one for which the polynomials $p_j(x, y)$ are binomials of bidegree $(2, 2)$. Such addition laws are known for Hessian models [8, 15, 22] and Edwards models [1, 10] of elliptic curves. After recalling some background in Sections 2 and 3, and proving results about the exceptional divisors of addition laws, we introduce the concept of addition law projections in Section 4, then relate this with affine addition laws discussed in Sections 5 and 6. This provides a means of explicitly determining the dimensions of spaces of addition laws and constructing addition laws (via their projections) of bidegree $(1, 1)$. In

Section 7 we introduce a G-module structure of addition laws, with respect to a rational torsion subgroup on E. In the final section we give examples of addition laws, observing that the simple laws coincide with the uniquely determined one-dimensional eigenspaces for the G-module structure. In analogy with the known examples of Edwards and Hessian curves, we construct new embeddings of families with torsion structure to obtain efficient addition laws on elliptic curves with prescribed torsion structure.

2. Divisors and invertible sheaves on abelian varieties

Let A/k be an abelian variety. We denote the addition morphism by μ, the difference morphism by δ, and let $\pi_i : A \times A \to A$ be the projection maps, for i in $\{1, 2\}$. We denote by μ^*, δ^*, and π_i^* the respective pullback morphisms of divisors and sheaves from E to $E \times E$.

We use the bijective correspondence between Weil divisors and Cartier divisors on abelian varieties, and to such a divisor D we associate an invertible subsheaf $\mathscr{L}(D)$ of the sheaf $\mathscr{K}$ of total quotient rings such that for an effective divisor, $\mathscr{L}(D)^{-1}$ is the ideal sheaf of D (see Hartshorne [11, Chap. II, Sect. 6]). For $\mathscr{L}(D)$ so defined, its space of global sections is the Riemann-Roch space:

$$\Gamma(A, \mathscr{L}(D)) = \{f \in k(A) \ : \ \mathrm{div}(f) \geq D\},$$

and an embedding $A \to \mathbb{P}^r$ given by the complete linear system $|\mathscr{L}(D)|$ is determined by

$$P \longmapsto (x_0(P) : x_1(P) : \cdots : x_r(P)),$$

for a choice of basis $\{x_0, x_1, \ldots, x_r\}$ of $\Gamma(A, \mathscr{L}(D))$. If D is an effective Weil divisor we may take $x_0 = 1$, in which case we recover D as the intersection with the hyperplane $X_0 = 0$ in $\mathbb{P}^r$.

2.1. Sheaves associated to the addition morphism

Lange and Ruppert [17] interpret an addition law of bidegree (m, n) as a homomorphism of sheaves $\mu^*\mathscr{L} \to \pi_1^*\mathscr{L}^m \otimes \pi_2^*\mathscr{L}^n$, then use the identification

$$\mathrm{Hom}(\mu^*\mathscr{L}, \pi_1^*\mathscr{L}^m \otimes \pi_2^*\mathscr{L}^n) = \Gamma(A \times A, \mu^*\mathscr{L}^{-1} \otimes \pi_1^*\mathscr{L}^m \otimes \pi_2^*\mathscr{L}^n),$$

to determine their structure. In view of Theorem 1, we will be interested in symmetric invertible sheaves $\mathscr{L}$, and the structure of sections of the sheaves

$$\mathscr{M}_{m,n} = \mu^*\mathscr{L}^{-1} \otimes \pi_1^*\mathscr{L}^m \otimes \pi_2^*\mathscr{L}^n.$$

and for the critical case of $\mathscr{M}_{2,2}$ we write more concisely $\mathscr{M}$.

2.2. Invertible sheaves on elliptic curves

A Weierstrass model of an elliptic curve E with base point O is determined with respect to $\mathscr{L}(3(O))$ and any other cubic model in $\mathbb{P}^2$ is obtained as a projective linear automorphism of the Weierstrass model. As a prelude to the study of models determined by more general symmetric divisors, we recall the characterization of divisors on an elliptic curve. For a divisor D on an elliptic curve let $e(D)$ be its evaluation on the curve.

Lemma 2. *Let $\mathscr{L} = \mathscr{L}(D)$ be an invertible sheaf of degree d on E. Then $\mathscr{L} \cong \mathscr{L}((d-1)(O) + (P))$ where $P = e(D)$. Moreover $\mathscr{L}$ is symmetric if and only if P is in $E[2]$.*

In the final sections we introduce models defined by embeddings with respect to symmetric divisors $D = \sum_{i=1}^{d}(P_i)$ where $G = \{P_i\}$ forms a subgroup of rational points on E. The permutation action on the divisor implies that $[-1]$ and the translation-by-P_i morphisms induce automorphisms of the k-vector spaces of global sections, hence determine automorphisms of E induced by a linear transformation of $\mathbb{P}^r$, fixing a hyperplane at infinity.

2.3. Invertible sheaves on $E \times E$

Let μ, δ, π_1, and π_2 be the addition, difference, and projection morphisms, as above. We define

$$V = \{O\} \times E \text{ and } H = E \times \{O\}$$

as divisors on $E \times E$. Similarly, let Δ and ∇ be the diagonal and anti-diagonal images of E in $E \times E$, respectively.

Lemma 3. *With the above notation we have:*

$$\pi_1^*\mathscr{L}((O)) = \mathscr{L}(V), \qquad \pi_2^*\mathscr{L}((O)) = \mathscr{L}(H),$$
$$\mu^*\mathscr{L}((O)) = \mathscr{L}(\nabla), \qquad \delta^*\mathscr{L}((O)) = \mathscr{L}(\Delta).$$

In particular if $\mathscr{L} = \mathscr{L}(d(O))$, then

$$\mu^*\mathscr{L}^{-1} \otimes \pi_1^*\mathscr{L}^m \otimes \pi_2^*\mathscr{L}^n = \mathscr{L}(-d\nabla + dmV + dnH).$$

Proof. This is immediate from

$$V = \pi_1^*(O),\ H = \pi_2^*(O),\ \nabla = \mu^*(O) \text{ and } \Delta = \delta^*(O). \qquad \square$$

We note that each of V, H, ∇, and Δ is an elliptic curve isomorphic to E. In the generalization of the divisor on E from $3(O)$ to a more general Weil divisor, we obtain translates of these elementary divisors, which motivates the definitions

$$\mu^*(P) = \nabla + (P, O) = \nabla + (O, P),$$

and

$$\delta^*(P) = \Delta + (P, O) = \Delta + (O, -P).$$

2.4. Addition laws of bidegree $(2,2)$

We now classify the sheaves of addition laws of bidegree $(2,2)$. We recall the definition of the invertible sheaf

$$\mathscr{M} = \mu^*\mathscr{L}^{-1} \otimes \pi_1^*\mathscr{L}^2 \otimes \pi_2^*\mathscr{L}^2.$$

Following Bosma and Lenstra [6], we let x be a degree 2 function on E with poles only at O, and observe that for $x_1 = x \otimes 1$ and $x_2 = 1 \otimes x$ in $k(E) \otimes_k k(E) \subset k(E \times E)$, we have

$$\operatorname{div}(x_1 - x_2) = \nabla + \Delta - 2V - 2H.$$

Analogously, for a 2-torsion point T, after a suitable linear transformation, we may assume x satisfies $\operatorname{div}(x) = 2(T) - 2(O)$, and $x(P+T)x(P) = 1$, whence:

$$\operatorname{div}(x_1x_2 - 1) = \nabla_T + \Delta_T - 2V - 2H.$$

This establishes the following lemma.

Lemma 4. *For any point T in $E[2]$, we have $\Delta_T + \nabla_T \sim 2V + 2H$.*

This lemma yields the following isomorphism of symmetric invertible sheaves.

Lemma 5. *If $\mathscr{L}$ is a symmetric invertible sheaf on E, then*

$$\mu^*\mathscr{L} \otimes \delta^*\mathscr{L} \cong \pi_1^*\mathscr{L}^2 \otimes \pi_2^*\mathscr{L}^2,$$

and hence $\mathscr{M} \cong \delta^*\mathscr{L}$.

Proof. By Lemma 2, we have $\mathscr{L} \cong \mathscr{L}((T) + (d-1)(O))$ for some point T in $E[2]$, and hence $\mathscr{L}^2 \cong \mathscr{L}(2d(O))$. The lemma then follows by the equivalences of Lemma 4, extended linearly to $(T) + (d-1)(O)$. □

The following theorem extends the analysis of Section 4 of Bosma and Lenstra [6], following the lines of proof of Section 2 of Lange and Ruppert [17].

Theorem 6. *Let $\iota : E \to \mathbb{P}^r$ be a projectively normal embedding of an elliptic curve, with respect to a symmetric sheaf $\mathscr{L} = \mathcal{O}_E(1) \cong \mathscr{L}(D)$. Then the space of global sections of $\mathscr{M}$ is isomorphic to the space of global sections of $\mathscr{L}$. Moreover, the exceptional divisor of an addition law of bidegree $(2,2)$ associated to a section in $\Gamma(E \times E, \mathscr{M})$ is of the form $\sum_{i=1}^{d} \Delta_{P_i}$ where $D \sim \sum_i (P_i)$.*

Proof. In view of Lemma 5, and since δ has connected fibers, we deduce that the difference morphism induces an isomorphism $\delta^* : \Gamma(E, \mathscr{L}) \to \Gamma(E \times E, \delta^*\mathscr{L})$. The structure of the exceptional divisor follows since for $D \sim \sum_i (P_i)$, we have $\delta^*D \sim \sum_i \Delta_{P_i}$. □

Since each Δ_{P_i} is isomorphic to E over the algebraic closure of k, this theorem gives a simple characterization of the exceptional divisor, and of arithmetic completeness.

Corollary 7. *The exceptional divisor $\mathfrak{D}$ of an addition law of bidegree $(2,2)$ is equal to $\delta^*(D)$, where $\mathfrak{D} \cap (E \times \{O\}) = D \times \{O\}$.*

PROOF. Every translate of Δ is of the form $\Delta_P = \Delta + (P, O)$, where P is uniquely determined. Thus we have identities $\Delta_P \cap (E \times \{O\}) = (P, O)$ and $\Delta_P = \delta^*(P)$, which extend linearly to general sums of divisors of the form Δ_P. □

Corollary 8. *An addition law of bidegree $(2,2)$ is arithmetically complete if and only if no irreducible component of the exceptional divisor is absolutely irreducible.*

PROOF. Each component Δ_P is a translate of the diagonal image of E in $E \times E$. It follows that a component Δ_P has a rational point if and only if P is in $E(k)$, if and only if Δ_P is fixed by the absolute Galois group. □

3. Divisors and intersection theory

For higher bidegrees, we do not expect to have an isomorphism between the spaces addition laws and sections of an invertible sheaf on E. In order to determine the dimensions of these spaces, we require an explicit determination of the Euler-Poincaré characteristic $\chi(E \times E, \mathscr{L})$ as a tool for determining the dimension of $H_0(E \times E, \mathscr{L}) = \Gamma(E \times E, \mathscr{L})$.

3.1. Euler-Poincaré characteristic and divisor equivalence

For a projective variety X/k and a sheaf $\mathscr{F}$, and let $\chi(X, \mathscr{F})$ be the Euler-Poincaré characteristic:

$$\chi(X, \mathscr{F}) = \sum_{i=0}^{\infty} (-1)^i \dim_k(H^i(X, \mathscr{F})).$$

For the classification of divisors or invertible sheaves of X, we have considered the *linear equivalence* classes in $\mathrm{Pic}(X)$. In order to determine the dimensions of spaces of addition laws, it suffices to consider the coarser *algebraic equivalence* class in the *Néron-Severi group* of X, defined as

$$\mathrm{NS}(X) = \mathrm{Pic}(X)/\mathrm{Pic}^0(X).$$

For a surface X, a divisor D is *numerically equivalent* to zero if the intersection product $C.D$ is zero for all curves C on X. This gives the coarsest equivalence relation on X and we denote the group of divisors modulo numerical equivalence by $\mathrm{Num}(X)$. We refer to Lang [16], Chapter IV for the general definition of $\mathrm{Num}(X)$, and the equality between $\mathrm{Num}(X)$ and $\mathrm{NS}(X)$ for abelian varieties:

Lemma 9. *If X is an abelian variety then $\mathrm{NS}(X) = \mathrm{Num}(X)$.*

By definition of numerical equivalence, the intersection product is nondegenerate on $\mathrm{Num}(X)$. In the application to $X = E \times E$, we can determine the structure of $\mathrm{NS}(X)$.

Lemma 10. *The following diagram is exact.*

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \mathrm{Pic}^0(E) \times \mathrm{Pic}^0(E) & \longrightarrow & \mathrm{Pic}^0(E \times E) & \longrightarrow & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Pic}(E) \times \mathrm{Pic}(E) & \xrightarrow{\pi_1^* \times \pi_2^*} & \mathrm{Pic}(E \times E) & \longrightarrow & \mathrm{End}(E) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{NS}(E) \times \mathrm{NS}(E) & \longrightarrow & \mathrm{NS}(E \times E) & \longrightarrow & \mathrm{End}(E) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Proof. Exactness of the middle horizontal sequence is Exercise IV 4.10 of Hartshorne [11], and the vertical sequences are exact by definition of the Néron-Severi group. Exactness of the upper and lower sequences follows by commutativity of the diagram. □

We note that since $\mathrm{NS}(E)$ and $\mathrm{End}(E)$ are free abelian groups, the lower sequence splits, with the splitting sending an endomorphism φ to its graph Γ_φ. Summarising arguments from Lange and Ruppert [18], particularly the proof of Lemma 1.3, we now determine the intersection pairing on $\mathrm{NS}(E \times E)$,

Lemma 11. *The Neron-Severi group* $\mathrm{NS}(E \times E)$ *is a finitely generated free abelian group, and if* $\mathrm{End}(E) \cong \mathbb{Z}$*, it is generated by* V*,* H*,* Δ*, and* ∇*, modulo the relation* $\Delta + \nabla \equiv 2V + 2H$*. The intersection product is nondegenerate on* $\mathrm{NS}(E \times E)$ *and given by*

	V	H	Δ	∇
V	0	1	1	1
H	1	0	1	1
Δ	1	1	0	4
∇	1	1	4	0

Proof. The divisors V and H are the generators of $\pi_1^*(\mathrm{NS}(E))$ and $\pi_2^*(\mathrm{NS}(E))$. Since Δ and ∇ are the graphs of $[1]$ and $[-1]$, their sum induces the zero homomorphism, thus must lie in the image of $\pi_1^* \times \pi_2^*$. The expression for $\Delta + \nabla$ follows from the linear equivalence relation of Lemma 4. Each of V, H, Δ and ∇ has trivial self-intersection, since they have trivial intersections with their translates in $E \times E$. The identities

$$V.H = V.\Delta = V.\nabla = H.\Delta = H.\Delta = 1,$$

hold since each pair has a unique intersection point (O, O), and finally $\Delta.\nabla = 4$ follows from $|\Delta \cap \nabla| = |\{(T, T) : T \in E[2]\}| = 4$. □

In the case of complex multiplication, the generator set can be extended by additional independent divisors $\Gamma_{\varphi_1}, \ldots, \Gamma_{\varphi_{r-1}}$, where $\{1, \varphi_1, \ldots, \varphi_{r-1}\}$ is a basis for $\mathrm{End}(E)$, by the splitting of the lower sequence of Lemma 10.

Theorem 12. *Let E be an elliptic curve and $\mathscr{L}$ be an invertible sheaf on $E \times E$. The Euler characteristic $\chi(E \times E, \mathscr{L})$ depends only on the numerical equivalence class of $\mathscr{L}$, and in particular*

$$\chi(E \times E, \mathscr{L}(\mathfrak{D})) = \frac{1}{2}\mathfrak{D}.\mathfrak{D}.$$

If $\mathscr{L}$ is ample, then $\chi(E \times E, \mathscr{L}) = \dim_k(\Gamma(E \times E, \mathscr{L})$.

Proof. The first statement is the Riemann-Roch theorem for abelian surfaces (see Hartshorne [11, Chap. V, Theorem 1.6] or Birkenhake and Lange [5, Chap. 3, Corollary 6.2]). The last statement is the Kodaira Vanishing Theorem (see Remark 7.15 of Hartshorne [11]) together with the isomorphism $\omega_A \cong \mathcal{O}_A$ for any abelian variety A [5, Chap. 1, Lem. (4.2)].

The following corollary of Theorem 12 and Lemma 11 is a synthesis of results of Lange and Ruppert [17, 18].

Corollary 13 (Lange-Ruppert). *Let E be an elliptic curve, then*

$$\chi(E \times E, \mathscr{L}(x_0\nabla + x_1 V + x_2 H)) = x_0x_1 + x_0x_2 + x_1x_2.$$

In particular, if $\mathscr{L}$ is an invertible sheaf of degree $d > 0$ on E, then

$$\chi(E \times E, \mathscr{M}_{m,n}) = d^2(mn - m - n).$$

Lemma 14. *The sheaf $\mathscr{M}_{m,n}$ is ample if and only if $(m, n) > (2, 2)$.*

Proof. An ample invertible sheaf on a surface has positive self-intersection, by the Nakai-Moishezon Criterion, Chap. V, Theorem 1.10, Hartshorne [11], but $\mathscr{M}_{m,n} = \mathscr{L}(-d\nabla + dmV + dnV)$ has self-intersection $d^2(mn - m - n)$ which is positive only for $m, n \geq 2$ and $(m, n) \neq (2, 2)$. On the other hand, for $m > n \geq 2$, we have

$$\begin{aligned}\mathscr{M}_{m,n} &\cong \mathscr{L}(\Delta + (m-2)V + (n-2)H)^d \\ &= \mathscr{L}(\Delta + V)^d \otimes \mathscr{L}((m-3)V + (n-2)H)^d.\end{aligned}$$

The sheaf $\mathscr{L}(\Delta+V)$ is ample since it is the pullback of the ample sheaf $\mathscr{L}(H+V)$ under the isomorphism $(P, Q) \mapsto (P + Q, Q)$. Since $(m-3)V + (n-2)H$ is non-negative, it follows that $\mathscr{M}_{m,n}$ is ample. □

3.2. Dimensions of spaces of addition laws

We are now in a position to relate the dimension of $\Gamma(E \times E, \mathscr{M}_{m,n})$ to $\chi(E \times E, \mathscr{M}_{m,n})$. As a first step, we recall the statement of the Riemann-Roch theorem for elliptic curves.

Theorem 15. *If $\mathscr{L}$ is an invertible sheaf of degree $d > 0$ on an elliptic curve E, then $\mathscr{L}$ is ample and $\dim_k(\Gamma(E, \mathscr{L})) = d$.*

Corollary 16. *Let $\mathscr{L}$ be a symmetric ample invertible sheaf of degree d on an elliptic curve E and*

$$\mathscr{M}_{m,n} = \mu^* \mathscr{L}^{-1} \otimes \pi_1^* \mathscr{L}^m \otimes \pi_2^* \mathscr{L}^n.$$

Then for $(m, n) = (2, 2)$,

$$\dim_k(H^0(E \times E, \mathscr{M})) = \dim_k(H^1(E \times E, \mathscr{M})) = d,$$

and for all other $m, n \geq 2$,

$$\dim_k(H^0(E \times E, \mathscr{M}_{m,n})) = d^2(mn - m - n).$$

PROOF. Since $\mathscr{M}_{m,n}$ is isomorphic to $\mathscr{L}(\mathfrak{D})$ for an effective divisor $\mathfrak{D}$, we have that

$$H^2(E \times E, \mathscr{M}_{m,n}) \cong H^0(E \times E, \mathscr{M}_{m,n}^{-1}) = 0$$

by Serre duality [11, Chap. III, Cor. 7.7], since $\omega_A \cong \mathcal{O}_A$ for any abelian variety A [5, Chap. 1, Lem. (4.2)]. The dimension of the first cohomology group of $\mathscr{M}_{m,n}$ is then determined by the dimension of $H^0(E \times E, \mathscr{M}_{m,n})$ and the Euler characteristic of Theorem 13.

For $(m, n) = (2, 2)$, the dimension of $H^0(E \times E, \mathscr{M})$ is determined by Theorem 6 and Theorem 15, and for all higher bidegrees the sheaf $\mathscr{M}_{m,n}$ is ample and the Euler-Poincaré characteristic $\chi(E \times E, \mathscr{M}_{m,n})$ equals $\dim_k(H^0(E \times E, \mathscr{M}_{m,n}))$ by Theorem 12. □

In Section 4 we introduce the notion of an addition law projection, for which we generalize the above results on dimensions of spaces of addition laws. This yields dimension formulas for the affine addition laws introduced in Section 6.

3.3. Dimensions of sections of the ideal sheaf

When E is embedded as a cubic curve in $\mathbb{P}^2$, the defining ideal sheaf $\mathscr{I}_E$ of E has no sections of degree 2, which is to say that $\dim_k(\Gamma(\mathbb{P}^2, \mathscr{I}_E(2))) = 0$. However, a degree 4 or higher divisor always includes quadratic defining relations. This introduces an ambiguity in the polynomial representative for the addition law coordinates. In what follows, we note that when E is not contained in a hyperplane of $\mathbb{P}^r$, the ideal sheaf contains no linear relations, and the degree d equals $r + 1$, since a projective normal embedding is given by a complete linear system.

Lemma 17. *Let E be an elliptic curve and $\iota : E \to \mathbb{P}^r$ be a projectively normal embedding of degree d. Then for the ideal sheaf $\mathscr{I}_E$, we have*

$$\dim_k(\Gamma(\mathbb{P}^r, \mathscr{I}_E(n))) = \binom{n+r}{r} - nd.$$

PROOF. Let $\mathscr{L} = \mathcal{O}_E(1)$ and note that $\Gamma(\mathbb{P}^r, \mathcal{O}(n)) \to \Gamma(E, \mathscr{L}^n)$ is surjective by hypothesis. Thus the dimension is determined by the number of monomials of degree n in $r+1$ variables minus the dimension of the space $\Gamma(E, \mathscr{L}^n)$. This latter space has dimension nd by Riemann-Roch, from which the result follows. □

The polynomial representatives for the coordinates of an addition law of bidegree (m, n) are well-defined only up to elements of

$$I_{m,n} = \Gamma(\mathbb{P}^r, \mathscr{I}_E(m)) \otimes \Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(n)) + \Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(m)) \otimes \Gamma(\mathbb{P}^r, \mathscr{I}_E(n)).$$

Since, for $d \geq 4$, the dimension of $\Gamma(\mathbb{P}^r, \mathscr{I}_E(2))$ is nonzero, the addition laws for any nonplanar model have nonunique representation by polynomials. We make this more precise in the following corollary.

Corollary 18. *An addition law of bidegree (m, n) is represented by a coset of a vector space of polynomials whose dimension is*

$$(r+1)\left(\binom{m+r}{r}\binom{n+r}{r} - d^2mn\right).$$

PROOF. The dimension of the vector space $I_{m,n}$ equals

$$\binom{m+r}{r}\binom{n+r}{r} - d^2mn,$$

determined by Lemma 17 and Möbius inversion with respect to the common vector subspace $\Gamma(\mathbb{P}^r, \mathscr{I}_E(m)) \otimes \Gamma(\mathbb{P}^r, \mathscr{I}_E(n))$. Since each of the $r+1$ polynomials representing the addition law coordinates is a coset of the vector space $I_{m,n}$ we obtain the cofactor $r+1$. □

4. Addition law projections

We introduce the notion of an addition law projection first in order to define the relation with the notion of affine addition laws, given by rational polynomial maps, in relation to $E \times E \mapsto \mathbb{P}^1$, and secondly to determine precise statements for the dimensions of addition laws of the form $E_1 \times E_1 \to E_0$ where E_1 and E_0 are different embeddings defined by divisors D_1 and D_0, with particular interest in the case $D_1 > D_0$ (up to linear equivalence).

4.1. Definition of an addition law projection

Let E be projectively normal in $\mathbb{P}^r$, let $\varphi : E \to C \subset \mathbb{P}^s$ be a morphism, and set $\mathscr{L}_\varphi = \varphi^*\mathcal{O}_C(1)$, and assume that $\mathscr{L}_\varphi \cong \mathscr{L}(D_\varphi)$. We now consider the space of *addition law projections* of bidegree (m, n) with respect to the composition $\varphi \circ \mu$ defined to be an $(s+1)$-tuple $(p_0, \ldots, p_s)$ with

$$p_j \in \Gamma(E \times E, \pi_1^*\mathcal{O}_E(m) \otimes \pi_2^*\mathcal{O}_E(n))$$

which determines $\varphi \circ \mu$ on an open subvariety of $E \times E$. As above, we interpret an addition law projection $\mathfrak{s}$ as an element of $\mathrm{Hom}(\mu^* \mathscr{L}_\varphi, \pi_1^* \mathscr{L}^m \otimes \pi_2^* \mathscr{L}^n)$, isomorphic to

$$\Gamma(E \times E, \mu^* \mathscr{L}_\varphi^{-1} \otimes \pi_1^* \mathscr{L}^m \otimes \pi_2^* \mathscr{L}^n).$$

The principal interest is when, up to isomorphism, $D > D_\varphi > 0$, and φ is either an isomorphism or a projection to $\mathbb{P}^1$. In such a case, the morphism φ has a linear representation and an addition law for μ restricts to an addition law projection for $\varphi \circ \mu$. On the other hand, the space of addition laws projections is in general larger and may be nonzero for bidegrees less than $(2, 2)$.

4.2. Dimensions of spaces of addition law projections

We are now in a position to determine the dimensions of the spaces of addition law projections. Let E be a projectively normal curve in $\mathbb{P}^r$ with $\mathscr{L} = \mathcal{O}_E(1) \cong \mathscr{L}(D)$ and φ a morphism to a curve C in $\mathbb{P}^s$ such that

$$\mathscr{L}_\varphi := \varphi^* \mathcal{O}_C(1) \cong \mathscr{L}(D_\varphi)$$

with $D > D_\varphi > 0$, and define

$$\mathscr{M}_{\varphi,m,n} = \mu^* \mathscr{L}_\varphi^{-1} \otimes \pi_1^* \mathscr{L}^m \otimes \pi_2^* \mathscr{L}^n.$$

Corollary 19. $\chi(\mathscr{M}_{\varphi,m,n}) = d(dmn - d_\varphi(m+n))$.

Suppose that $d = 2d_\varphi$. The critical case for the Euler-Poincaré characteristic is then bidegree $(1, 1)$.

Theorem 20. *Let $\iota : E \to \mathbb{P}^r$ be a projectively normal embedding of an elliptic curve, with respect to a symmetric sheaf $\mathscr{L} = \mathcal{O}_E(1) \cong \mathscr{L}(D)$, and let $\varphi : E \mapsto \mathbb{P}^s$ be a nonconstant map, with respect to a symmetric sheaf $\mathscr{L}_\varphi \cong \mathscr{L}(D_\varphi)$. Suppose that $D > D_\varphi > 0$ Then the space of global sections of $\mathscr{M}_{\varphi,1,1}$ is isomorphic to the space of global sections of $\mathscr{L}_\varphi$. Moreover, the exceptional divisor of an addition law projection of bidegree $(1, 1)$ associated to a section in $\Gamma(E \times E, \mathscr{M}_{\varphi,1,1})$ is of the form $\sum_{i=1}^{d_\varphi} \Delta_{P_i}$ where $D \sim \sum_i (P_i)$.*

Corollary 21. *Let $\mathscr{L}$, $\mathscr{L}_\varphi$, and $\mathscr{M}_{\varphi,m,n}$ be as above, with $d = 2d\varphi$. Then for $(m, n) = (1, 1)$,*

$$\dim_k(H^0(E \times E, \mathscr{M})) = \dim_k(H^1(E \times E, \mathscr{M})) = d_\varphi,$$

and for all other $m, n \geq 1$,

$$\dim_k(H^0(E \times E, \mathscr{M}_{m,n})) = d_\varphi^2((2m-1)(2n-1) - 1).$$

5. Affine models and projective normal closure

A nonsingular projective curve is uniquely (up to unique isomorphism) determined by any affine model C [11, Chap. I, Cor. 6.12]. As a consequence, it is standard to specify a curve by an affine model which determines it. On the other hand, in order to define addition laws in terms of a given affine model we requires some definition. We begin with the notation of a projective normal closure.

5.1. Projective normal closure

Let C/k be a nonsingular affine curve in $\mathbb{A}^s$, with coordinate functions $x_1, \ldots, x_s$ and X its associated nonsingular projective curve. We defined the *divisor at infinity* of C to be the divisor $D = \sup(\{\mathrm{div}_\infty(x_i)\})$, on X, where $\mathrm{div}_\infty(x)$ is the polar divisor of x.

Let $\{x_0, x_1, \ldots, x_r\}$ be a generator set for $\Gamma(X, \mathscr{L}(D))$, where we assume $x_0 = 1$, and $x_1, \ldots, x_s$ are the coordinate functions on C. Since C is nonsingular, its coordinate ring is integrally closed, and by the definition of D, we have

$$k[x_1, \ldots, x_s] = k[x_1, \ldots, x_r].$$

A *projectively normal closure* of C is a model for X in $\mathbb{P}^r$, determined by the morphism

$$P \longmapsto (x_0(P) : x_1(P) : \cdots : x_r(P)),$$

which identifies C as the open affine of X given by $X_0 = 1$. Clearly any two projectively normal closures are isomorphic via a linear isomorphism determined by the choice of generator set extending $x_0, \ldots, x_s$.

5.2. Examples of nonsingular affine models

Consider the affine plane model C_0

$$C_0 : y^2 = x(x^2 + ax + 1),$$

of an elliptic curve E with divisor at infinity is $3(O)$. The projective normal closure of C_0 is the standard projective plane Weierstrass model:

$$E_0 : Y^2Z = X(X^2 + aXZ + Z^2),$$

with identity $O = (0 : 1 : 0)$ and 2-torsion point $T = (0 : 0 : 1)$. We construct three affine models with divisors at infinity $4(O)$, $2(O) + 2(T)$, and equivalent to $3(O) + (T)$.

Case $D = 4(O)$**.** A basis for $\Gamma(E, \mathscr{L}(4(O)))$ is $\{1, x, y, x^2\}$, determining a projectively normal curve in $\mathbb{P}^3$:

$$E_1 : X_2^2 = X_1(X_0 + aX_1 + X_3),\ X_0X_3 = X_1^2.$$

A nonsingular affine plane model is given by projection to the (x, s)-plane, where $s = y + x^2$:

$$C_1 : (x^2 - s)^2 = x(x^2 + ax + 1).$$

The resulting plane curve has divisor at infinity $4(O)$.

Case $D = 2(O)+2(T)$**.** A basis for $\Gamma(E, \mathscr{L}(2(O)+2(T)))$ consisting of common eigenvectors for $[-1]^*$ and for τ_T*, where τ_T is the translation-by-T map, is

$$\{1, (x + 1/x)/2, (x - 1/x)/2, y/x\},$$

determining a projectively normal curve in $\mathbb{P}^3$:

$$E_2 : X_3^2 = X_0(aX_0 + 2X_1),\ X_1^2 = X_0^2 + X_2^2.$$

A nonsingular affine plane model is given by projection to the (v, w)-plane, where $(w, v) = (x - 1/x, y/x)$:

$$C_2 : w^2 = (v^2 - a)^2 - 4,$$

in the form of a Jacobi quartic. The resulting plane curve has divisor at infinity $2(O) + 2(T)$ and any projective normal closure is linearly isomorphic to E_2.

The divisors $4(O)$ and $2(O) + 2(T)$ are linearly equivalent so there exists a projective linear isomorphism between them. Explicitly, the map $E_1 \to E_2$ is induced by the transformation:

$$(X_0 : X_1 : X_2 : X_3) \mapsto (X_1 : (X_3 + X_0)/2 : (X_3 - X_0)/2 : X_2).$$

Next we construct a quartic model whose divisor at infinity is equivalent to the symmetric divisor $3(O) + (T)$. Since $4(O)$ is not equivalent to $3(O) + (T)$, it follows that this model is not linearly equivalent to E_1 or E_2.

Case $D \sim 3(O) + (T)$. We construct D as the sum of two coprime symmetric divisors D_0 and D_1, such that each is invariant under translation by T, and such that $D_0 \sim 2(O)$ and take $D_1 = (O) + (T)$.

A basis for $\Gamma(E, \mathscr{L}(3(O) + (T)))$ is $\{1, x, y/x, y\}$, determining a projectively normal curve in $\mathbb{P}^3$:

$$E_3 : X_2X_3 = X_0^2 + aX_0X_1 + X_1^2,\ X_0X_3 = X_1X_2.$$

The function $v = y/x$ has the polar divisor D_1. In order to construct D_0, we let τ_T be the translation-by-T map and note that $\tau_T^*(x) = 1/x$. Thus $u = (x + 1)/(x - 1)$ is an eigenfunction for τ_T^* with eigenvalue -1. The projection to the (u, v)-plane, is then a nonsingular affine plane model:

$$C_4 : u^2v^2 = (a + 2)u^2 + v^2 - (a - 2).$$

The resulting plane curve has divisor at infinity $D = D_0 + D_1$, and $\Gamma(E, \mathscr{L}(D))$ is $\{1, u, v, uv\}$, hence we obtain the projective normal closure

$$E_4 : X_3^2 = (a + 2)X_1^2 + X_2^2 - (a - 2)X_0^2,\ X_0X_3 = X_1X_2.$$

The isomorphism $E_3 \to E_4$ is then the linear transformation:

$$(X_0 : X_1 : X_2 : X_3) \mapsto (X_1 - X_0 : X_1 + X_0 : X_3 - X_2, X_3 + X_2).$$

In each of the three cases, we observe that we obtain an affine plane quartic model such that the coordinate functions, together with 1, do not span the basis of $\Gamma(E, \mathscr{L}(D))$. Nevertheless, we will see that the addition laws are naturally defined in terms of a full generator set of $\Gamma(E, \mathscr{L}(D))$, determined by the affine model.

Remark. By Lemma 2 any degree 4 symmetric model of an elliptic curve must be projectively linearly isomorphic to a curve of the form E_1 or E_3, the latter case depending on a choice of rational 2-torsion point. The form of model E_4 can be recognized as a twisted Edwards model (see Section 8). This canonical form requires the existence of u and v, which are common eigenvectors for $[-1]^*$ and τ_T^*. The existence of the degree 2 function u, requires the zero and polar divisors of u to be stable under τ_T^*, and since $[-1]^*(u) = u$, this implies that these divisors are supported on pairs of 4-torsion points.

5.3. Arithmetically complete affine models

To conclude this section, we note that the notion of completeness of addition laws is sometimes coupled with an independent condition on a particular affine model. By definition an abelian variety is a complete group variety – completeness is a geometric notion which is stable under base extension. We define an affine curve C to be *arithmetically complete* if $C(k) = X(k)$ for any projective nonsingular X containing C. For an elliptic curve, this ensures that the rational points of the affine model form a group. Over a sufficiently large base field, one can find suitable line which misses all rational points and pass to an arithmetically complete affine model by a projective change of variables. Nice arithmetically complete models (e.g. twisted Edwards curves [2] or twisted Hessian curves [4]) tend to have an eigenvector for a torsion subgroup as the prescribed line at infinity.

6. Affine addition laws

Suppose that C is a nonsingular affine curve in $\mathbb{A}^s$ of an elliptic curve, and let E be a projective normal closure in $\mathbb{P}^r$. If $x_1, \ldots, x_s$ are the coordinate functions on C, then we denote by x_i also the projections $E \to \mathbb{P}^1$ extending $x_i : C \to \mathbb{A}^1$. Let $k[C] = k[x_1, \ldots, x_s]$ be the coordinate ring of C, recalling that since C is nonsingular, $k[x_1, \ldots, x_s] = k[x_1, \ldots, x_r] = \Gamma(C, \mathcal{O}_E)$, where $x_i = X_i/X_0$. We write

$$k[C] \otimes_k k[C] = k[x_1, \ldots, x_r, y_1, \ldots, y_r]$$

where we identity x_i with $x_i \otimes 1$ and write y_i for $1 \otimes x_i$, and similarly identify X_i with

$$X_i \otimes 1 \in \Gamma(E \times E, \pi_1^* \mathcal{O}_E(1) \otimes \pi_2^* \mathcal{O}_E(0)),$$

and Y_i with

$$1 \otimes X_i \in \Gamma(E \times E, \pi_1^* \mathcal{O}_E(0) \otimes \pi_2^* \mathcal{O}_E(1)).$$

An affine addition law for C is an s-tuple of pairs (f_i, g_i) in $(k[C] \otimes_k k[C])^2$ such that

$$\mu^*(x_i) = \frac{f_i}{g_i} \in k(E \times E).$$

We refer to (f_i, g_i) as an *affine addition law projection* for x_i. We define the *bidegree* of an addition law $\mathfrak{s}_i = (f_i, g_i)$ to be the smallest m_i and n_i such

that $\mathfrak{s}_i$ is the restriction of an addition law projection of bidegree (m_i, n_i), and the bidegree of $\mathfrak{s} = (\mathfrak{s}_1, \ldots, \mathfrak{s}_s)$ to be $(m, n) = (\max_i(\{m_i\}), \max_i(\{n_i\}))$. We note that the bidegree of an addition law is determined by the minimal degree polynomial expression in $\{x_1, \ldots, x_r, y_1, \ldots, y_r\}$ for f_i and g_i, rather than as a polynomial in the coordinate functions on $\{x_1, \ldots, x_s, y_1, \ldots, y_s\}$.

Hereafter we express an affine addition law projection (f_i, g_i) as a fraction f_i/g_i and similarly write

$$\mathfrak{s} = \left(\frac{f_1}{g_1}, \frac{f_2}{g_2}, \ldots, \frac{f_s}{g_s}\right),$$

for an affine addition law. We note that in this context f_i/g_i should not be confused with the equivalence class $z_i = \mu^*(x_i)$ in $k(E \times E)$, and that in this notation the vector space structure is written:

$$a\frac{f_i}{g_i} + b\frac{f_i'}{g_i'} = \frac{af_i + bf_i'}{ag_i + bg_i'}.$$

Since $f_i = g_i z_i$ and $f_i' = g_i' z_i$, the equivalence class in $k(E \times E)$ remains the same:

$$a\frac{f_i}{g_i} + b\frac{f_i'}{g_i'} = a\frac{g_i z_i}{g_i} + b\frac{g_i' z_i}{g_i'} = \frac{(ag_i + bg_i')z_i}{ag_i + bg_i'}.$$

Theorem 22. *The affine addition laws for C in $\mathbb{A}^s$ of bidegree (m, n) form a vector space isomorphic to the direct sum of the spaces of addition law projections for the coordinate functions $x_1, \ldots x_s$ of bidegree (m, n).*

Proof. Every polynomial form p_i in $\Gamma(E \times E, \pi_1^*\mathcal{O}_E(m) \otimes \pi_2^*\mathcal{O}_E(n))$ determines a unique function $f_i = p_i/X_0^m Y_0^n$ in

$$k[C] \otimes k[C] = \Gamma(C, \mathcal{O}_E) \otimes \Gamma(C, \mathcal{O}_E)$$

and injectivity of $p_i \mapsto f_i$ follows from injectivity of $\Gamma(E, \mathcal{O}_E(m)) \to k[C]$. □

7. Torsion module structure

Let E/k be an elliptic curve with finite torsion subgroup $G \subset E(k)$. A divisor D is said to be *G-invariant* if $\tau_P^* D = D$ for all P in G, where $\tau_P : E \to E$ is the translation-by-P morphism. We hereafter assume that E/k is equipped with a projectively normal embedding in $\mathbb{P}^r$ by $\mathscr{L} = \mathscr{L}(D)$, where D is an effective G-invariant divisor.

Lemma 23. *Let $\iota : E \to \mathbb{P}^r$ be a projectively normal embedding of E, with respect to $\mathscr{L}$. Let G be a finite torsion subgroup, and suppose that $\mathscr{L} = \mathscr{L}(D)$ where D is an effective G-invariant divisor. Then G acts on E by projective linear transformations of $\mathbb{P}^r$.*

PROOF. Since D is G-invariant, the space $\Gamma(E, \mathscr{L})$ has a k-linear representation by G. Since we have a surjective homomorphism $\Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(1)) \to \Gamma(E, \mathscr{L})$, every linear automorphism of $\Gamma(E, \mathscr{L})$ lifts to an automorphism of $\Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(1))$, hence to a projective linear transformation of $\mathbb{P}^r$. □

From the action of τ_P^* on $\Gamma(E, \mathscr{L})$, and lifting to $\Gamma(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(1))$, we identify τ_P with a linear polynomial map in $k[X_0, \ldots, X_r]^{r+1}$. Let G_2 be the kernel of the homomorphism $G \times G \times G \to G$ defined by $(R, S, T) \mapsto R+S+T$, and let G_1 be the subgroup of G_2 with $T = 0$. We define the action of G_2 (hence of G_1) on the space of addition laws of bidegree (m, n) by $(R, S, T) \cdot \mathfrak{s} = \tau_T \circ \mathfrak{s} \circ (\tau_R \times \tau_S)$, so that

$$(R, S, T) \cdot \mathfrak{s}(P, Q) = \mathfrak{s}(P + R, Q + S) + T.$$

Clearly G_2 is isomorphic to $G \times G$, and is generated by

$$\{(S, T - S, -T) : S, T \in G\}.$$

Lemma 24. *The group G_2 acts linearly on the addition laws of bidegree (m, n).*

PROOF. The image $(R, S, T) \cdot \mathfrak{s}$ is the composition of polynomials of bidegree (m, n) with linear polynomial maps, which, by the hypothesis that $R+S+T = O$, determines another addition law. □

Lemma 25. *The group G_2 acts linearly on the set of divisors of addition laws for E. In particular the action on the components of addition laws of bidegree $(2, 2)$ is given by*

$$(R, S, T)^* \Delta_P = \Delta_{P-R+S}.$$

PROOF. The action on divisors is $\mathrm{div}((R, S, T) \cdot \mathfrak{s}) = (\tau_R \times \tau_S)^* \mathrm{div}(\mathfrak{s})$, and the action on Δ_P follows from

$$(\tau_R \times \tau_S)^* \Delta_P = \Delta + (P - R, -S) = \Delta + (P - R + S, O) = \Delta_{P-R+S}.$$

Since T determines a linear automorphism of the polynomials of $\mathfrak{s}$, it has no bearing on the divisor which they cut out. □

Theorem 26. *An addition law $\mathfrak{s}$ is an eigenvector for an element (R, S, T) of G_2 if and only if the exceptional divisor of $\mathfrak{s}$ is fixed by (R, S, T).*

The abstract vector spaces of addition laws, as well as the G_2-module structure are independent of the choice of bases for $\Gamma(E, \mathscr{L})$ as well as $\Gamma(E \times E, \mathscr{M})$. However, the simplicity of the addition laws (as measured, for example, by their sparseness as polynomials) on Edwards and Hessian models, is entirely dependent on the choice of the sections in $\Gamma(E, \mathscr{L})$ and the corresponding coordinate functions of the projective embedding, and of the addition laws. This study grew out of the observation that the simplest addition laws arise from the bases which arise either as eigenspaces of G_1 or which have a permutation representation with respect to G_1.

8. Addition law constructions

In this section we report on examples which demonstrate the structure of addition laws outlined above. In order to determine such models, we assume that a family of elliptic curves with prescribed torsion subgroup G is given as input. Such families can be found in the literature or constructed by means of parametrizations by modular curves. Moreover, the computations require algorithms for solving the following problems.

1. An algorithm for determing Riemann-Roch spaces $\Gamma(E, \mathscr{L})$.
2. An algorithm for computing the space of addition laws of bidegree (m, n).
3. An algorithm for computing the G-module structures of $\Gamma(E, \mathscr{L})$ and of the spaces of addition laws.

The first algorithm is provided by the computational algebra system Magma [19] as implemented by Hess [12], and code for the remaining problems was implemented by the author using linear algebra in Magma or Sage [21], to be made available in ECHIDNA [9] and Sage. The complete spaces of addition laws of given bidegree can be determined by interpolating the addition morphism with monomials of the correct bidegree, each evaluated on random points (for which we use formal points in the neighborhood of O). This approach through morphism interpolation was communicated to me by Bernstein and Lange, and a similar interpolation algorithm was recently described by Castryck and Vercauteren [7]. Hisil et al. [14] use an analogous Gröbner basis approach of Monagan and Pierce [20] to systematically search for rational expressions for affine addition laws. An effective addition morphism can be determined by means of an isomorphism with an elliptic curve in Weierstrass model, determined by explicit Riemann-Roch, together with an existing implementation of the group law on the Weierstrass model.

8.1. Level 4: Twisted Edwards curves

In 2007, Edwards [10] introduced a remarkable new affine model for elliptic curves

$$x^2 + y^2 = c^2(1 + dx^2y^2).$$

The parameter d, equal to 1 in Edwards' model, was introduced by Bernstein and Lange [1], to obtain an arithmetically complete addition law for nonsquare values of d (and moreover the parameter c may be subsumed into d as a square factor). Subsequently, Bernstein et al. [2] introduced twisted Edwards curves

$$ax^2 + y^2 = 1 + dx^2y^2.$$

The complete addition law, in affine coordinates takes the form

$$(x_1, y_1) + (x_2, y_2) \longmapsto \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

Neither affine nor singular models fit in the framework of Lange and Ruppert. Although the projective closure in $\mathbb{P}^2$ is singular, as a curve in $\mathbb{P}^1 \times \mathbb{P}^1$ the projective closure

$$E_2 : aX^2W^2 + Y^2Z^2 = Z^2W^2 + dX^2Y^2,$$

is nonsingular and the addition law well-defined of multi-degree $((1,1),(1,1))$. Here we describe the interplay between the embedding in $\mathbb{P}^3$ and $\mathbb{P}^1 \times \mathbb{P}^1$, exploited in the simple addition laws of Hisil [13] for models in $\mathbb{P}^3$, and interpret the addition laws and their completeness properties in terms of eigenspaces under the 4-torsion subgroup. The addition laws so determined on the curve E_2 embedded in $\mathbb{P}^1 \times \mathbb{P}^1$ are those studied by Bernstein and Lange [3], who prove their completeness properties. The above theory gives a means of explaining the canonical nature of these simple addition laws.

In order to apply the theoretical description of addition laws, we embed E_2 in projective space via the Segre embedding $\varphi : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$, given by

$$((X : Z), (Y : W)) \longmapsto (XY : XW : ZY : ZW) = (X_0 : X_1 : X_2 : X_3)$$

This gives the model

$$E_1 : dX_0^2 + X_3^2 = aX_1^2 + X_2^2, \quad X_0X_3 = X_1X_2,$$

with identity $O = (0 : 0 : 1 : 1)$. The projection morphisms are respectively

$$\begin{array}{l}(X_0 : X_1 : X_2 : X_3) \longmapsto (X_0 : X_2) = (X_1 : X_3), \text{ and} \\ (X_0 : X_1 : X_2 : X_3) \longmapsto (X_0 : X_1) = (X_2 : X_3).\end{array}$$

The embedding in $\mathbb{P}^3$ appears in Hisil et al. [13], for the coordinate functions

$$(T, X, Y, Z) = (X_0, X_1, X_2, X_3),$$

under the name extended Edwards coordinates, although we do not use these coordinate names here, and instead write $(X_0, X_1, X_2, X_3, Y_0, Y_1, Y_2, Y_3)$ for the coordinate functions on $\mathbb{P}^3 \times \mathbb{P}^3$.

Suppose that c and e are square roots of a and d, respectively, in the algebraic closure of the base field of E_2. Then $T_1 = (0 : 1 : 0 : c)$ and $T_2 = (1 : 0 : e : 0)$ are points of order 4, and the translation-by-T_1 morphism is

$$(X_0 : X_1 : X_2 : X_3) \longmapsto (-X_0 : c^{-1}X_2 : -cX_1 : X_3).$$

and that for translation-by-T_2 is:

$$(X_0 : X_1 : X_2 : X_3) \longmapsto (-e^{-1}X_3 : X_1 : -X_2 : eX_0).$$

We note that $2T_1 = 2T_2 = (0 : 0 : -1 : 1)$,

$$T_1 + T_2 = (-c : e : 0 : 0) \text{ and } T_1 - T_2 = (c : e : 0 : 0)$$

and $E_1[2] = \{O, 2T_i, T_1 \pm T_2\}$. Let G be the torsion subgroup $\langle T_1, T_2 \rangle$, isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. We now state the characterization of the spaces of addition laws for the group morphism $E_1 \times E_1 \to E_2$, in terms of bases of distinguished eigenvectors and their exceptional divisors. These addition laws, as well as the characterization of exceptional divisors, can be deduced from the addition laws for $E_2 \times E_2 \to E_2$ of Bernstein and Lange [3], by factoring through the Segre embedding (see note below Corollary 31).

Theorem 27. *The space of addition laws for $E_1 \times E_1 \to E_2$ of bidegree $(1,1)$ is spanned by $\{(\mathfrak{s}_i, \mathfrak{t}_j) : 0 \le i, j \le 1\}$, where*

$$\begin{aligned} \mathfrak{s}_0 &= (X_0Y_3 + X_3Y_0,\ aX_1Y_1 + X_2Y_2), \\ \mathfrak{s}_1 &= (X_1Y_2 + X_2Y_1,\ dX_0Y_0 + X_3Y_3), \end{aligned}$$

with respective exceptional divisors $\Delta_{T_1} + \Delta_{-T_1}$ and $\Delta_{T_2} + \Delta_{-T_2}$, and

$$\begin{aligned} \mathfrak{t}_0 &= (X_0Y_3 - X_3Y_0,\ X_1Y_2 - Y_1X_2), \\ \mathfrak{t}_1 &= (aX_1Y_1 - X_2Y_2,\ dX_0Y_0 - X_3Y_3), \end{aligned}$$

with respective exceptional divisors $\Delta_O + \Delta_{2T_i}$ and $\Delta_{T_1+T_2} + \Delta_{T_1-T_2}$.

Proof. The correctness of the addition laws is verified by explicit substitution. The dimensions of each of the addition law projections is 2, in accordance with Corollary 21 and the degrees of the projections of E_2 to $\mathbb{P}^1$. Thus the two sets $\{\mathfrak{s}_0, \mathfrak{s}_1\}$ and $\{\mathfrak{t}_0, \mathfrak{t}_1\}$ are bases for the spaces of addition law projections. Correctness of the exceptional divisors can be verified by intersection with $E \times \{O\}$. □

Let G_1 and G_2 be the subgroups defined in the previous section, with respect to the group $G = \langle T_1, T_2 \rangle$. The group G_1 has a well-defined action on the two spaces spanned by $\{\mathfrak{s}_0, \mathfrak{s}_1\}$ and $\{\mathfrak{t}_0, \mathfrak{t}_1\}$, while the action of G_2 only becomes well-defined on the span of tuples $\{(s_i, t_j)\}$.

Corollary 28. *The sets $\{\mathfrak{s}_0, \mathfrak{s}_1\}$ and $\{\mathfrak{t}_0, \mathfrak{t}_1\}$ are stabilized by G_1 and pointwise fixed by the subgroup $\langle (2T_i, 2T_i, O) \rangle$. Moreover each of $k\mathfrak{s}_j$ and $k\mathfrak{t}_j$ are eigenspaces for the action of G_1. The action of G_2 stabilizes the sets of eigenspace pairs $\{(k\mathfrak{s}_0, k\mathfrak{t}_0), (k\mathfrak{s}_1, k\mathfrak{t}_1)\}$ and $\{(k\mathfrak{s}_0, k\mathfrak{t}_1), (k\mathfrak{s}_1, k\mathfrak{t}_0)\}$, and acts transitively on their product.*

Proof. By Theorem 26, the eigenvectors are characterized by the action on the exceptional divisors. By Lemma 16 and the form of the exceptional divisors in Theorem 27, we see that the exceptional divisors are stabilized by $(T_i, -T_i, O)$ and hence $\mathfrak{s}_0$, $\mathfrak{s}_1$, $\mathfrak{t}_0$ and $\mathfrak{t}_1$ are eigenvectors. By explicit substitution we find eigenvalues $(-1, 1, -1, 1)$ for T_1 and eigenvalues $(1, -1, -1, 1)$ for T_2. Hence each of the spaces spanned by $\{\mathfrak{s}_0, \mathfrak{s}_1\}$ and $\{\mathfrak{t}_0, \mathfrak{t}_1\}$ decomposes into one-dimensional eigenspaces. The action on eigenspace pairs follows similarly from the action on exceptional divisors. □

Theorem 29. *The addition law projection $\mathfrak{s}_0$, $\mathfrak{s}_1$, or $\mathfrak{t}_1$ is arithmetically complete if and only if a, d, or ad is a nonsquare, respectively. In particular, over a finite field, either zero or two of $\mathfrak{s}_0$, $\mathfrak{s}_1$ and $\mathfrak{t}_1$ are arithmetically complete.*

PROOF. The sets $\{T_1, -T_1\}$, $\{T_2, -T_2\}$ and $\{T_1+T_2, T_1-T_2\}$ are Galois orbits of non k-rational points when a, d, or ad is a nonsquare, respectively, in which case the respective divisor $\Delta_{T_1} + \Delta_{-T_1}$, $\Delta_{T_2} + \Delta_{-T_2}$ or $\Delta_{T_1+T_2} + \Delta_{T_1-T_2}$, is irredducible over k and hence has no rational point. Over a finite field, either zero or two of a, d, and ad are nonsquares. □

Let $\varphi : E_2 \times E_2 \to E_1$ be the restriction of the Segre embedding $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$, and identify φ with the polynomial map $((X,Z),(Y,W)) \mapsto (XY, XW, ZY, ZW)$. As a consequence of the above theorem, the four dimensional space of addition laws for E_1 is obtained in factored form as the pairwise combination of these pairs of addition laws, under the Segre embedding in $\mathbb{P}^3$.

Corollary 30. *The space of addition laws of bidegree $(2,2)$ for*

$$\mu : E_1 \times E_1 \longrightarrow E_1$$

is spanned by $\{\varphi(\mathfrak{s}_i, \mathfrak{t}_j) : 0 \le i, j \le 1\}$.

Similarly, we obtain a factored form $E_2 \times E_2 \to E_1 \times E_1 \to E_2$ for the addition laws on E_2.

Corollary 31. *The space of addition laws of multidegree $((1,1),(1,1))$ for*

$$\mu : E_2 \times E_2 \longrightarrow E_2$$

is spanned by $\{((\mathfrak{s}_i \circ \varphi \times \varphi, \mathfrak{t}_j \circ \varphi \times \varphi) : 0 \le i, j \le 1\}$.

In expanded form Corollary 30 gives the addition laws:

$$\begin{aligned}
\varphi(\mathfrak{s}_0, \mathfrak{t}_0) &= \big((X_0Y_3 + X_3Y_0)(X_0Y_3 - X_3Y_0),\ (X_0Y_3 + X_3Y_0)(X_1Y_2 - Y_1X_2),\\
&\qquad (aX_1Y_1 + X_2Y_2)(X_0Y_3 - X_3Y_0),\ (aX_1Y_1 + X_2Y_2)(X_1Y_2 - Y_1X_2)\big),\\
\varphi(\mathfrak{s}_0, \mathfrak{t}_1) &= \big((X_0Y_3 + X_3Y_0)(aX_1Y_1 - X_2Y_2),\ (X_0Y_3 + X_3Y_0)(aX_1Y_1 - X_2Y_2),\\
&\qquad (aX_1Y_1 + X_2Y_2)(dX_0Y_0 - X_3Y_3),\ (aX_1Y_1 + X_2Y_2)(dX_0Y_0 - X_3Y_3)\big),\\
\varphi(\mathfrak{s}_1, \mathfrak{t}_0) &= \big((X_1Y_2 + X_2Y_1)(X_0Y_3 - X_3Y_0),\ (X_1Y_2 + X_2Y_1)(X_1Y_2 - Y_1X_2),\\
&\qquad (dX_0Y_0 + X_3Y_3)(X_0Y_3 - X_3Y_0),\ (dX_0Y_0 + X_3Y_3)(X_1Y_2 - Y_1X_2)\big),\\
\varphi(\mathfrak{s}_1, \mathfrak{t}_1) &= \big((X_1Y_2 + X_2Y_1)(aX_1Y_1 - X_2Y_2),\ (X_1Y_2 + X_2Y_1)(dX_0Y_0 - X_3Y_3),\\
&\qquad (dX_0Y_0 + X_3Y_3)(aX_1Y_1 - X_2Y_2),\ (dX_0Y_0 + X_3Y_3)(dX_0Y_0 - X_3Y_3)\big).
\end{aligned}$$

The forms $\varphi(\mathfrak{s}_1, \mathfrak{t}_1)$ and $\varphi(\mathfrak{s}_0, \mathfrak{t}_0)$, with given factorization, appear as equations (5) and (6), respectively, in Hisil et al. [13]. Similarly, in expanded form Corollary 31 gives the addition law projections of Bernstein and Lange [3]:

$$\begin{aligned}
\mathfrak{s}_0 \circ \varphi \times \varphi &= (X_1Y_1Z_2W_2 + Z_1W_1X_2Y_2,\ aX_1W_1X_2W_2 + Z_1W_1Z_2W_2),\\
\mathfrak{s}_1 \circ \varphi \times \varphi &= (X_1W_1Z_2Y_2 + Z_1Y_1X_2W_1,\ dX_1Y_1X_2Y_2 + Z_1W_1Z_2W_2),\\
\mathfrak{t}_0 \circ \varphi \times \varphi &= (X_1Y_1Z_2W_2 - Z_1W_1X_2Y_2,\ X_1W_1Z_2Y_2 - X_1W_1Z_2Y_2),\\
\mathfrak{t}_1 \circ \varphi \times \varphi &= (aX_1W_1X_2W_2 - Z_1Y_1Z_2Y_2,\ dX_1Y_1X_2Y_2 - Z_1W_1Z_2W_2).
\end{aligned}$$

The set of exceptional divisors of these addition laws, described in Bernstein and Lange [3, Sec. 8], is equivalent to that of Theorem 27, since the Segre embedding is globally defined by a single polynomial map with trivial exceptional divisor.

8.2. Level 3: Symmetric triangular and twisted Hessian curves

In Bernstein, Kohel, and Lange [4], two families of elliptic curve models are studied, the symmetric triangular elliptic curves $S_{(r,s)}$:

$$X^3 = rYZW,\ X = s(Y + Z + W),$$

and twisted Hessian curves $H_{(a,d)}$:

$$aX^3 + Y^3 + Z^3 = dXYZ.$$

A similar analysis applies to these curves with level 3 torsion structure. In particular, their spaces of addition laws, exceptional divisors, and completeness properties are studied.

8.3. Level 5: Pentagonal elliptic curves

We describe a model for elliptic curves over the function field $k(t)$ of $X_1(5)$. Let $E/k(t)$ be the elliptic curve in $\mathbb{P}^4$ defined by

$$\begin{gathered} tU_0^2 + U_2U_3 - U_1U_4 = tU_0U_1 + U_2U_4 - U_3^2 = U_1^2 + U_0U_2 - U_3U_4 = 0 \\ U_1U_2 + U_0U_3 - U_4^2 = U_2^2 - U_1U_3 + tU_0U_4 = 0, \end{gathered}$$

with base point $O = (0 : 1 : 1 : 1 : 1)$. This model is derived from an input Weierstrass model E over $k(t)$ by computing the Riemann-Roch space $\Gamma(E, \mathscr{L}(G))$ where $G = \langle T \rangle$ is a cyclic subgroup of order 5, considered as a divisor on E. The coordinate functions U_i are determined by a choice of basis of eigenfunctions for the translation-by-T map. For a 5-th root of unity ζ, the image of T is $(0 : \zeta : \zeta^2 : -\zeta^3 : -\zeta^4)$ and translation-by-T induces:

$$(U_0 : U_1 : U_2 : U_3 : U_4) \longmapsto (U_0 : \zeta U_1 : \zeta^2 U_2 : \zeta^3 U_3 : \zeta^4 U_4).$$

We note that the projection to $(U_0 : U_1 : U_4)$ yields a plane model

$$U_1^5 + U_4^5 - (t-3)U_1^2U_4^2U_0 + (2t-1)U_1U_4U_0^3 - tU_0^5,$$

but that being singular the dimension formulas fail to apply. Indeed there are no bidegree $(2,2)$ addition laws for this planar model.

Theorem 32. *The space of addition laws of bidegree* $(2,2)$ *on* E *is of dimension* 5 *and decomposes over* $k(t)$ *into eigenspaces for the action of* G_1*. The eigenspace for* 1 *is given by the polynomial maps:*

$$\begin{aligned} (\ & U_0^2V_1V_4 - U_1U_4V_0^2 = (U_1U_4V_2V_3 - U_2U_3V_1V_4)/t = -U_2U_3V_0^2 + U_0^2V_2V_3 : \\ & U_0U_1V_2V_4 - U_2U_4V_0V_1 = (-U_2U_4V_3^2 + U_3^2V_2V_4)/t = U_0U_1V_3^2 - U_3^2V_0V_1 : \\ & U_0U_2V_3V_4 - U_3U_4V_0V_2 = U_0U_2V_1^2 - U_1^2V_2V_0 = -U_1^2V_3V_4 + U_3U_4V_1^2 : \\ & U_0U_3V_1V_2 - U_1U_2V_0V_3 = U_0U_3V_4^2 - U_4^2V_0V_3 = -U_1U_2V_4^2 + U_4^2V_1V_2 : \\ & U_0U_4V_1V_3 - U_1U_3V_0V_4 = U_0U_4V_2^2 - U_2^2V_0V_4 = (U_1U_3V_2^2 - U_2^2V_1V_3)/t). \end{aligned}$$

Remark. The function t can be identified with a modular function generating the function field of $X_1(5)$. The modular curve $X(5)$ is also of genus 0, and there exists a modular function e satisfying $t = e^5$ which generates the function field of $X(5)$. Over this extension the 5-torsion point $S = (1 : e : -e^2 : e^3 : 0)$, and the translation-by-S morphism is:

$$(U_0 : U_1 : U_2 : U_3 : U_4) \longmapsto (-U_4 : e^4U_0 : e^3U_1 : -e^2U_2 : eU_3).$$

The remaining eigenspaces of addition laws are permuted by the action induced by the subgroup $G = \langle S \rangle$. In particular, since the action is a scaled monomial permutation, the remaining eigenspaces are also described by binomial biquadratic polynomials.

Acknowledgement. The author thanks Dan Bernstein and Tanja Lange for helpful discussions and motivation to undertake this study. Moreover this work benefited from discussion with Christophe Ritzenthaler and pointers from Marc Hindry. Finally, the author thanks the anonymous referees for careful reading and comments leading to an improvement of the article.

References

[1] D. J. Bernstein, T. Lange. Faster addition and doubling on elliptic curves. *Advances in Cryptology: ASIACRYPT 2007*, Lecture Notes in Computer Science, **4833**, Springer, 29–50, 2007.

[2] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, C. Peters, Twisted Edwards curves. *Progress in cryptology – AFRICACRYPT 2008*, Lecture Notes in Computer Science, **5023**, 389–405, 2008.

[3] D. Bernstein and T. Lange. A complete set of addition laws for incomplete Edwards curves, preprint, `http://eprint.iacr.org/2009/580`, 2009.

[4] D. Bernstein, D. Kohel, and T. Lange. Twisted Hessian curves, preprint, 2010.

[5] C. Birkenhake and H. Lange. *Complex abelian varieties*. Grundlehren der Mathematischen Wissenschaften, **302**, Springer-Verlag, 2004.

[6] W. Bosma and H. W. Lenstra, Jr. Complete systems of two addition laws for elliptic curves. *J. Number Theory*, **53** (2), 229–240, 1995.

[7] W. Castryck and F. Vercauteren. Toric forms of elliptic curves and their arithmetic. preprint 2010.

[8] D. V. Chudnovsky and G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Adv. in Appl. Math.*, **7**, (4), 385–434, 1986.

[9] ECHIDNA Algorithms Archive, version 1.0, 2009. http://echidna.maths.\-usyd.\-edu.au/\-kohel/alg/index.html

[10] H. Edwards. A normal form for elliptic curves. Bulletin of the American Mathematical Society, **44**, 393–422, 2007.

[11] R. Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, **52**, Springer-Verlag, 1977.

[12] F. Hess. Computing Riemann—Roch spaces in algebraic function fields and related topics. *J. Symbolic Computation*, **33**, Issue 4, 425–445, 2002.

[13] H. Hisil, K. K.-H. Wong, G. Carter, E. Dawson, Twisted Edwards curves revisited, *Advances in cryptology – ASIACRYPT 2008*, Lecture Notes in Computer Science, **5350**, Springer, Berlin, 326–343, 2008.

[14] H. Hisil, K. K.-H. Wong, G. Carter, E. Dawson, Faster group operations on elliptic curves, 2007. http://eprint.iacr.org/2007/441

[15] M. Joye and J.-J. Quisquater, Hessian elliptic curves and side-channel attacks. *Cryptographic hardware and embedded systems—CHES 2001 (Paris)*, Lecture Notes in Computer Science, **2162**, Springer, Berlin, 402–410, 2001.

[16] S. Lang. Abelian varieties. Springer-Verlag, 1983.

[17] H. Lange and W. Ruppert. Complete systems of addition laws on abelian varieties. *Invent. Math.*, **79** (3), 603–610, 1985.

[18] H. Lange and W. Ruppert. Addition laws on elliptic curves in arbitrary characteristics, *J. Algebra*, **107**, 106–116, 1987.

[19] Magma Computational Algebra System, version 2.16, 2010. http://magma.maths.usyd.edu.au/-magma/htmlhelp/MAGMA.htm

[20] M. Monagan and R. Pierce. Rational simplification modulo a polynomial ideal. *ISSAC 2006*, 239–245, ACM, New York, 2006.

[21] Sage, version 4.3.5, 2010. http://www.sagemath.org

[22] N. Smart. The Hessian form of an elliptic curve. *Cryptographic hardware and embedded systems—CHES 2001 (Paris)*, 118–125, Lecture Notes in Computer Science, **2162**, Springer, Berlin, 2001.