ON EISENSTEIN INTEGER TORSION FIELDS OF ELLIPTIC CURVES WITH HEXIC SYMMETRIES

TANNON N. WARNICK

Abstract. We investigate the algebraic and Galois structures of torsion fields generated by elliptic curves of the form $E : y^2 = x^3 + D$, which admit complex multiplication by the ring of Eisenstein integers $\mathbb{Z}[\omega]$. Unlike the classical quartic symmetry collapse observed in curves with Gaussian multiplication, the presence of a sixth root of unity ζ_6 introduces a hexic symmetry variation in the associated division ideals. We establish recursive relations for the corresponding Eisenstein division polynomials ψ_α for $\alpha \in \mathbb{Z}[\omega]$ and analyze the conditions under which these polynomials yield irreducible Eisenstein configurations over $\mathbb{Q}(\omega)$. Finally, we outline the structural obstructions to achieving direct cyclic transitions in the associated x-coordinate splitting fields.

1. Introduction and Endomorphism Structure

Let E be the elliptic curve defined by $y^2 = x^3 + D$ over $\mathbb{Q}$, where $D \in \mathbb{Z} \setminus \{0\}$. This family of curves admits complex multiplication by the ring of Eisenstein integers $\mathbb{Z}[\omega]$, where $\omega = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$. The automorphism group $\mathrm{Aut}(E)$ is cyclic of order 6, generated by the hexic map:

$$[\zeta_6] : (x, y) \mapsto (\zeta_6^2 x, \zeta_6^3 y) = (\omega x, -y). \tag{1.1}$$

In this paper, we generalize the classical division polynomial machinery to track the arithmetic of the $\mathbb{Z}[\omega]$-torsion submodules $E[\alpha]$ for algebraic primes $\alpha \in \mathbb{Z}[\omega]$. We focus on characterizing the unique structural transitions that occur when the standard coordinate collapse $x(P) = x(-P)$ interacts with a six-fold symmetry rather than a four-fold symmetry.

2. Eisenstein Division Polynomials

For an element $\alpha = n + m\omega \in \mathbb{Z}[\omega]$, the multiplication-by-$\alpha$ map $[\alpha]$ cannot be represented as a simple rational function of x alone due to the action of ω rescaling the underlying coordinate plane by non-units.

We construct the composite ideal polynomial $\Psi_\alpha \in \mathbb{Z}[\omega][x]$ associated with the decomposition $[\alpha]P = [n]P + [m]([\omega]P)$.

2.1. The Recurrence Hurdles.

Because $\omega^3 = 1$, the leading terms of the corresponding division ideals do not scale cleanly with the norm $N(\alpha) = n^2 - nm + m^2$ in the same manner as the Gaussian integers. Instead, they form alternating weight classes based on the residue of $\alpha \pmod 3$.

3. Hexic Symmetry and Galois Degree Obstructions

In the case of $y^2 = x^3 + x$, the map $x([i]P) = -x$ directly implied that $\psi_\pi(x)$ was an even polynomial, easily enabling the factorized form $\prod(x^2 - x_j^2)$ and cutting the splitting field degree precisely in half to $\frac{1}{2}(N(\pi) - 1)$.

For $y^2 = x^3 + D$, the action of the automorphism yields:

$$x([\omega]P) = \omega x. \tag{3.1}$$

Consequently, the roots of the Eisenstein division polynomials are closed under multiplication by ω. This structurally implies that $\psi_\alpha(x)$ is a polynomial in x^3, leading to a core factorization of the form:

$$\psi_\alpha(x) = \prod(x^3 - x_j^3). \tag{3.2}$$

3.1. **The Galois Consequences.** Because the coordinate collapse wraps around three roots instead of two, the field extensions generated by the x-coordinates do not collapse by a factor of 2, but rather by a factor of 3 or 6 depending on the ramification behavior of the prime ideal (α) over $\mathbb{Q}(\omega)$. This presents a distinct obstruction to proving direct cyclicity using standard 1-dimensional vector space frameworks.

4. Computational Framework and Conjectural Bounds

Using a custom symbolic array in SymPy, we calculate the explicit forms of Ψ_α for low-norm primes such as $\alpha = 2 + \omega$ $(N(\alpha) = 3)$ and $\alpha = 3 + \omega$ $(N(\alpha) = 7)$. We evaluate the intermediate coefficient divisions to establish structural bounds for an generalized Eisenstein criterion over $\mathbb{Z}[\omega]$.

References

[1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer, 2nd ed., 2009.

[2] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, Chapman & Hall/CRC, 2nd ed., 2008.

Department of Mathematics, University of Utah, Salt Lake City, UT 84112
Email address: tannon.warnick@utah.edu