*Proceedings of the Edinburgh Mathematical Society* (2023) **66**, 548–556
doi:10.1017/S0013091523000275

# ON THE ALGEBRA OF ELLIPTIC CURVES

TOMASZ BRZEZIŃSKI[1,2]

[1] *Department of Mathematics, Swansea University, Swansea University Bay Campus, Swansea, UK*
[2] *Faculty of Mathematics, University of Białystok, Białystok, Poland*
(T.Brzezinski@swansea.ac.uk)

(Received 23 September 2022)

*Abstract* It is argued that a nonsingular elliptic curve admits a natural or fundamental abelian heap structure uniquely determined by the curve itself. It is shown that the set of complex analytic or rational functions from a nonsingular elliptic curve to itself is a truss arising from endomorphisms of this heap.

*Keywords:* elliptic curve; heap; truss

*2020 Mathematics subject classification:* Primary 14H52; 20N10; 16Y99; 08A99

## 1. Introduction

It is well known that a nonsingular complex elliptic curve $\mathcal{E} : y^2 = 4x^3 - g_2x - g_3$ has a natural additive group structure. On the one hand, this structure can be understood as arising from the identification of $\mathcal{E}$ as the quotient $\mathbb{C}/\Lambda(\omega_1, \omega_2)$, where $\Lambda(\omega_1, \omega_2) = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $\Im(\omega_1/\omega_2) > 0$ is the lattice of periods. Since $\Lambda(\omega_1, \omega_2)$ is an additive subgroup of $\mathbb{C}$, the quotient inherits the addition from that of complex numbers. On the other hand, the addition can be defined geometrically as follows (see, e.g. [11, Section III.2] or [7, pp. 12–14], where this addition is very suggestively called a *chord-tangent law*). By the Bézout theorem, a line intersects $\mathcal{E}$ in three points (counted with multiplicities). Thus, a line through points $A$ and $B$ on $\mathcal{E}$ intersects the curve in the third point, which is declared to be $-(A + B)$. Reflecting this point through the $x$-axis, we obtain another point of $\mathcal{E}$ that gives $A + B$. If the line happens to be tangent to, say, $A$, then $A+B = -A$, while for a point $A$ of multiplicity three, $A + A = -A$. Both constructions make a choice of the neutral point for this operation. While it might be clear why the zero complex number should be the zero of the induced operation (after all, zero plays a special role in the usual arithmetic of complex numbers), why the point in infinity on the curve should have this privileged position might not be so transparent; when the curve is embedded in

https://doi.org/10.1017/S0013091523000275 Published online by Cambridge University Press

the projective plane $\mathbb{CP}^2$, the point $[0:1:0]$ is no different for any others. Of course, the geometric construction can be repeated by fixing any point as the zero of the operation (the drawing of lines and description of intersections become a bit more complicated then, see, e.g. [7, p. 14] or [9, Section 5.7]), but the fact that a choice of this point has to be made in the first place raises a question of dependence of the structure on this choice rather than the curve alone. In this note, we argue that it is more natural to consider a ternary algebraic structure on an elliptic curve and first liberate oneself from making any choices of special points and, second, interpret holomorphic (or rational in the case of a general field) endomorphisms[1] of the curve as special endomorphisms of this structure that combine together into an object with two operations similar to albeit substantially different from a ring. In this way, one can deal with **all** endomorphisms of an elliptic curve, not only those that fix an arbitrarily chosen point (isogenies).

## 2. The result

Given three points $A, B, C$ on an elliptic curve $\mathcal{E}$, we determine the fourth point $[A, B, C]$ as follows. Suppose that the line through $A$ and $C$ intersects the curve at a point $D \neq B$. Then $[A, B, C]$ is the point of intersection of $\mathcal{E}$ with the line through $D$ and $B$ (see Figure 1). If it happens that $D = B$, then $[A, B, C]$ is the intersection point of the line tangent to $\mathcal{E}$ at $B$ with the curve $\mathcal{E}$. If $A = C$, then $D$ is the intersection point of the line tangent to $\mathcal{E}$ at $A$ with $\mathcal{E}$. If $B = C$, then this construction gives $[A, C, C] = A$. Similarly, if $B = A$, then $[A, A, C] = C$.

The just described operation $(A, B, C) \longmapsto [A, B, C]$ defines an *abelian heap* structure on $\mathcal{E}$ (see [2, 10]). That is, for all points $A, B, C, D, E$ on $\mathcal{E}$,

$$[[A, B, C], D, E] = [A, B, [C, D, E]],$$
$$[A, B, B] = [B, B, A] = A \quad \text{and} \quad [A, B, C] = [C, B, A].$$

We denote this heap by $H(\mathcal{E})$.[2]

This geometric construction can also be expressed either analytically or purely algebraically. Let $\mathcal{E} = \mathbb{C}/\Lambda(\omega_1, \omega_2)$ and let $\wp$ be the Weierstrass function associated with the lattice $\Lambda(\omega_1, \omega_2)$. Take any $A, B, C \in \mathcal{E}$ and view them in $\mathbb{C}^2$ as $A = (\wp(a), \wp'(a))$, $B = (\wp(b), \wp'(b))$, $C = (\wp(c), \wp'(c))$, where $a, b, c \in \mathbb{C}$. Choose $d \in \mathbb{C}$ such that $a + c + d \in \Lambda(\omega_1, \omega_2)$. The corresponding point $D = (\wp(d), \wp'(d)) \in \mathcal{E}$ is collinear with $A$ and $C$. Let $\langle a, b, c\rangle$ denote any complex number such that $b + d + \langle a, b, c\rangle \in \Lambda(\omega_1, \omega_2)$. Then

$$[A, B, C] = (\wp(\langle a, b, c\rangle), \wp'(\langle a, b, c\rangle)).$$

[1] By the term *endomorphism of an elliptic curve* we mean an analytic in the complex and rational in the general case function from the curve to itself without requesting preservation of any points. For those that preserve a distinguished point, we use the term *isogeny* as in [11, Chapter III.4].

[2] The reader might recognize that $[A, B, C] = A - B + C$, where the addition and subtraction are defined with respect to a fixed point $O$ or the point in infinity in the standard way as recalled in the introduction. The proof that $\mathcal{E}$ with $+$ is an abelian group can be found in, e.g. [7, pp. 66–67]), and hence $\mathcal{E}$ with $[-,-,-]$ is an abelian heap. The latter also becomes clear from the forthcoming description of the ternary operation in the algebraic way.

https://doi.org/10.1017/S0013091523000275 Published online by Cambridge University Press

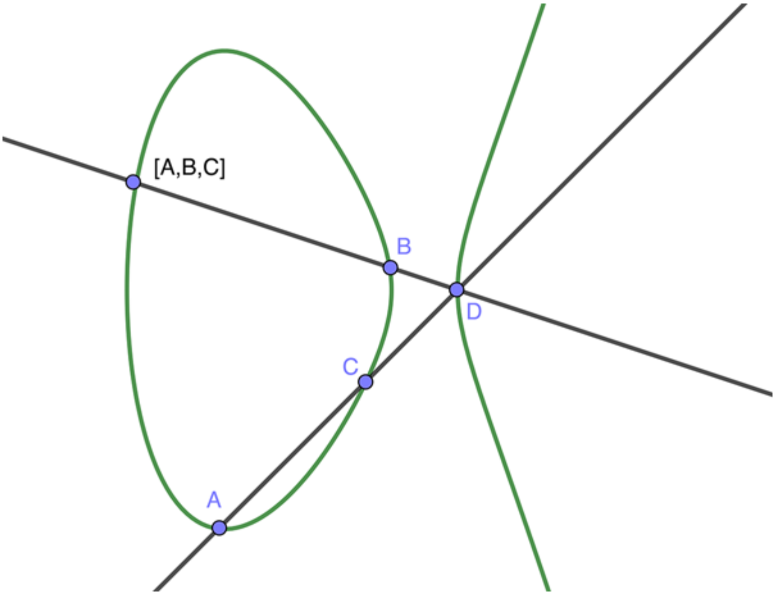

Figure 1. Construction of the heap operation

From the algebraic point of view, since $\Lambda(\omega_1, \omega_2)$ is a subgroup of the additive group of $\mathbb{C}$ (and hence a sub-heap of the associated heap), writing $A := [a] \in \mathbb{C}/\Lambda(\omega_1, \omega_2)$ for the class of $a \in \mathbb{C}$ etc., we find

$$[A, B, C] = [a - b + c].$$

Note that although analytically number $\langle a, b, c\rangle \in \mathbb{C}$ is not defined uniquely, algebraically $[a, b, c] := a - b + c$ is. Hence, $H(\mathcal{E})$ is a *bona fide* quotient of the heap structure on the additive group of $\mathbb{C}$.

The following lemma is a standard result in the theory of elliptic curves (see e.g. [6, Proposition IV 4.18] or [8, Chapter I Theorem 4.1]).

**Lemma 2.1.** *All (analytic) endomorphisms of a nonsingular elliptic curve $\mathcal{E} := \mathbb{C}/\Lambda(\omega_1, \omega_2)$ are quotients of analytic functions*

$$f_{a,b} : \mathbb{C} \longrightarrow \mathbb{C}, \qquad z \longmapsto az + b,$$

*where $a, b \in \mathbb{C}$ and $a\Lambda(\omega_1, \omega_2) \subseteq \Lambda(\omega_1, \omega_2)$.*

**Proof.** Any analytic function on $\mathcal{E}$ corresponds to an analytic function $f : \mathbb{C} \to \mathbb{C}$ with periods $\omega_1$ and $\omega_2$ modulo $\Lambda(\omega_1, \omega_2)$. Thus, for all $\alpha \in \Lambda(\omega_1, \omega_2)$, there is an analytic (hence continuous) function

$$f_\alpha : \mathbb{C} \longrightarrow \Lambda(\omega_1, \omega_2), \qquad z \longmapsto f(z + \alpha) - f(z).$$

https://doi.org/10.1017/S0013091523000275 Published online by Cambridge University Press

Since $\Lambda(\omega_1, \omega_2)$ is discrete, $f_\alpha$ is constant, which implies that

$$f'(z+\alpha) = f'(z), \quad \text{for all } \alpha \in \Lambda(\omega_1, \omega_2).$$

In other words, the derivative $f^{'}$ is a doubly-periodic function on $\mathbb{C}$, and hence it is fully determined by its values on the fundamental parallelogram of $\Lambda(\omega_1, \omega_2)$ with vertices, say, $0$, $\omega_1$, $\omega_2$ and $\omega_1 + \omega_2$. Since the latter is compact, $f^{'}$ is bounded, and thus by Liouville's theorem, $f'(z) = a$, for some $a \in \mathbb{C}$. Therefore, $f(z) = az + b$, for some $a, b \in \mathbb{C}$. The constraints $f(z+\alpha) - f(z) \in \Lambda(\omega_1, \omega_2)$ yield $a\alpha \in \Lambda(\omega_1, \omega_2)$, for all $\alpha \in \Lambda(\omega_1, \omega_2)$, as stated. □

Recall from [3, 4] that a *truss* is an abelian heap $T$ together with an associative multiplication denoted by juxtposition that distributes over the ternary heap operation $[-,-,-]$, that is, for all $a, b, c, d \in T$,

$$a[b,c,d] = [ab, ac, ad], \qquad [a,b,c]d = [ad, bd, cd].$$

The main result of this note is contained in the following

**Theorem 2.2.** *Let $\mathcal{E} = \mathbb{C}/\Lambda(\omega_1, \omega_2)$ be a nonsingular elliptic curve. Endomorphisms of $\mathcal{E}$ are endomorphisms of the heap $H(\mathcal{E})$. Consequently, the set of all endomorphisms of $\mathcal{E}$ forms a (unital) truss $T(\mathcal{E})$ with the ternary structure inherited from that of $H(\mathcal{E})$, that is,*

$$[f,g,h](A) = [f(A), g(A), h(A)], \quad \textit{for all } A \in \mathcal{E},$$

*and with the multiplication given by composition.*

**Proof.** By Lemma 2.1, every analytic endomorphism of $\mathcal{E}$ arises as the quotient of $f_{a,b}(z) = az + b$, $a\Lambda(\omega_1, \omega_2) \subseteq \Lambda(\omega_1, \omega_2)$. Each of these functions is an endomorphism of the heap of $\mathbb{C}$, i.e.

$$\begin{aligned} f_{a,b}([z, z', z'']) &= f(z - z' + z'') \\ &= (az+b) - (az'+b) + (az''+b) = [f_{a,b}(z), f_{a,b}(z'), f_{a,b}(z'')]. \end{aligned}$$

Since $\Lambda$ is an abelian subgroup and hence also a sub-heap of $\mathbb{C}$, the functions $f_{a,b}$ descend to endomorphisms of $H(\mathcal{E})$, and thus they inherit the structure of a heap as described.

Obviously, the composition of two endomorphisms of $\mathcal{E}$ is again an endomorphism. Explicitly, if $f$ corresponds to $f_{a,b}$ and $g$ corresponds to $f_{a',b'}$, then $f \circ g$ corresponds to $f_{aa',ab'+b}$. By the definition of the heap structure $[-,-,-]$ on endomorphisms of $H(\mathcal{E})$, the composition right-distributes over $[-,-,-]$ and it left distributes by the fact that analytic endomorphisms of $\mathcal{E}$ preserve the heap operation of $H(\mathcal{E})$. □

**Remark 2.3.** It might be worth pointing out that the truss $T(\mathcal{E})$ is not arising from a ring. Any abelian heap can be converted to an abelian group by retracting it at the middle term in the ternary operation (see e.g. [4, Section 2.2]). Fixing different points on a curve leads to different albeit isomorphic groups, with the isomorphism provided

https://doi.org/10.1017/S0013091523000275 Published online by Cambridge University Press

by translation.[3] As explained in [4, Lemma 3.9] to retract $T(\mathcal{E})$ into a ring one would need to have a morphism $\Theta : \mathcal{E} \to \mathcal{E}$, such that $f \circ \Theta = \Theta \circ f = \Theta$ for all $f \in T(\mathcal{E})$. The condition $\Theta \circ f = \Theta$ implies that $\Theta$ must be a constant function, say $\Theta : A \mapsto O$ for a fixed point $O \in \mathcal{E}$. The condition $f \circ \Theta = \Theta$ now implies that $f(O) = O$, for all morphisms $f$ of $\mathcal{E}$. This is not possible, as taking a morphism $f$ corresponding to $f_{0,b}$, where $b \notin O$ or equivalently $O \neq (\wp(b), \wp'(b))$, one immediately obtains that $f(O) \neq O$.

We can retract the ternary heap operation on $\mathcal{E}$ at $O$ to the abelian group operation $A+B = [A, O, B]$, for which $O$ is the neutral element. Then $-A = [O, A, O]$ and $[A, B, C] = A - B + C$. The induced group structure on the set of endomorphisms has $\Theta$ as the neutral element. The composition of endomorphisms right distributes over this addition, but the truss left distributives law yields, for all endomorphisms $f, g, h$ and $A \in \mathcal{E}$,

$$f \circ (g + h)(A) = f \circ (g - \Theta + h)(A) = f \circ g(A) - f(O) + f \circ h(A),$$

and thus $T(\mathcal{E})$ with this (or any other for that matter) addition is not a ring (unless $f(O) = O$ for all endomorphisms $f$ of $\mathcal{E}$, which as argued above cannot be the case).

**Remark 2.4.** Notwithstanding Remark 2.3, as explained in [1, Theorem 4.3], any truss, and hence also $T(\mathcal{E})$, gives rise to a heap or family of isomorphic rings. For any $A \in \mathcal{E}$, let $c_A$ denote the constant function $c_A : \mathcal{E} \to \mathcal{E}$, $B \mapsto A$ and let us fix a point $O \in \mathcal{E}$. The abelian group $T(\mathcal{E})$ with addition $+ := [-, c_O, -]$ admits the associative multiplication

$$f \bullet g = f \circ g - c_{f(O)},$$

which distributes over the addition and hence makes the set of all endomorphisms of $\mathcal{E}$ a (non-unital) ring. It is clear, however, that this conversion of a truss into a ring requires one to make a choice of an element of the curve.

**Remark 2.5.** In view of the product of endomorphisms described in the proof of Theorem 2.2, $T(\mathcal{E})$ can be seen as the extension of a ring by a module [5, Theorem 4.2]. Let $\mathcal{E} = \mathbb{C}/\Lambda(\omega_1, \omega_2)$ and let $R(\omega_1, \omega_2)$ be the ring of all complex numbers $r$ such that $r\Lambda(\omega_1, \omega_2) \subseteq \Lambda(\omega_1, \omega_2)$. Then $R(\omega_1, \omega_2)$ acts on the heap $H(\mathcal{E})$ by the (analytic) formula: for all $r \in R(\omega_1, \omega_2)$ and $A = (\wp(a), \wp'(a))$,[4]

$$rA := (\wp(ra), \wp'(ra)).$$

Since, for all $r \in R(\omega_1, \omega_2)$, $r\Lambda(\omega_1, \omega_2) \subseteq \Lambda(\omega_1, \omega_2)$, multiplying by elements of $R(\omega_1, \omega_2)$ preserves the collinearity of points. In consequence,

$$r[A, B, C] = [rA, rB, rC], \qquad (r - s + t)A = [rA, sA, tA],$$

[3] The reader interested in the explicit description of this isomorphism in the case of elliptic curves might like to consult [9, Theorem 5.22].

[4] Thus, in particular, if $r\Lambda(\omega_1, \omega_2) = \Lambda(\omega_1, \omega_2)$, then $rA := (r^{-2}\wp(a), r^{-3}\wp'(a))$ by the homogeneity property of the Weierstrass $\wp$-function.

https://doi.org/10.1017/S0013091523000275 Published online by Cambridge University Press

for all $r, s, t \in R(\omega_1, \omega_2)$, $A, B, C \in \mathcal{E}$. Therefore, $\mathcal{E}$ is a module over the truss $T(R(\omega_1, \omega_2))$ [4], where $T(R(\omega_1, \omega_2))$ has the same multiplication as that in $R(\omega_1, \omega_2)$ and the induced abelian heap structure $[r, s, t] = r - s + t$.

Following [5, Theorem 4.2], we can now fix any $O = (\wp(o), \wp'(o))$ and define the truss $T(\omega_1, \omega_2)$ built on the set $R(\omega_1, \omega_2) \times \mathcal{E}$ with the Cartesian product heap operation

$$[(r, A), (s, B), (t, C)] = (r - s + t, [A, B, C])$$

and multiplication

$$(r, A)(s, B) = (rs, [A, rO, rB]).$$

In view of the proof of Theorem 2.2, $T(\mathcal{E}) \cong T(\omega_1, \omega_2)$.

Viewed algebraically, that is when the heap structure on $\mathcal{E}$ arises from the quotient of $\mathbb{C}$ by its subgroup and hence sub-heap $\Lambda(\omega_1, \omega_2)$, and fixing $O = [0] = \Lambda(\omega_1, \omega_2)$, the multiplication in $T(\omega_1, \omega_2)$ takes a simpler form

$$(r, [a])(s, [b]) = (rs, [a + rb]).$$

Up to isomorphism complex elliptic curves can be parametrized by lattices with periods $\omega_1 = \tau, \omega_2 = 1$, and in the following examples, we will restrict to this case and write $\Lambda(\tau)$ for $\Lambda(\tau, 1) = \mathbb{Z}\tau + \mathbb{Z}$, $R(\tau)$ for $R(\tau, 1)$ and $T(\tau)$ for $T(\tau, 1)$.

**Example 2.6.** In the case $\tau = i$, $R(i)$ is the ring of Gaussian integers $\mathbb{Z}[i]$ and so it coincides with $\Lambda(i)$ (see [6, Example IV 4.20.1]). Thus, the truss of endomorphisms of the curve $\mathcal{E} = \mathbb{C}/\Lambda(i)$ can be identified with $\mathbb{Z} \times \mathbb{Z} \times \mathcal{E}$ with operations

$$[(m, n, [a]), (m', n', [a']), (m'', n'', [a''])] = (m - m' + m'', n - n' + n'', [a - a' + a'']),$$

$$(m, n, [a], )(m', n', [a']) = (mm' - nn', mn' + nm', [(m + in)a' + a]).$$

**Example 2.7.** In the case $\tau = 2i$, $R(2i)$ coincides with the subring of the ring of integers $\mathbb{Z}[i]$ of the quadratic field $\mathbb{Q}(i) \subset \mathbb{C}$ with conductor 2, that is

$$R(i) = \mathbb{Z} + 2\mathbb{Z}[i] = \{m + 2ni \, | m, n \in \mathbb{Z}\},$$

(see [6, Example IV 4.20.3]). Thus, $T(\mathbb{C}/\Lambda(2i))$ can be identified with $\mathbb{Z} \times 2\mathbb{Z} \times \mathcal{E}$ with the Cartesian product heap operations as in Example 2.6 and multiplication

$$(m, 2n, [a])(m', 2n', [a']) = (mm' - 4nn', 2(mn' + nm'), [(m + 2ni)a' + a]) \,.$$

**Example 2.8.** Examples 2.6–2.7 describe curves with complex multiplication, such that $R(\tau)$ is strictly bigger than $\mathbb{Z}$. By [6, Theorem IV 4.19], this is the case if and only

https://doi.org/10.1017/S0013091523000275 Published online by Cambridge University Press

if $\tau = p + q\sqrt{-d}$, where $p, q \in \mathbb{Q}$ and $d$ is a positive integer, and then

$$R(\tau) = \{m + n\tau \mid m, n \in \mathbb{Z}, \text{ such that } 2np, n(p^2 + dq^2) \in \mathbb{Z}\} \subseteq \Lambda(\tau).$$

For all $p, q \in \mathbb{Q}$ and positive integers $d$, let us define the additive subgroup (hence a sub-heap) of $\mathbb{Z}$,

$$\mathbb{Z}(p, q, d) = \{n \in \mathbb{Z} \mid 2np \text{ and } n(p^2 + dq^2) \in \mathbb{Z}\}.$$

Then the multiplication in the truss

$$T(\mathbb{C}/\Lambda(p + q\sqrt{-d})) \cong \mathbb{Z} \times \mathbb{Z}(p, q, d) \times \mathbb{C}/\Lambda(p + q\sqrt{-d})$$

comes out as

$$\begin{aligned}&(m, n, [a])(m', n', [a'])\\ &\quad = \left(mm' - nn'(p^2 + dq^2), n + n' + 2nn'p, \left[\left(m + n\left(p + q\sqrt{-d}\right)\right)a' + a\right]\right).\end{aligned}$$

**Example 2.9.** Let $\tau$ be the third root of unity with the positive imaginary part. Since then $\tau = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$, we find ourselves in the setup of Example 2.8, with $p = -\frac{1}{2}$, $q = \frac{1}{2}$ and $d = 3$. One easily computes that

$$\mathbb{Z}\left(\frac{1}{2}, \frac{1}{2}, -3\right) = 2\mathbb{Z}.$$

Therefore, the truss of endomorphisms of the curve $\mathcal{E} = \mathbb{C}/\Lambda(\tau)$ comes out as $T(\tau) = \mathbb{Z} \times 2\mathbb{Z} \times \mathcal{E}$ with multiplication

$$\begin{aligned}&(m, 2n, [a])(m', 2n', [a'])\\ &\qquad\qquad = \left(mm' + 2nn', 2(n + n' - nn'), \left[\left(m - n + n\sqrt{-3}\right)a' + a\right]\right).\end{aligned}$$

## 3. In other fields

Of course, the construction of a truss of endomorphisms of an elliptic curve can be performed for the general non-complex case even though curves can be no longer identified with tori. Let $\mathbb{F}$ be a (perfect) field and let $\mathcal{E}$ be a smooth curve of genus one with a non-empty set of rational points $\mathcal{E}(\mathbb{F})$[5] (and hence an elliptic curve over $\mathbb{F}$). By using the Riemann–Roch theorem and mapping $\mathcal{E}$ into the projective plane $\mathbb{P}^2$, $\mathcal{E}$ can be represented by a cubic equation in the Weierstrass form. By the Bézout theorem, every line through two points in $\mathcal{E}$ crosses $\mathcal{E}$ at the third point, and hence the geometric construction of the

[5] These are all the points of $\mathcal{E}$ that are solutions in $\mathbb{F}$ to a polynomial equation with coefficients from $\mathbb{F}$.

heap operation

$$[-,-,-]:\mathcal{E}\times\mathcal{E}\times\mathcal{E}\longrightarrow\mathcal{E},\qquad (A,B,C)\longmapsto[A,B,C],$$

described at the beginning of § 2 can be repeated verbatim, thus leading to the abelian heap $H(\mathcal{E})$.

**Lemma 3.1.** *Every endomorphism of an elliptic curve $\mathcal{E}$ over $\mathbb{F}$ is an endomorphism of the heap $H(\mathcal{E})$. Consequently, endomorphisms of $\mathcal{E}$ form a truss $T(\mathcal{E})$.*

**Proof.** We can retract $H(\mathcal{E})$ to a group $G(\mathcal{E};O)$ at any rational point $O\in\mathcal{E}(\mathbb{F})$, so that $A+B=[A,O,B]$. Any endomorphism $f$ of $\mathcal{E}$ is an isogeny $\phi$ of $\mathcal{E}$ with respect to $O$, that is an endomorphism of $G(\mathcal{E};O)$, combined with the translation by $f(O)$ (see e.g. [11, Chapter III Example 4.7]). The isogeny $\phi$ is fully determined by $f$. Explicitly,

$$f(A)=[\phi(A),O,f(O)]=\phi(A)+f(O),\qquad \phi(A)=[f(A),f(O),O]=f(A)-f(O).$$

Since $[A,B,C]=A-B+C$ and $\phi$ is an endomorphism of $G(\mathcal{E};O)$, one easily checks that $f$ is a heap endomorphism. □

Similarly to the complex curve case, the truss $T(\mathcal{E})$ can be interpreted as a crossed product. The group $G(\mathcal{E};O)$ is a left module over the ring $R(\mathcal{E};O)$ of all isogenies of $\mathcal{E}$ at $O$ by evaluation, $(\phi,A)\mapsto\phi(A)$. Hence, $R(\mathcal{E};O)\times\mathcal{E}$ is a truss with the Cartesian product heap operation and multiplication

$$(\phi,A)(\psi,B)=(\phi\circ\psi,[A,O,\phi(B)])$$

isomorphic with $T(\mathcal{E})$ by the map

$$R(\mathcal{E};O)\times\mathcal{E}\longrightarrow T(\mathcal{E}),\qquad (\phi,A)\longmapsto[B\mapsto[\phi(B),O,A]]\,.$$

The product in the ring associated to $R(\mathcal{E};O)\times\mathcal{E}$ at the point $(c_O:A\mapsto O,O)$ as in Remark 2.4 comes out as

$$(\phi,A)\bullet(\psi,B)=(\phi\circ\psi,\phi(B)).$$

**Acknowledgements.** The author would like to thank Laiachi El Kaoutit first for raising the question about the additive structure on elliptic curves during the conference of *Hopf algebras, monoidal categories and related topics*, Bucharest, July 27–29, 2022, and second for the subsequent comments and suggestions. The author would also like to thank Simion Breaz and Bernard Rybołowicz for their comments and suggestions.

**Funding Statement.** This research is partially supported by the National Science Centre, Poland (grant no. 2019/35/B/ST1/01115).

## References

(1) R. R. Andruszkiewicz, T. Brzeziński and B. Rybołowicz, *Ideal ring extensions and trusses*, *J. Algebra* **600** (2022), 237–278.

(2) R. Baer, Zur Einführung des Scharbegriffs, *J. Reine Angew. Math.* **160** (1929), 199–207.

(3) T. Brzeziński, Trusses: Between braces and rings, *Trans. Amer. Math. Soc.* **372**(6) (2019), 4149–4176.

(4) T. Brzeziński, Trusses: Paragons, ideals and modules, *J. Pure Appl. Algebra* **224**(6) (2020), 106258.

(5) T. Brzeziński, and B. Rybołowicz, Congruence classes and extensions of rings with an application to braces, *Comm. Contemp. Math.* **23**(4) (2021), 2050010.

(6) R. Hartshorne, *Algebraic Geometry* (Springer-Verlag, New York, 1977).

(7) D. Husemöller, *Elliptic Curves*, 2nd edn. (Springer, New York, 2004).

(8) S. Lang, *Elliptic Curves: Diophantine Analysis* (Springer-Verlag, New York, 1978).

(9) I. Niven, H. S. Zuckerman and H. Montgomery, *An Introduction to the Theory of Numbers*, 5th edn. (Wiley, New York, 1991).

(10) H. Prüfer, Theorie der Abelschen Gruppen. I. Grundeigenschaften, *Math. Z.* **20**(1) (1924), 165–187.

(11) J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edn. (Springer-Verlag, Dordrecht, 2009).

https://doi.org/10.1017/S0013091523000275 Published online by Cambridge University Press