**2.6.1 The Correspondence between Ideals and Isogenies**

The correspondence between ideals and isogenies provides a bridge between algebra and geometry, specifically within elliptic curves. Elliptic curves are described as “smooth, projective, algebraic curves of genus one, on which there is a specified point O" (Elliptic). These curves aren't just abstract mathematical objects, they have a group structure, meaning you can add points on the curve in a well-defined way, with O acting as the identity element. This structure makes them incredibly versatile, especially in applications like cryptography.

At the heart of this connection is the concept of an endomorphism. An endomorphism is a map of the elliptic curve. It takes points on the curve and maps them back onto the curve, all while preserving the group structure. The set of all such endomorphisms forms a mathematical structure called the endomorphism ring. This ring captures the symmetries and internal structure of the elliptic curve, and in the case of supersingular elliptic curves, it has a deep connection to quaternion algebras, which are special number systems that extend the idea of complex numbers.

Furthermore, there is a one-to-one correspondence between certain algebraic objects, called left ideals in the endomorphism ring, and geometric subgroups of the elliptic curve, which correspond to isogenies. Essentially, every left ideal maps to the kernel of an isogeny, and every isogeny maps back to an ideal. For instance, if you consider the supersingular elliptic curve y^2 = x^3 + x, its endomorphism ring naturally connects to these ideals, creating a seamless relationship between algebra and geometry.

**2.6.2 Converting -Ideals to Isogenies**

Kernels play a crucial role in the conversion of ideals and isogenies. Kernels are used in isogenies as they portray the set of points that show a change. If you know the kernel, you can construct the isogeny. We start with an ideal, and as the ideal acts on the elliptic curve, so let’s say E1 is guided to E2, the kernel is generated as a subgroup of points of E1 that have vanished by the transformation, which are then mapped to the identity point 0 on E2 to preserve the groupstructure**.** This kernel then fully defines the isogeny.

So, looking at the Ideal to Isogeny algorithm, the first input is an ideal I, P prime D and Q prime D which are the transformed points of PD and QD after applying an isogeny. To simplify these steps in the algorithm, think of it as: first, compute the action of the ideal I, then, solve for the kernel generator, which is the starting point that generates the kernel using scalar multiplication; and finally, construct the isogeny using this kernel (SQI Sign). The kernel plays a big role because it is the central component that connects the ideal to the isogeny. In essence, this process provides a computationally practical method for bridging the gap between ideals and isogenies, which is crucial for protocols in post-quantum cryptography.

Additionally, constructing matrices from the ideal and determining its kernel, which gives the generator of the associated isogeny, is an important concept called the “push-through isogeny”. This takes a basis of E[D] and maps it to the image under a separable isogeny. The construction of this isogeny is efficient, as it simply reuses the coefficients calculated during the translation of the ideal. The Ideal to Isogeny algorithm uses this and simplifies this step further by directly generating the separable isogeny from its kernel.

**2.6.3 Converting**  **-Ideals of large**

The process of converting -ideals with large prime power norms to isogenies plays a critical role in the key generation and signing procedures of cryptographic systems like SQI Sign because it establishes the mathematical foundation for secure and efficient operations. This process is handled by the Ideal to Isogeny Eichler**​** algorithm, which transforms an ideal into its corresponding isogeny. The procedure is divided into two main phases: one focused on quaternion operations and the other on elliptic curve operations.

In the first phase, quaternion calculations are used to reduce a sequence of ideals while calculating their norms and key isogeny parameters. This process leverages the algebraic properties of quaternions, which are described as "a four-dimensional associative normed division algebra over the real numbers" (Quaternion). Using the Ideal Step algorithm, the ideals are refined step by step, ensuring all necessary values are ready for the next stage. In the second phase, these simplified ideals are transformed into isogenies by using torsion bases and building separable isogenies. This phase relies on the groundwork laid by the quaternion calculations to ensure the process is both accurate and efficient.

The process also incorporates techniques like compression and endomorphism evaluation. Compression and Endomorphism evaluation plays a crucial role in ensuring efficient and practical use. First, let's talk about compression, so Compression is all about reducing the size of the isogeny output. Isogenies often requires a lot of data to represent. By compressing this information, we save memory and bandwidth, making it more efficient. For endomorphism evaluation, this step focuses on efficiently computing the action of an isogeny. These optimizations are critical for making the algorithm practical in post-quantum cryptography.

Ultimately, this process bridges the gap between quaternion-based ideal arithmetic and elliptic curve-based isogeny construction. It provides a scalable method for handling large prime power norms, which is essential for secure and efficient cryptographic applications.

**2.6.4 Converting Isogenies to Ideals**

Converting isogenies into their corresponding ​-ideals is a simpler process compared to the reverse. The goal is to find the ideal associated with an isogeny generated by a point P of order D. This involves a technique called decomposition, which plays a crucial role in translating an isogeny back into its ideal efficiently. Decomposition is particularly valuable in SQISign because it avoids computationally expensive operations, making the process both secure and practical. The reason for translating an isogeny into an ideal is that ideals offer a more algebraic and structured representation, making them easier to store, manipulate, and verify in cryptographic systems.

**Bibliography**

“Elliptic Curve.” *Wikipedia*, Wikimedia Foundation, 12 Nov. 2024, en.wikipedia.org/wiki/Elliptic\_curve.

Jorge Chavez-Saab, Maria Corte-Real Santos, Luca DeFeo, Jonathan Komada Eriksen, Basil Hess, David Kohel, Antonin Leroux, Patrick Longa, Michael Meyer, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Francisco Rodríguez Henríquez, Sina Schaeffler, and Benjamin Wesolowski. SQISIGN (June 2023)

“Quaternion.” *Wikipedia*, Wikimedia Foundation, 27 Oct. 2024, en.wikipedia.org/wiki/Quaternion.