# THE RANK OF $y^2 = x^3 - 2$ VIA MAZUR-TATE METHODS

DAVID BENJAMIN LIM

When I was a young kid, I heard the mathematical fact that the only (positive) integer that is one more than a square and one less than a cube is 26. Said differently, the only integer solutions $(x, y)$ to $y^2 = x^3 - 2$ are given by $(3, \pm 5)$. There are elementary methods to prove this, using the fact that the ring of integers of $\mathbf{Q}(\sqrt{-2})$ is a unique factorization domain. However, what if we now ask for *rational* solutions? The equation

$$E : y^2 = x^3 - 2$$

is of course an elliptic curve over $\mathbf{Q}$. Therefore, this more difficult question is equivalent to calculating asking for the *structure* of the Mordell-Weil group of $E$.

Let us first analyze the structure of the torsion subgroup of $E$, namely $E_{\text{tors}}$. The discriminant of $E$ is $\Delta = -4^3 \cdot 3^3$ and so $E$ has good reduction outside of 2 and 3. One checks that $\#E(\mathbf{F}_5) = 6$ and $\#E(\mathbf{F}_7) = 7$, and thus $E(\mathbf{Q})_{\text{tors}} = 0$. It now remains to compute the rank of $E$. In Silverman's *Arithmetic of Elliptic Curves*, one finds an algorithm to compute the rank of an elliptic curve over $\mathbf{Q}$ - in the case that the 2-torsion is defined over $\mathbf{Q}$. However, the 2-torsion of $E$ is *not* defined over $\mathbf{Q}$, so the method in Silverman cannot be applied. In this article, we prove the following theorem:

**Theorem 1.** *The rank of $E$ is* 1.

We remark that since $P = (3, 5)$ is non-torsion, it is enough to show that $\operatorname{rank}(E) \leq 1$. Certainly, it is true that there are computer programs such as MAGMA that can calculate the rank of $E$. Nonetheless, we believe that there is value in bounding the rank of $E$ "by hand." Reason being, the latter method requires non-trivial input about the arithmetic of a certain $S_3$-extension of $\mathbf{Q}$. In addition, the calculations turns out to be very explicit (computing invariants in terms of generators and relations) which is always fun!

## 1. The method of 2-descent

We will use the method of 2-descent to compute the rank of $E$. As in the proof of the weak Mordell-Weil theorem, we want to compute the dimension of the $\mathbf{F}_2$-vector space $E(\mathbf{Q})/2E(\mathbf{Q})$, and in fact for the purposes of Theorem 1, we want to show that $\dim_{\mathbf{F}_2} E(\mathbf{Q})/2E(\mathbf{Q}) \leq 1$.To this end, consider the short exact sequence of étale sheaves on $\operatorname{Spec} \mathbf{Q}$

$$0 \to E[2] \to E \xrightarrow{2\cdot} E \to 0.$$

This gives an injection

$$\frac{E(\mathbf{Q})}{2E(\mathbf{Q})} \hookrightarrow H^1(G_{\mathbf{Q}}, E[2](\overline{\mathbf{Q}})).$$

Now we run into the following problem: The Galois cohomology group $H^1(G_{\mathbf{Q}}, E[2](\overline{\mathbf{Q}}))$ is often infinite-dimensional. To illustrate this, let us suppose for the moment that the 2-torsion of $E$ is defined over $\mathbf{Q}$. Then $E[2](\overline{\mathbf{Q}}) \simeq (\mathbf{Z}/2\mathbf{Z})^{\oplus 2}$, and identifying $\mathbf{Z}/2\mathbf{Z}$ with $\mu_2$, we deduce by the Kummer sequence that $H^1(G_{\mathbf{Q}}, E[2](\overline{\mathbf{Q}})) \simeq (\mathbf{Q}^\times/\mathbf{Q}^{\times 2})^{\oplus 2}$. This is *very* infinite-dimensional!

The get-out-of-jail-free card, as introduced in the Mazur-Tate article is to work *integrally*. The reason this is great is because for a number field $K$, the group of non-squares $K^\times/K^{\times 2}$ is infinite-dimensional, but $\mathcal{O}_K^\times/\mathcal{O}_K^{\times 2}$ is not, thanks to Dirichlet's unit theorem. In view of this, we will now modify our approach above as follows. First, observe that the elliptic curve $E$ has bad reduction at 2 and 3 and nowhere else. Therefore, we may extend $E$ to an elliptic scheme $\mathcal{E}$ over $\operatorname{Spec} \mathbf{Z}[1/6]$. In simple terms, $\mathcal{E}$ is simply the vanishing locus of the same equation for $E$ in $\mathbf{P}^2_{\mathbf{Z}[1/6]}$, since $E$ is already defined integrally. The more advanced reader may note that $\mathcal{E}$ is also the Néron model of $E$ over $\operatorname{Spec} \mathbf{Z}[1/6]$, since any abelian scheme over a Dedekind base is the Néron model of its generic fiber.

*Date*: August 21, 2021.

Now by the valuative criteria for properness,

$$\frac{E(\mathbf{Q})}{2E(\mathbf{Q})} = \frac{\mathcal{E}(\mathbf{Z}[1/6])}{2\mathcal{E}(\mathbf{Z}[1/6])}$$

and therefore it suffices to show that $\dim_{\mathbf{F}_2} \mathcal{E}(\mathbf{Z}[1/6])2\mathcal{E}(\mathbf{Z}[1/6]) \leq 1$. Furthermore, by considering the exact sequence arising from multiplication by 2 on $\mathcal{E}$, we obtain (as in the case for $E$) an injection

$$\frac{\mathcal{E}(\mathbf{Z}[1/6])}{2\mathcal{E}(\mathbf{Z}[1/6])} \hookrightarrow H^1(\mathbf{Z}[1/6], \mathcal{E}[2]). \tag{1}$$

The upshot of replacing $E$ with $\mathcal{E}$? The group $H^1(\mathbf{Z}[1/6], \mathcal{E}[2])$ is finite! In fact, its dimension as an $\mathbf{F}_2$-vector space is bounded by 1. This is what we will show next.

## 2. Computing $H^1(\mathbf{Z}[1/6], \mathcal{E}[2])$

2.1. **Preliminaries.** Let $K$ denote the splitting field of $x^3 - 2$. It is a basic exercise in Galois theory that $K = \mathbf{Q}(\sqrt[3]{2}, \omega)$, where $\omega$ is a primitive third root of unity. By definition of the group law on an elliptic curve, the 2-torsion on $E$ is precisely the zero locus of $x^3 - 2$, and therefore

$$E[2] \otimes_{\mathbf{Q}} K \simeq \{\infty, \sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\} \simeq (\mathbf{Z}/2\mathbf{Z})^{\oplus 2}$$

where the last isomorphism is non-canonical, i.e. depends on a choice of basis. Now as we will see later, calculating $H^1(\mathbf{Z}[1/6], \mathcal{E}[2])$ boils down to performing explicit computations in some extension of $\mathcal{O}_K^\times$ mod squares. Hence, we now record the following theorem from a note of Keith Conrad. It contains essentially all important information about $K$, such as its discriminant, class number, etc.

**Theorem 2.** *The field $K$ has class number 1 and discriminant $-2^4 3^7$. The ramified primes 2 and 3 factor as*

$$(2) = (\sqrt[3]{2})^3, \qquad (3) = (\eta)^3,$$

*where $\eta = \sqrt{-3}/(1 + \sqrt[3]{2})$. Moreover, the ring of integers of $K$ is $\mathbf{Z}[\varepsilon]$, where*

$$\varepsilon = -\frac{1 + 2\sqrt[3]{2} + \sqrt[3]{4}}{3} + \frac{1 - \sqrt[3]{2} + \sqrt[3]{4}}{3}\omega = \frac{\omega - u}{\pi}$$

*with $\pi = 1 + \sqrt[3]{2}$, satisfies $\varepsilon^2 = -u\varepsilon - u$, where $u = 1 + \sqrt[3]{2} + \sqrt[3]{4}$ is the fundamental unit of $\mathbf{Q}(\sqrt[3]{2})$. The unit group of $\mathcal{O}_K$ has six roots of unity (namely powers of $-\omega$), rank 2, and basis $\{\varepsilon, \overline{\varepsilon}\}$.*

In addition, we make the following important observation. Let $S$ be the set of primes in $\mathcal{O}_K$ lying over 2 and 3. By Theorem 2 above, $S = \{(\sqrt[3]{2}), (\eta)\}$ and consequently $\operatorname{Spec} \mathcal{O}_{K,S} \to \operatorname{Spec} \mathbf{Z}[1/6]$ is finite étale, where

$$\mathcal{O}_{K,S} := \{x \in K : \nu_{\mathfrak{p}}(x) \geq 0 \text{ for all } \mathfrak{p} \notin S\}.$$

Furthermore, the Galois group $G := \operatorname{Gal}(K/\mathbf{Q})$ acts on the ring $\mathcal{O}_{K,S}$, and we claim that in fact $G$ is equal to the full automorphism group of $\mathcal{O}_{K,S}$ over $\mathbf{Z}[1/6]$, i.e. $\operatorname{Spec} \mathcal{O}_{K,S} \to \operatorname{Spec} \mathbf{Z}[1/6]$ is a Galois cover with Galois group $G$. Indeed, this follows from the fact that any automorphism of the generic fiber $K$ preserves $\mathcal{O}_{K,S}$, since $G(S) \subseteq S$.

To conclude this subsection, we show that $\mathcal{E}[2]$ splits over $\mathcal{O}_{K,S}$.

**Proposition 3.** *The group scheme $\mathcal{E}[2]$ splits over $\mathcal{O}_{K,S}$, and is (non-canonically) isomorphic to the constant group $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.*

*Proof.* Since the generic fiber of $\mathcal{E}[2]$, namely $E[2]$ splits over $K = \operatorname{Frac}(\mathcal{O}_{K,S})$, the claim follows from the following lemma. □

**Lemma 4.** *Let $G_1, G_2$ be finite étale group schemes over a normal scheme $\operatorname{Spec} A$. Let $K$ denote the fraction field of $A$. If $(G_1)_K \simeq (G_2)_K$ (as group schemes) then $G_1 \simeq G_2$.*

*Proof.* By Lemma 2.1.3 of Brian Conrad's reductive group schemes notes, the Hom functor $\underline{\operatorname{Hom}}_{A\text{–Gp}}(G_1, G_2)$ is represented by an affine scheme scheme of finite presentation over $\operatorname{Spec} A$. In fact, by passing to a trivialization of $G_1$ and $G_2$, we see that the representing scheme $\operatorname{Spec} B$ is finite over $\operatorname{Spec} A$ . The lemma now follows from the fact that

$$\underline{\operatorname{Hom}}_{A\text{–Gp}}(G_1, G_2)(A) \to \underline{\operatorname{Hom}}_{A\text{–Gp}}(G_1, G_2)(K)$$

is surjective. Indeed, given an $A$-algebra homomorphism $B \to K$, the image is necessarily integral over $A$. But $A$ is normal and hence the image of this homomorphism lands in $A$. $\square$

2.2. **Kummer theory.** By Proposition 3, we know that $\mathcal{E}[2]$ is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^{\oplus 2}$ over $\operatorname{Spec} \mathcal{O}_{K,S}$. Therefore, if we want to calculate $H^1(\mathbf{Z}[1/6], \mathcal{E}[2])$, it only seems natural to pass to $\mathcal{O}_{K,S}$, for the simple reason that $\mathcal{E}[2]$ is now isomorphic to the explicit group scheme $(\mathbf{Z}/2\mathbf{Z})^{\oplus 2} \simeq \mu_2^{\oplus 2}$. Even better, we now have the Kummer sequence at our disposal, which as we will see makes everything *very* explicit. To this end, recall that

$$\operatorname{Spec} \mathcal{O}_{K,S} \to \operatorname{Spec} \mathbf{Z}[1/6]$$

is Galois with Galois group $G$. Therefore, we have a Hochschild-Serre spectral sequence

$$H^i(G, H^j(\mathcal{O}_{K,S}, \mathcal{E}[2])) \implies H^{i+j}(\mathbf{Z}[1/6], \mathcal{E}[2]).$$

The low degree terms of this spectral sequence give rise to an exact sequence

(2)

$$\begin{tikzcd}
0 \arrow[r] & H^1(G, H^0(\mathcal{O}_{K,S}, \mathcal{E}[2])) \arrow[r] & H^1(\mathbf{Z}[1/6], \mathcal{E}[2]) \arrow[d] & \\
& & H^1(\mathcal{O}_{K,S}, \mathcal{E}[2])^G \arrow[r] & H^2(G, H^0(\mathcal{O}_{K,S}, \mathcal{E}[2])).
\end{tikzcd}$$

We claim:

**Lemma 5.** *We have*

$$H^1(G, H^0(\mathcal{O}_{K,S}, \mathcal{E}[2])) = 0.$$

*Proof.* Since

$$H^0(\mathcal{O}_{K,S}, \mathcal{E}[2]) = \mathcal{E}[2](\mathcal{O}_{K,S}) = E[2](K),$$

it suffices to show that

$$H^1(G, E[2](K)) = 0.$$

Now consider the normal subgroup $H := \operatorname{Gal}(K/\mathbf{Q}(\omega))$. By inflation-restriction with respect to this normal subgroup, we obtain an exact sequence

$$0 \to H^1(G/H, E[2](K)^H) \to H^1(G, E[2](K)) \to H^1(H, E[2](K)).$$

The term on the right is zero because $\#H = 3$ while $\#E[2](K) = 4$. On the other hand, the term on the left is also zero because $E[2](K)^H = \{\infty\}$. Hence $H^1(G, E[2](K)) = 0$ as desired. $\square$

Recall our goal is to show that

$$\dim_{\mathbf{F}_2} H^1(\mathbf{Z}[1/6], \mathcal{E}[2]) \leq 1.$$

By Lemma 5 above and (2), we obtain an injection

$$H^1(\mathbf{Z}[1/6], \mathcal{E}[2]) \hookrightarrow H^1(\mathcal{O}_{K,S}, \mathcal{E}[2])^G \tag{3}$$

and so it suffices to show that the same is true of the right side of (3). Let us spell out the right side of (3) without the Galois invariants. By Proposition 3, the 2-torsion $\mathcal{E}[2]$ is abstractly isomorphic to $\mu_2^{\oplus 2}$. Therefore, the calculation of $H^1(\mathcal{O}_{K,S}, \mathcal{E}[2]) \simeq H^1(\mathcal{O}_{K,S}, \mu_2)^{\oplus 2}$ reduces to one using the Kummer sequence

$$0 \to \mu_2 \to \mathbf{G}_m \to \mathbf{G}_m \to 0.$$

Note that this is exact on the étale site of $\operatorname{Spec} \mathcal{O}_{K,S}$, precisely because 2 is an $S$-unit.

If we pass to the long exact sequence in cohomology, we get a short exact sequence

$$0 \to \mathcal{O}_{K,S}^\times / \mathcal{O}_{K,S}^{\times 2} \to H^1(\mathcal{O}_{K,S}, \mu_2)^{\oplus 2} \to \operatorname{Pic}(\mathcal{O}_{K,S})[2]^{\oplus 2} \to 0.$$

But $\operatorname{Pic}(\mathcal{O}_{K,S})$ is zero because it receives a surjection from $\operatorname{Pic}(\mathcal{O}_K)$ which is zero by Theorem 2. In summary, we have shown that as *abstract abelian groups*,

$$H^1(\mathcal{O}_{K,S}, \mathcal{E}[2]) \simeq H^1(\mathcal{O}_{K,S}, \mu_2)^{\oplus 2} \simeq (\mathcal{O}_{K,S}^\times / \mathcal{O}_{K,S}^{\times 2})^{\oplus 2}. \tag{4}$$

At this point, it is tempting to think that the Galois action on $(\mathcal{O}_{K,S}^\times / \mathcal{O}_{K,S}^{\times 2})^{\oplus 2}$ is coordinate-wise given by the usual Galois action on $K$. However, this is false because the Galois action on $(\mathcal{O}_{K,S}^\times / \mathcal{O}_{K,S}^{\times 2})^{\oplus 2}$ is "twisted," in the sense that it comes from the Galois action on $\mathcal{E}[2]$.

## 3. The Galois action on $(\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2})^{\oplus 2}$

Before we begin any explicit computations, recall that $K = \mathbf{Q}(\sqrt[3]{2},\omega)$ where $\omega$ is a primitive third root of unity. The Galois group of $K$ (always denoted $G$) is abstractly isomorphic to $S_3$, with explicit generators given by

$$\begin{aligned} \sigma : \sqrt[3]{2} &\mapsto \sqrt[3]{2}\omega \qquad & \tau : \omega &\mapsto \omega^2 \\ \omega &\mapsto \omega, & \sqrt[3]{2} &\mapsto \sqrt[3]{2} \end{aligned}$$

satisfying the relations $\sigma^3 = \tau^2 = 1$, $\sigma\tau = \tau\sigma^2$. For any $(a,b) \in (\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2})^{\oplus 2}$, we want to give an explicit description of $\sigma \cdot (a,b)$ and $\tau \cdot (a,b)$ via the isomorphism (3.2). To write down such an action explicitly, it makes sense intuitively that we must *also* compute the (usual) Galois action on the finite-dimensional $\mathbf{F}_2$-vector space $\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$, where by "usual" we mean the one coming from the Galois action on $K$.

This section is organized as follows. In Subsection 3.1, we determine an explicit $\mathbf{F}_2$-basis for $\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$. We then compute the "usual" Galois action on $\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$ in terms of this basis. As a sanity check, we note that the Galois action on $\mathcal{O}_K^\times$ descends to $\mathcal{O}_{K,S}^\times$. Why? Two reasons: First, for any prime $p \in \mathbf{Z}$, $G$ can only permute the primes $\mathfrak{p} \in \mathcal{O}_K$ *lying over* $p$. Second, for each of $2, 3 \in \mathbf{Z}$, there is a *unique* prime in $\mathcal{O}_K$ lying over each of these respectively (Theorem 2). Finally, in Subsection 3.2, we compute the twisted Galois action on $(\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2})^{\oplus 2}$ via the isomorphism (3.2).

### 3.1. The restriction of the Galois action on $K$ to $\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$.

**Lemma 6.** *The group $\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$ has an $\mathbf{F}_2$-basis*

$$\{-1, \varepsilon, \overline{\varepsilon}, \eta, \sqrt[3]{2}\}.$$

*Proof.* Let $S$ (as before) denote the set of primes in $\operatorname{Spec}\mathcal{O}_K$ lying over $2, 3 \in \mathbf{Z}$. Observe that we have an exact sequence

$$1 \to \mathcal{O}_K^\times \to \mathcal{O}_{K,S}^\times \to \prod_{\mathfrak{p}\in S} \mathbf{Z} \to 1 \tag{5}$$

where the last map sends an element $x$ to the product of its $\mathfrak{p}$-adic valuations. This map is surjective precisely because the primes in $S$ are principal. Now an argument with the snake lemma shows that (5) gives rise to a (split) exact sequence of $\mathbf{F}_2$-modules

$$1 \to \mathcal{O}_K^\times/\mathcal{O}_K^{\times 2} \to \mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2} \to \prod_{\mathfrak{p}\in S} \mathbf{F}_2 \to 1.$$

In particular, we have

$$\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2} \simeq \mathcal{O}_K^\times/\mathcal{O}_K^{\times 2} \oplus \prod_{\mathfrak{p}\in S} \mathbf{F}_2.$$

Now for each of the (not necessarily primitive) 6-th roots of unity $-\omega, \omega^2, -1, \omega, -\omega^2, 1$, we see that only $-1$ is not a square. Therefore, it follows that $\mathcal{O}_K^\times/\mathcal{O}_K^{\times 2}$ has basis $\{-1, \varepsilon, \overline{\varepsilon}\}$. Hence $\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$ has basis

$$\{-1, \varepsilon, \overline{\varepsilon}, \eta, \sqrt[3]{2}\}$$

as claimed. □

**Proposition 7.** *The action of $\tau$ on each of the five basis elements of $\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$ is given as follows:*

$$\begin{aligned} \tau(-1) &= -1 \qquad (6)\\ \tau(\varepsilon) &= \overline{\varepsilon} \qquad (7)\\ \tau(\overline{\varepsilon}) &= \varepsilon \qquad (8)\\ \tau(\eta) &= -\eta \qquad (9)\\ \tau(\sqrt[3]{2}) &= \sqrt[3]{2}. \qquad (10) \end{aligned}$$

*Proof.* (6) and (10) are immediate. For (7) and (8), we will use the relation

$$\varepsilon^2 = -u\varepsilon - u$$

from Theorem 2. Noting that $\tau$ fixes $u = 1 + \sqrt[3]{2} + \sqrt[3]{4}$, it follows from this relation that $\tau(\varepsilon)$ must either fix $\varepsilon$ or send it to its conjugate $\overline{\varepsilon}$. Now if it fixes $\varepsilon$, then $\varepsilon \in K^{\langle\tau\rangle} = \mathbf{Q}(\sqrt[3]{2})$. Then $\mathcal{O}_K = \mathbf{Z}[\varepsilon]$ must be contained in the ring of integers of $\mathbf{Q}(\sqrt[3]{2})$ which is a contradiction. This establishes (7) and hence (8) as well. Finally, (9) is a straight up calculation:

$$\begin{aligned} \tau(\eta) &= \frac{\tau(\sqrt{-3})}{\tau(1+\sqrt[3]{2})} \\ &= \frac{\tau(2\omega+1)}{1+\sqrt[3]{2}} \\ &= \frac{2\omega^2+1}{1+\sqrt[3]{2}} \\ &= \frac{-2\omega-1}{1+\sqrt[3]{2}} \\ &= -\eta. \end{aligned}$$

□

**Proposition 8.** *The action of $\sigma$ on each of the five basis elements of $\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$ is given as follows:*

$$\sigma(-1) = -1 \tag{11}$$
$$\sigma(\varepsilon) = \varepsilon\overline{\varepsilon} \tag{12}$$
$$\sigma(\overline{\varepsilon}) = \varepsilon \tag{13}$$
$$\sigma(\eta) = \varepsilon\eta \tag{14}$$
$$\sigma(\sqrt[3]{2}) = \sqrt[3]{2}. \tag{15}$$

*Proof.* The action of $\sigma$ is trickier to compute than $\tau$. As most of the computations are done in the note of Keith Conrad, we will only give a brief overview. Now (11) is evidently trivial, while for (15) observe crucially that $\omega$ is already a square in $\mathcal{O}_{K,S}^\times$. Therefore,

$$\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega = \sqrt[3]{2}$$

in $\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$.

Now comes the tricky part, computing (12), (13) and (14). To this end, consider the log map

$$\begin{aligned} L: \quad \mathcal{O}_K^\times &\to \mathbf{R}^3 \\ x &\mapsto (2\log|x|, 2\log|\sigma(x)|, 2\log|\sigma^2(x)|). \end{aligned}$$

An important property of the log map is that $\ker L$ consists entirely of roots of unity (this is true for any number field). To see this, suppose that $L(x) = 0$. Then this means for every embedding $\phi : K \hookrightarrow \mathbf{C}$, $\phi(x) = 1$. Since the embeddings $K \hookrightarrow \mathbf{C}$ permute the roots of the minimal polynomial $p(T)$ of $x$, and the coefficients of $p(T)$ are symmetric functions in the roots, it follows in fact that the coefficients of $p(T)$ must be *bounded*. Said differently, only finitely many polynomials in $\mathbf{Q}[T]$ can arise as minimal polynomials of elements in $\ker L$, so $|\ker L| < \infty$. This proves that any $x \in \mathcal{O}_K^\times$ with $L(x) = 0$ must be a root of unity. Consequently, if $L(x) = L(y)$, then $x = \zeta y$ for some root of unity $\zeta$.

The log map is useful to test for equality between two elements of $\mathcal{O}_K^\times$, simply because the "linearized" version of the problem can now be checked coordinate-wise. On the bottom of page 12 of Keith Conrad's note, he computes that $L(\sigma(\varepsilon)) = L(\overline{\varepsilon}) - L(\varepsilon)$, and therefore by the fact above, $\sigma(\varepsilon) = \zeta\varepsilon^{-1}\overline{\varepsilon}$ for some root of unity $\zeta$. Taking traces down to $\mathbf{Q}$, he finds that $\zeta = 1$. In conclusion,

$$\sigma(\varepsilon) = \varepsilon^{-1}\overline{\varepsilon} = \varepsilon\overline{\varepsilon}$$

in $\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$, proving (12). For (13), we use the result (computed on page 13) that $\sigma^2(\varepsilon) = \overline{\varepsilon}^{-1}$. Applying $\sigma$ to both sides of (11), we obtain

$$\sigma(\overline{\varepsilon}) = \sigma(\varepsilon)^{-1}\sigma^2(\varepsilon) = \varepsilon$$

in $\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$. Finally for (14), on page 14 of the note we find that $\sigma(\eta)/\eta = \varepsilon\omega$, and therefore

$$\sigma(\eta) = \varepsilon\eta$$

since $\omega$ is a square in $\mathcal{O}_K^\times$. □

**3.2. The twisted Galois action on $(\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2})^{\oplus 2}$.** Recall the isomorphism of abstract abelian groups (3.2), namely

$$H^1(\mathcal{O}_{K,S}, \mathcal{E}[2]) \simeq H^1(\mathcal{O}_{K,S}, \mu_2)^{\oplus 2} \simeq (\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2})^{\oplus 2}.$$

To determine the twisted Galois action on $(\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2})^{\oplus 2}$, we will need to fix a basis of $\mathcal{E}[2](\mathcal{O}_{K,S})$, and then compute the Galois action in terms of this basis.

Let $\{e_1, e_2\}$ denote the standard basis of $\mu_2^{\oplus 2}$, and by abuse of notation, the standard basis of $H^1(\mathcal{O}_{K,S}, \mu_2)^{\oplus 2}$. Under the Kummer isomorphism

$$H^1(\mathcal{O}_{K,S}, \mu_2)^{\oplus 2} \simeq (\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2})^{\oplus 2},$$

to understand the Galois on the right hand side, it is enough to understand the Galois action on the left hand side. But the Galois action on the left hand side is the one coming from an *identification* of

$$\mathcal{E}[2](\mathcal{O}_{K,S}) = E[2](K) = \{\infty, \sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\}$$

with $\mu_2^{\oplus 2}$. If we choose the following identification, namely

$$\begin{aligned} e_1 &:= \sqrt[3]{2}; \\ e_2 &:= \sqrt[3]{2}\omega; \\ e_1 + e_2 &:= \sqrt[3]{2}\omega^2; \end{aligned}$$

then we can compute the Galois action entirely in terms of $e_1$ and $e_2$.

**Proposition 9.** *For $(a, b) \in (\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2})^{\oplus 2}$, we have*

$$\begin{aligned} \tau \cdot (a, b) &= (\tau(a), \tau(ab)); \\ \sigma \cdot (a, b) &= (\sigma(b), \sigma(ab)); \end{aligned}$$

*where the action on the right hand side is the (usual) Galois action on elements of $\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$.*

*Proof.* The element $(a, b) \in (\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2})^{\oplus 2}$ corresponds to $ae_1 + be_2 \in H^1(\mathcal{O}_{K,S}, \mathcal{E}[2])$. We first compute the action of $\tau$. We have

$$\tau(e_1) = \tau(\sqrt[3]{2}) = \sqrt[3]{2} = e_1$$

and

$$\tau(e_2) = \tau(\sqrt[3]{2}\omega) = \sqrt[3]{2}\omega^2 = e_1 + e_2.$$

Thus

$$\tau(ae_1 + be_2) = \tau(a)e_1 + \tau(b)(e_1 + e_2) = \tau(a)e_1 + \sigma(ab)e_2,$$

i.e.

$$\tau \cdot (a, b) = (\tau(a), \tau(ab)).$$

For $\sigma$, we have

$$\sigma(e_1) = \sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega = e_2$$

and

$$\sigma(e_2) = \sigma(\sqrt[3]{2}\omega) = \sqrt[3]{2}\omega^2 = e_1 + e_2.$$

Thus

$$\sigma(ae_1 + be_2) = \sigma(a)e_2 + \sigma(b)(e_1 + e_2) = \sigma(b)e_1 + \sigma(ab)e_2,$$

i.e.

$$\sigma \cdot (a, b) = (\sigma(b), \sigma(ab)).$$

□

## 4. Proof of Theorem 1

We now prove Theorem 1. By (1) and (3), we have injections

$$\frac{\mathcal{E}(\mathbf{Z}[1/6])}{2\mathcal{E}(\mathbf{Z}[1/6])} \hookrightarrow H^1(\mathbf{Z}[1/6], \mathcal{E}[2]) \hookrightarrow H^1(\mathcal{O}_{K,S}, \mathcal{E}[2])^G.$$

Furthermore, the right-most term is isomorphic to $((\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2})^{\oplus 2})^G$ with the $G$-action given by Proposition (9):

$$\begin{aligned} \tau \cdot (a,b) &= (\tau(a), \tau(ab)) \\ \sigma \cdot (a,b) &= (\sigma(b), \sigma(ab)) \end{aligned}$$

By $\tau(a), \sigma(b)$, etc, we mean the restriction of the Galois action on $K$ to $\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$, as computed in Propositions 8 and 7. To this end, let us write

$$\begin{aligned} a &= (-1)^{m_1}\varepsilon^{m_2}\overline{\varepsilon}^{m_3}\eta^{m_4}\sqrt[3]{2}^{m_5} \\ b &= (-1)^{n_1}\varepsilon^{n_2}\overline{\varepsilon}^{n_3}\eta^{n_4}\sqrt[3]{2}^{n_5}. \end{aligned}$$

for $\vec{m} := (m_1, \ldots, m_5)$ and $\vec{n} := (n_1, \ldots, n_5)$ in $\mathbf{F}_2^{\oplus 5}$.

Now suppose that $(a,b) \in (\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2})^{\oplus 2}$ is invariant under $\tau$ and $\sigma$. Then the following relations must hold:

$$\begin{aligned} \tau(a) &= a \\ \sigma(b) &= a \\ \tau(ab) &= b \\ \sigma(ab) &= b. \end{aligned}$$

The first relation $\tau(a) = a$ says

$$(-1)^{m_1+m_4}\overline{\varepsilon}^{m_2}\varepsilon^{m_2}\eta^{m_4}\sqrt[3]{2}^{m_5} = (-1)^{m_1}\varepsilon^{m_2}\overline{\varepsilon}^{m_3}\eta^{m_4}\sqrt[3]{2}^{m_5},$$

which implies that

$$\begin{aligned} m_4 &= 0 \\ m_2 &= m_3. \end{aligned}$$

In other words,

$$a = (-1)^{m_1}\varepsilon^{m_2}\overline{\varepsilon}^{m_2}\sqrt[3]{2}^{m_5}. \tag{16}$$

Now consider the second relation $\sigma(b) = a$. Using (16), this reads

$$(-1)^{n_1}\varepsilon^{n_2+n_3+n_4}\overline{\varepsilon}^{n_2}\eta^{n_4}\sqrt[3]{2}^{n_5} = (-1)^{m_1}\varepsilon^{m_2}\overline{\varepsilon}^{m_2}\sqrt[3]{2}^{m_5}.$$

Comparing coefficients, we obtain

$$\begin{aligned} m_1 &= n_1 \\ m_2 &= n_2 + n_3 + n_4 \\ m_2 &= n_2 \\ n_4 &= 0 \\ n_5 &= m_5. \end{aligned}$$

and therefore $n_3 = 0$ as well. Now we summarize what we have deduced about $\vec{m}$ and $\vec{n}$ so far:

$$\begin{aligned} \vec{m} &= (m_1, m_2, m_2, 0, m_5) \\ \vec{n} &= (m_1, m_2, 0, 0, m_5). \end{aligned}$$

We're nearly there. Now consider the third relation $\tau(ab) = b$. The product $ab$ corresponds to adding the vectors $\vec{m}$ and $\vec{n}$. But $\vec{m} + \vec{n} = (0, 0, m_2, 0, 0)$ and therefore

$$\tau(ab) = \tau(0, 0, m_2, 0, 0) = (0, m_2, 0, 0, 0).$$

This must equal $b$, which in terms of $\vec{n}$, says

$$(0, m_2, 0, 0, 0) = (m_1, m_2, 0, 0, m_5).$$

In other words, $m_1 = m_5 = 0$. The final relation does not yield any extra information since $\sigma(ab) = \tau(ab)$. We have thus proven that $((\mathcal{O}_{K,S}^{\times}/\mathcal{O}_{K,S}^{\times 2})^{\oplus 2})^G$ is spanned by $(\varepsilon, \varepsilon)$, in particular is 1-dimensional. This completes the proof of Theorem 1.