KOLYVAGIN SEMINAR: COMPLEX MULTIPLICATION

KIRAN KEDLAYA

Class field theory classifies the abelian extensions of a number field in terms of certain quotients of the group of ideals of the ring of integers. Over $\mathbb{Q}$, the situation becomes much more explicit: by Kronecker-Weber, the maximal abelian extension is generated by roots of unity. In these talks, we will see how over imaginary quadratic fields, elliptic curves with complex multiplication permit a similar description of abelian extension.

References: for class field theory, Lang's *Algebraic Number Theory* exists but is unpleasant; Cassels and Fröhlich, *Algebraic Number Theory* is dense but more readable; and Milne's notes (at `www.jmilne.org`) are better yet. For elliptic curves, Silverman's *Arithmetic of Elliptic Curves* and *Advanced Topics in the Arithmetic of Elliptic Curves* are the standard references (complex multiplication is covered in Chapter II of AEC2).

1. Review of Class Field Theory

In this talk, by a *conductor* for a field K we shall mean a pair $(\mathfrak{m}, S)$, where $\mathfrak{m}$ is an ideal in $\mathfrak{o}_K$ and S is a set of real embeddings of K. Let $I_{K,\mathfrak{m}}$ denote the group of ideals in $\mathfrak{o}_K$ coprime to $\mathfrak{m}$, and $P_{K,\mathfrak{m},S}$ the subgroup generated by ideals which are principal, and admit a generator congruent to 1 modulo $\mathfrak{m}$ and positive in all embeddings in S. (Warning: these collections are monoids, not groups. When I refer to such a thing as a "group", I really mean the quotient group of the monoid. Equivalently, work with fractional ideals instead of ideals and then the monoid itself is already a group.)

For L/K abelian and $\mathfrak{p}$ a prime of K which does not ramify in L, there is an element $\sigma \in \mathrm{Gal}(L/K)$ such that $x^\sigma \equiv x^{N\mathfrak{p}} \pmod{\mathfrak{q}}$ for all primes $\mathfrak{q}$ over $\mathfrak{p}$. We call σ the *Frobenius at* $\mathfrak{p}$. In the obvious way (multiplicativity), the assignment of $\mathfrak{p}$ to σ extends to a map from the group of ideals not divisible by any ramified primes to $\mathrm{Gal}(L/K)$. This map is called the *Artin map*.

Theorem 1 (Artin reciprocity law)**.** *If L/K is abelian, there exists a conductor $(\mathfrak{m}, S)$ such that $P_{K,\mathfrak{m},S}$ is in the kernel of the Artin map.*

The "minimal" such pair is called the *conductor of* L/K. One can also describe the kernel of the Artin map more precisely: it is generated by $P_{K,\mathfrak{m},S}$ with $(\mathfrak{m}, S)$ equal to the conductor, plus norms of ideals of L.

Theorem 2 (Existence theorem)**.** *If P is a subgroup of $I_{K,\mathfrak{m}}$ containing $P_{K,\mathfrak{m},S}$ for some $\mathfrak{m}$ and S, then there exists an abelian extension L over K, ramified only over the primes in $\mathfrak{m}$, the kernel of whose Artin map (restricted to $I_{K,\mathfrak{m}}$) is precisely P.*

In particular, if P is the group of principal ideals, the corresponding extension is the maximal abelian unramified extension of K, also known as the *Hilbert class field* of K. More generally, if $\mathfrak{o}$ is an order of K (a subring of K which is a $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$) and P is the group of ideals which restrict to principal ideals in $\mathfrak{o}$, the corresponding extension is called the *ring class field* of $\mathfrak{o}$. In particular, the Hilbert class field is the ring class field of the maximal order; in general, the ring class field of an order of conductor N is intermediate between the Hilbert class field and the ray class field of conductor N.

2. Intermezzo: Orders in Imaginary Quadratic Fields

Before proceeding, a few words of explanation about orders. Because orders are not Dedekind domains (failing to be integrally closed) in general, they do not have unique factorization of ideals, nor of elements

Date: Version of February 16, 2000.

even when the class group is trivial. Of course, if you invert the conductor, the result becomes a Dedekind domain (since you get the same ring as if you had inverted the conductor in the maximal order), so unique factorization holds for ideals prime to the conductor.

The orders of an imaginary quadratic field K are easy to classify.

Theorem 3. *If $\mathfrak{o}$ is an order in the imaginary quadratic field K, then there exists $N \in \mathbb{N}$ such that $\mathfrak{o} = \mathbb{Z} + N\mathfrak{o}_K$.*

Proof is left as an exercise.

Likewise, the class group $\mathrm{Pic}(\mathfrak{o})$ of an order is easily related to the class group of the maximal order. This formula will come up in Gross' paper.

Theorem 4. *If $\mathfrak{o} = \mathbb{Z} + N\mathfrak{o}_K$, then the quotient $\mathrm{Pic}(\mathfrak{o})/\mathrm{Pic}(\mathfrak{o}_K)$ is isomorphic to $(\mathfrak{o}_K/N\mathfrak{o}_K)^*/[(\mathbb{Z}/N\mathbb{Z})^*\mathfrak{o}_K^*]$.*

Of course, if K is not $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$, the term $\mathfrak{o}_K^*$ is redundant.

Proof. The quotient may be identified with the quotient of the group of ideals which are principal in $\mathfrak{o}_K$ by the group of those which remain principal in $\mathfrak{o}$. Now if α is the generator of a given principal ideal, then α lies in $\mathfrak{o}$ if and only if it is congruent modulo N to an element of $\mathbb{Z}$. □

3. Elliptic Curves with Complex Multiplication

Now let us proceed to elliptic curves with complex multiplication and their relevance to ring class fields. Recall that the ring of endomorphisms of an elliptic curve over a field of characteristic 0 is either $\mathbb{Z}$ or an order in an imaginary quadratic field. (Over $\mathbb{C}$, the elliptic curve can be written as $\mathbb{C}$ modulo the lattice $\langle 1, \tau \rangle$, and an endomorphism must act as multiplication by a complex number α on $\mathbb{C}$ so as to map the lattice into itself. Thus $\alpha = a + b\tau$ and $\alpha\tau = c + d\tau$, whence α and τ are quadratic over $\mathbb{Q}$; for τ to generate a lattice with 1, $\mathbb{Q}(\tau)$ must be imaginary quadratic.) If the latter holds, we say the elliptic curve has *complex multiplication*, or *CM* for short, by that order.

Beware that there are two ways to identify $\mathfrak{o}$, as an abstract ring, with the corresponding ring of endomorphisms of an elliptic curve with CM by $\mathfrak{o}$. We choose the one with the property that $\alpha \in \mathfrak{o}$ acts on the tangent space to the elliptic curve at the origin by multiplication by α (and not by $\overline{\alpha}$).

The reader is probably familiar with the notation $E[n]$ used to denote the group of n-torsion points on an elliptic curve E. If E has CM by $\mathfrak{o}$, this notation can be extended: if α is an element of $\mathfrak{o}$, we denote by $E[\alpha]$ the kernel of multiplication by α. Furthermore, if $\mathfrak{m}$ is an ideal of E, we denote by $E[\mathfrak{m}]$ the intersection of $E[\alpha]$ over all $\alpha \in \mathfrak{m}$. It can be shown that $E[\mathfrak{m}]$ is a finite flat group scheme of order $\mathbf{N}\mathfrak{m}$ and that $E/E[\mathfrak{m}]$ is again an elliptic curve. Moreover, if $\mathfrak{m}$ is prime to the conductor of $\mathfrak{o}$, then E again has CM by $\mathfrak{o}$ (otherwise, E may have CM by a different order).

To reiterate the previous paragraph in terms of lattices: if $E \cong \mathbb{C}/\Lambda$, then $E[\mathfrak{m}] \cong \mathfrak{m}^{-1}\Lambda/\Lambda$ and $E/E[\mathfrak{m}] \cong \mathbb{C}/\mathfrak{m}^{-1}\Lambda$ (where $\mathfrak{m}^{-1}\Lambda$ is the set of $x \in \mathbb{C}$ such that $x\mathfrak{m} \subseteq \Lambda$), and the isogeny $E \to E/E[\mathfrak{m}]$ is simply the map $\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{m}^{-1}\Lambda$ induced by the identity map on $\mathbb{C}$.

Fixing an order $\mathfrak{o}$, we see that the lattices stabilized by multiplication by $\mathfrak{o}$ are, up to homothety, representatives of the ideal classes of $\mathfrak{o}$. In particular, there are finitely many of them, and any two are isogenous. Moreover, the $j(E)$ all generate the same field over K, since one can find an elliptic curve with j-invariant $j(E)$ defined over $K(j(E))$, and then this curve is isogenous over this same field to curves with all of the other possible j-invariants.

Theorem 5. *Let E be an elliptic curve over a field of characteristic 0 having complex multiplication. Then $j(E)$ is an algebraic number.*

Proof. Let $\mathfrak{o} = \mathrm{Gal}(E)$. Any automorphism of $\mathbb{C}$ over $\mathbb{Q}$ carries E to another elliptic curve with CM by $\mathfrak{o}$, and the number of possible j-invariants of these is finite. □

In other words, all of the isomorphism classes over $\mathbb{C}$ of elliptic curves with complex multiplication by a given order $\mathfrak{o} \subseteq K$ are represented by curves defined over number fields. When we say such a curve is defined over a number field L, we insist that L contain K; this is enough to force $\mathfrak{o}$ to act by endomorphisms defined over

L. (Proof: each endomorphism is determined by its action on the tangent space at the origin; since these actions are multiplications by elements of K, they are invariant under $\mathrm{Gal}(\overline{L}/L)$.)

4. CM and Class Field Theory

Our goal is to prove the following.

Theorem 6. *Let K be an imaginary quadratic field, $\mathfrak{o}$ an order of K and E an elliptic curve with complex multiplication by $\mathfrak{o}$. Then $M = K(j(E))$ is the ring class field of $\mathfrak{o}$. More precisely, there exists an isomorphism $\pi : \mathrm{Pic}(\mathfrak{o}) \to \mathrm{Gal}(M/K)$ such that*

$$j(E)^{\pi(\mathfrak{p})} = j(E/E[\mathfrak{p}]) \tag{1}$$

for all primes $\mathfrak{p}$ not dividing the conductor of $\mathfrak{o}$, and the Artin map factors through π (that is, $\pi(\mathfrak{p})$ is the Artin symbol of $\mathfrak{p}$).

Our approach is to reduce elliptic curves modulo primes and use facts about separability of isogenies in positive characteristic.

First we show that M contains the other j-invariants of curves with CM by $\mathfrak{o}$. To see this, choose E to be defined over M; then for each ideal class of $\mathfrak{o}$, choose a representative $\mathfrak{m}$ prime to the conductor N of $\mathfrak{o}$, and note that $E/E[\mathfrak{m}]$ is defined over M, as then is its j-invariant.

We hereby declare the following primes of $\mathfrak{o}$ to be "bad":

- all primes lying under primes of bad reduction for E;
- all primes dividing primes of $\mathbb{Q}$ which ramify in M (so in particular, all primes dividing the difference between any two of the CM j-invariants);
- all primes dividing the conductor of $\mathfrak{o}$.

We begin by proving (1) for the remaining primes, beginning with the following congruence.

Theorem 7. *Let K be an imaginary quadratic field, $\mathfrak{o}$ an order of K, and E an elliptic curve defined over a number field L containing K with complex multiplication by $\mathfrak{o}$. Then for every prime $\mathfrak{p}$ of $\mathfrak{o}$ which is not bad and every prime $\mathfrak{q}$ of L over $\mathfrak{p}$,*

$$j(E)^{\mathrm{N}\mathfrak{p}} \equiv j(E/E[\mathfrak{p}]) \pmod{\mathfrak{q}}.$$

Proof. First suppose $\mathfrak{p}$ has absolute degree 1 and let $p = N\mathfrak{p}$. Choose an ideal $\mathfrak{r}$ prime to the conductor N of $\mathfrak{o}$ and to $\mathfrak{p}$, and lying in the ideal class of $\overline{\mathfrak{p}}$. Then $\mathfrak{p}\mathfrak{r}$ is principal; let α be a generator. Now consider the isogenies

$$E \to E' = E/[\mathfrak{p}] \to E'/E'[\mathfrak{r}] = E/E[\mathfrak{p}\mathfrak{r}] = E/E[\alpha] = E.$$

The composite map from E to E is precisely multiplication by α, which on the residue field is inseparable (since $\alpha \in \mathfrak{p}$). On the other hand, the second isogeny has degree $N\mathfrak{r}$ prime to the residue characteristic, and so is separable. Therefore the isogeny the isogeny $E \to E/E[\mathfrak{p}]$ must be inseparable. In particular, it factors through the Frobenius isogeny $E \mapsto E^{\mathrm{N}\mathfrak{p}}$ and the other factor has degree 1, so is an isomorphism.

Now suppose $\mathfrak{p}$ has absolute degree 2 and let $\mathfrak{p} = (p)$. Then our goal is to show that $j(E)^{p^2} \equiv j(E)$. We have that multiplication by p on E factors as the Frobenius isogeny F followed by its dual $\hat{F}$, and the former is inseparable. We shall show that the latter is also inseparable.

Let τ be the Frobenius of $\mathfrak{q}$ over $\mathbb{Q}$, so that $j(E)^\tau \equiv E^p \pmod{p}$. Now $j(E)^\tau$ is one of the CM j-invariants, so there exists an ideal $\mathfrak{r}$ such that $j(E^\tau/E^\tau[\mathfrak{r}]) = j(E)$. Now consider the isogenies

$$E \to E' = E^\tau \to E'/E[\mathfrak{r}] = E.$$

The composite map from E to E is multiplication by some $\alpha \in \mathfrak{o}$, which must lie in $\mathfrak{p}$ since on the residue field the map is inseparable. (Its first factor is precisely the Frobenius isogeny.) The dual isogeny to multiplication by α is multiplication by $\overline{\alpha}$, which is also inseparable because $\overline{\alpha} \in \mathfrak{p}$. On the other hand, the dual of a composite is the composite of the duals in the opposite order, and the dual of $E^\tau \to E'/[\mathfrak{r}]$ ∎

From this let us deduce our main theorem. First, note that for $\mathfrak{q}$ above a good prime, the Frobenius σ of $\mathfrak{q}$ satisfies $j(E)^\sigma = j(E/E[\mathfrak{p}])$. (We know that the left side is one of the CM j-invariants, that the two sides are congruent modulo $\mathfrak{q}$, and that no two distinct CM j-invariants are congruent modulo $\mathfrak{q}$.) In particular, σ does not depend on $\mathfrak{q}$; therefore M/K is abelian. Now define π on an ideal class by choosing a prime $\mathfrak{p}$ in that class and mapping the class to the Artin symbol σ of that prime. From the equality $j(E)^\sigma = j(E/E[\mathfrak{p}])$, we know σ depends only on the isomorphism class of $E/E[\mathfrak{p}]$, which is to say on the class of $\mathfrak{p}$, and not on $\mathfrak{p}$ itself.

We see that π is surjective by Čebotarev (every element of Galois occurs as an Artin symbol). Moreover, it is injective because if the classes of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ both map to σ, then $E/E[\mathfrak{p}_1]$ and $E/E[\mathfrak{p}_2]$ have the same j-invariant, which implies that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are in the same class. Thus π is an isomorphism and the Artin map factors through it.

In particular, up to a finite number, the same primes of K are split completely in M and the ring class field of $\mathfrak{o}$. (A prime coprime to N is split in the ring class field if and only if it is in the principal ideal class.) Thus (by applying Čebotarev to the compositum of these two extensions) these extensions must be the same, as desired. (Note that the previous assertion uses the fact that both extensions are known at this point to be abelian.)

Since we were explicitly able to describe the Artin map on $j(E)$, all we really have used class field theory for is to control the ramification of the ring class field. It should be noted that this can also be done directly.

Theorem 8. *Let K be an imaginary quadratic field, $\mathfrak{o}$ an order of K, and E an elliptic curve defined over a number field L containing K with complex multiplication by $\mathfrak{o}$. Then E has potentially good reduction everywhere. (In particular, its j-invariant is integral.)*

This result is due to Serre and Tate. (See AEC2 for a proof sketch.) It implies that the field generated by the $j(E)$ is unramified away from the conductor of $\mathfrak{o}$.

We won't need to do so here, but one can go further and describe all of the abelian extensions of K. In fact, any finite abelian extension of K is contained in the field obtained by adjoining the j-invariant of a curve with CM in the maximal order of K, together with the coordinates of a torsion point on the curve. (That extension is actually not abelian, but if one instead takes the coordinates of the image of the torsion point after quotienting the curve by its automorphism group, one gets a smaller extension which is in fact abelian.)