SHIMURA RECIPROCITY - FOLLOWING SERRE IN CASSELS/FROHLICH

ANDREW FIORI

1. The Problem - Explicit Class Field Theory

One is interested in the general problem of explicitly giving generators for the maximal abelian extension of a number field.

For $\mathbb{Q}$ these are given by the coordinates of the solutions of $Z(x^n - y^n) \in \mathbb{P}^1$. Or equivalently the points of finite order in $\mathbb{G}_m$.

We wish to do the same thing for K which is quadratic imaginary.

2. The results

Let E be an elliptic curve over $\mathbb{C}$. There are two options for the endomorphism ring of E.

$$\mathrm{End}_{\mathbb{C}}(E) = \begin{cases} \mathbb{Z} & \text{normally} \\ R_f = \mathbb{Z} \oplus f\mathcal{O}_K & K \text{ is a CM-field} \end{cases}$$

In the second case we call f the conductor of E.

Theorem 2.1. *The elliptic curves with endomorphism ring R_f are in bijective correspondance (up to isomorphism) with the class group $CL(R_f)$.*

Proof. Recall that for an order R_f the ideals (rank one modules) form a monoid with the invertible elements corresponding to the projective (locally free or equiv locally principal) ideals. The class group $CL(R_f)$ (resp Pic^0) is then precisely the invertible ideals (resp ideals) modulo principal ideals (modules isomorphic to R_f).

Now, such a curve E is isomorphic to $\mathbb{C}/\Lambda$. The endomorphisms of E lift to $\mathbb{C}$ and map Λ to Λ. We thus have that Λ is a rank one R_f module. (Somehow i think that all such maps factor is equivalent to the projective module assumption)

Conversely, it is clear that if we take the natural inclusion of R_f into $\mathbb{C}$ any ideal will be a lattice and that $\mathbb{C}/I$ is an analytic variety where R_f acts by endomorphism.

It is clear by the homethety equivalance of rescaled lattices we must take these conditions up to principal ideals. It is slightly less 'clear' that any isomorphism of such lattices must take the form of multiplication by a principal ideal, but this is indeed true of ideals in these rings.

□

Theorem 2.2 (Weber-Feuter)**.** *Suppose the conductor $f = 1$, Let $K = (\mathbb{Q} \otimes R_f)$, then $K(j(E))$ is the absolute class field of K. Moreover $\mathrm{Gal}(K(j(E))/K)$ acts transitively on $j(E)$.*

Theorem 2.3 (Hasse)**.** *Let $\mathfrak{p}$ be a good prime of K with $(\mathfrak{p}, f) = (1)$; let $\mathfrak{p}_f = \mathfrak{p} \cap R_f$ be the corresponding ideal of R_f. Let $\Gamma \in CL(K)$. The the Frobenius element $F(\mathfrak{p})$ acts on $j(\Gamma)$ by:*

$$F(\mathfrak{p})(j(\Gamma)) = j(\Gamma \cdot \mathfrak{p}_f^{-1})$$

Remark. Good prime I can only assume means something about the reduction of E...

Sketch. (1) $j(E)$ is algebraic.

If not there would be infinitely many curves with complex multiplication by R_f.

(2) For a rank 1 module P over R_f define:

$$P * E = \mathrm{Hom}(P, E)$$

Let $R_f^m \xrightarrow{\phi} R_f^n \to P$ be a resolution of P Noting that $\mathrm{Hom}(R_f, E) = E$ we have $\mathrm{Hom}(P, E) = \mathrm{Ker}(\phi^t : E^n \to E^m)$. We see that this gives a way for the class group to act algebraicly on the elliptic curves with endomorphisms by R_f.

$\mathrm{Gal}(\overline{K}/K)$ acts on this set of elliptic curves and preserves the structure of the class group orbits.

(3) The action of the galois group thus must correspond to translations by the rank one modules.
(4) It follows that we have a map from the galois group to the class group.
(5) We assert that good primes act like frobenious.
(6) if $N(p) = p$ then we have a degree p isogeny from E to $p * E$ after reduction mod p. Thus the map is inseperable. Thus the map is the map $x \mapsto x^p$.
(7) if $N(p) = p^2$ then p is innert in $K/\mathbb{Q}$ then "one can show" that E has no point of order p after reduction mod p, the map thus has trivial kernel and is thus an inseperable isogeny. and so it is $x \mapsto x^{2p}$ which is again frobenious.

□