TATE'S ISOGENY THEOREM

GAL PORAT

As a preparation for proving the Honda-Tate theorem, in this lecture we will prove a nice theorem due to Tate. Due to time constraints we will prove it only in the case $Hom_k(E_1, E_2) \neq 0$.

Tate's Isogeny Theorem

Let k is a finite field, $G = Gal(\overline{k}/k)$ its absolute Galois group, and $l \neq char(k)$ is any prime.

Theorem (Tate's Isogeny Theorem). *For all elliptic curves E_1, E_2 defined over k the map*

$$\eta : Hom_k(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to Hom_G(T_l(E_1), T_l(E_2))$$

is an isomorphism.

Remark. This is not true for arbitrary fields, for example for local fields. However the theorem does hold for number fields.

Due to time constraints we will prove it only in the case $Hom_k(E_1, E_2) \neq 0$.

For the next proposition, we will need a lemma.

Lemma. *Let $M \subset Hom_k(E_1, E_2)$ be a finitely generated subgroup. Put $M^{div} = \{\phi \in Hom_k(E_1, E_2) : [m] \circ \phi$ for some integer $m \geq 1\}$, i.e. this is the subgroup of $Hom_k(E_1, E_2)$ corresponding to the torsion subgroup of $Hom_k(E_1, E_2)/M$. Then M^{div} is finitely generated and free.*

Proof. There is a natural map $M^{div} \to M \otimes \mathbb{R}$ defined by $\phi \mapsto [m] \circ \phi \otimes \frac{1}{m}$ where m is any integer such that $[m] \circ \phi \in M$. Since $Hom_k(E_1, E_2)$ is torsion-free, so is M, so M is free since it is finitely generated. Hence $M \to M \otimes \mathbb{R}$, $\phi \mapsto \phi \otimes 1$ is an injection (this is like $\mathbb{Z}^n \to \mathbb{R}^n$). This means that for $\phi \in M^{div}$, each $\phi \otimes 1 \neq 0$, hence $M^{div} \to M \otimes \mathbb{R}$ is also an injection. On the other hand, we claim the image of M^{div} is also a discrete subgroup of $M \otimes \mathbb{R}$. Indeed, continue deg linearly as a quadratic form to $M \otimes \mathbb{R}$, and put $U = \{\sum_i \phi_i \otimes \alpha_i \in M \otimes \mathbb{R} : deg\phi < 1\}$. Then U is open and $M^{div} \cap U = 0$. Since M^{div} is a discrete subgroup of a

finite dimensional real vector space it follows that it is finitely generated. It is clear that it is also free since it is a subgroup of the torsion free subgroup $Hom_k(E_1, E_2)$.

□

We can now prove the first part of Tate's Isogeny theorem. This part is true for any field, not just for finite fields.

Proposition. *The map* $\eta : Hom_k(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to Hom_G(T_l(E_1), T_l(E_2))$ *is injective and has torsion free cokernel.*

Proof. (Recall that $Hom_G(T_l(E_1), T_l(E_2))$ is a $\mathbb{Z}_l$-module defined by $(x\psi)(y) := x\psi(y)$, i.e. this is the $\mathbb{Z}_l$-module structure inherited from the $\mathbb{Z}_l$-module structure of every Tate module. This explains how the map in the proof is defined).

Let $\phi \in Hom_k(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l$, $\phi_l = \eta(\phi)$. We shall prove first the following:

(*): if ϕ_l is divisible by l, then so is ϕ.

Write $\phi \in M \otimes_{\mathbb{Z}} \mathbb{Z}_l$ where M is a finitely generated subgroup of $Hom_k(E_1, E_2)$. Let $\psi_1, ..., \psi_t$ be a free basis for M^{div}, which we know exists by the previous lemma. We can therefore write $\phi = \sum_i \psi_i \otimes \alpha_i$ where $\alpha_i \in \mathbb{Z}_l$. Now let $a_1, ..., a_t \in \mathbb{Z}$ be such that $a_i \equiv \alpha_\mathrm{i}$, and put $\phi' = \sum_i a_i\psi_i = \sum_i [a_i] \circ \psi_i \in Hom_k(E_1, E_2)$. In particular, $\phi' \in M^{div}$ since each $\psi_i \in M^{div}$. Now since ϕ_l is divisible by l, it killes all of $E_1[l]$. This also happens mod l, so ϕ' also kills all of $E_1[l]$. This is just another way of saying that $ker[l] \subset ker\phi'$.

In general, we have seen that if we have maps $f : E_1 \to E_2$ and $g : E_1 \to E_3$ with $kerf \subset kerg$ with f separable, there is a unique isogeny solution $\lambda : E_2 \to E_3$ such that $\lambda \circ g = f$. In this case we can take $[l]$ as the separable map and our ϕ' as the second map to obtain a map $\lambda : E_1 \to E_2$ such that $[l] \circ \lambda = \lambda \circ [l] = \phi'$ (we can't apply this argument to ϕ since it isn't an element of $Hom_k(E_1, E_2)$, so this is why we needed to define ϕ'). Since $\phi' \in M^{div}$ it follows that $\lambda \in M^{div}$, and we can write $\lambda = \sum_i b_i\psi_i$, which gives $a_i = lb_i$, so $a_i \equiv 0(l)$. Hence each α_i is divisible by l, so indeed ϕ is divisible by l, and **(*)** is proved.

Why does this give us what we need? First let use show that η is injective. Suppose that $\phi_l = 0$. Thenϕ_l is infinitely l divisible; by **(*)**, so is ϕ. But this implies that $\phi = 0$ since $Hom_k(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ is a free $\mathbb{Z}_l$-module. Now we show the cokernel is torsion free. $Hom_G(T_l(E_1), T_l(E_2))$ is a finitely-generated $\mathbb{Z}_l$-module, hence so is the cokernel. The cokernel then has trivial torsion if and only if it has trivial l torsion, and the latter is equivalent to **(*).**

□

Now put $V_l(E) = T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. The map η from before induces a map

$$Hom_k(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Q}_l \xrightarrow{\eta'} Hom_G(V_l(E_1), V_l(E_2))$$

Lemma. *If η' is an isomorphism, Tate's Isogeny Theorem holds.*

Proof. Indeed, by the previous proposition we have the following exact sequence:

$$0 \to Hom_k(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \xrightarrow{\eta} Hom_G(T_l(E_1), T_l(E_2)) \to coker\eta \to 0$$

Since $\mathbb{Q}_l$ is a flat $\mathbb{Z}_l$ module, we see after tensoring $\mathbb{Q}_l$ with the exact sequence above that η' is an isomorphism if and only if $coker\eta \otimes \mathbb{Q}_l = 0$ and η is an isomorphism if and only if $coker\eta = 0$. Since this is a torsion free $\mathbb{Z}_l$ module, both are equivalent.

□

For the following proof, recall some facts from noncommutative algebra:

1. Any division ring is simple as a ring, and its center is a field. Therefore it is a central simple algebra over its center.

2. (Centralizer Theorem) for a central simple algebra S with finite dimension over its center k, and R any simple subalgebra, one has $[S : k] = [R : k][C(R) : k]$, where $C(R)$ is the centralizer of R.

We will now prove Tate's Isogeny Theorem under the hypothesis that $Hom_k(E_1, E_2) \neq 0$.

Proof. Let $\psi : E_1 \to E_2$ be any isogeny. We can define a map $End_k(E_1) \otimes \mathbb{Q}_l \to Hom_k(E_1, E_2) \otimes \mathbb{Q}_l$ by extending the map $\phi \mapsto \psi \circ \phi$. We can define a map in the reverse direction by $\phi \mapsto \hat{\psi} \circ \phi$. Since the composition in both directions is $[deg\psi]\phi$, this is clearly an isomorphism of $\mathbb{Q}_l$ vectors spaces. A similar analysis can be done for the pair $Hom_G(V_l(E_1), V_l(E_2))$ and $End_G(V_l(E_1))$. Therefore $dim_{\mathbb{Q}_l}(Hom_k(E_1, E_2) \otimes \mathbb{Q}_l) = dim_{\mathbb{Q}_l}(End_k(E_1) \otimes \mathbb{Q}_l)$, and similarly for the Tate modules. Rewriting $E = E_1$, it is enough to prove

$$dim_{\mathbb{Q}_l}(End_k(E) \otimes \mathbb{Q}_l) \geq dim_{\mathbb{Q}_l}(End_G(V_l(E)))$$

Now let π be the Frobenius endomorphism of E. Put $F = \mathbb{Q}(\pi)$, $D = End_k(E) \otimes \mathbb{Q}$ (we know that D is a division ring). Notice that F is contained in the center of D, since π commutes with every element. Also recall that π satisfies a quadratic equation over $\mathbb{Z}$ and so $[F : \mathbb{Q}] \leq 2$.

First case: $[F : \mathbb{Q}] = 2$. Extension of scalars doesn't change dimension, so $[F \otimes \mathbb{Q}_l : \mathbb{Q}_l] = 2$, and this implies that $\pi_l \notin \mathbb{Q}_l$. Moreover, since $F \subset D$, it follows that $dim_{\mathbb{Q}_l} D \otimes \mathbb{Q}_l \geq 2$. On the other hand, since π_l generates $Gal(\overline{k}/k)$ topologically, elements that commute with π_l are precisely those that commute with $Gal(\overline{k}/k) \simeq \hat{\mathbb{Z}}$. Hence the $C(\mathbb{Q}(\pi_l)) = End_G(V_l(E))$ in the simple algebra $End(V_l(E))$. We also have $End(V_l(E)) \simeq M_2(\mathbb{Q}_l)$ so its dimension over $\mathbb{Q}_l$ is 4. By the Centralizer Theorem, we must have $dim_{\mathbb{Q}_l}(End_G(V_l(E))) = 2$ since

$[\mathbb{Q}_l(\pi_l) : \mathbb{Q}_l] = 2$. So in this case, $dim_{\mathbb{Q}_l}(End_k(E) \otimes \mathbb{Q}_l) = dim_{\mathbb{Q}_l} D \otimes \mathbb{Q}_l \geq 2$, $dim_{\mathbb{Q}_l}(End_G(V_l(E))) = 2$ and the inequality holds.

Second case: $[F : \mathbb{Q}] = 1$, so $\pi \in \mathbb{Q}$. In this case E is supersingular, because $\hat{\pi} = \pi$ is purely inseparable. Also, every element of G commutes with π since π is rational. Then $End_k(E) = End_{\overline{k}}(E)$ which is a quaternion algebra of order 4. Then $dim_{\mathbb{Q}_l}(End_k(E) \otimes \mathbb{Q}_l) = 4 = dim_{\mathbb{Q}_l}(End(V_l(E))) \geq dim_{\mathbb{Q}_l}(End_G(V_l(E)))$.

□