COMPLEX MULTIPLICATION: LECTURE 14

Proposition 0.1. *Let K be any field.*

i) Two elliptic curves over $\overline{K}$ are isomorphic if and only if they have the same j-invariant.

ii) For any $j_0 \in \overline{K}$, there exists an elliptic curve with j-invariant j_0.

Proof. i) We prove this when $\mathrm{char} K \neq 2, 3$. The transformation relations show that any two isomorphic elliptic curves have the same j invariant. Conversely uppose E and E' have Weierstrass equations:

$$y^2 = x^3 + Ax + B$$

$$y'^2 = x'^3 + A'x' + B'$$

and they have the same j-invariants. Thus

$$\frac{4A^3}{4A^3 - 27B^2} = \frac{4A'^3}{4A'^3 - 27B'^2}$$

which yields

$$A^3 B'^2 = A'^3 B^2$$

We look for a relation

$$(x, y) = (u^2 x', u^3 y')$$

We divide this up into three cases.

Case 1: $A = 0 (j = 0)$. Then $B \neq 0$ since $\Delta \neq 0$, and we may take $u = (B/B')^{1/6}$.

Case 2: $B = 0 (j = 1728)$. For the same reason as before we have $A \neq 0$ and we may take $u = (A/A')^{1/4}$.

Case 3: $AB \neq 0$, then $A'B' \neq 0$ since $\Delta' \neq 0$, hence we may take $u = (A/A')^{1/4} = (B/B')^{1/6}$.

ii) First assume $j_0 \neq 0, 1728$, the equation

$$y^2 + xy == x^3 - \frac{36}{j_0 - 1728} x - \frac{1}{j_0 - 1728}$$

has $\Delta = \frac{j_0^2}{j_0 - 1728}^3 \neq 0$ and $j = j_0$. Thus this equation defines a non-singular curve over K, hence an elliptic curve with the correct j-invariant.

For the remaining cases we take:

$$j_0 = 0, y^2 + y = x^3, \ \Delta = -27, \ j = 0$$

$$j_0 = 1728, y^2 = x^3 + x, \ \Delta = -64, \ j = 1728$$

Note that when $\mathrm{char} K = 2$ or 3, these are the only divisors of 1728, so $j = 0$ for the above two curves and we note that at least one must have $\Delta \neq 0$.

□

Corollary 0.2. *Let E be an elliptic curve with $j_0 \in K$, then E is defined over K, i.e. there exists a Weierstrass equation for E with coefficients in K.*

Let L/K be an extension of fields and $\sigma \in \mathrm{Aut}(L/K)$. For E an elliptic curve over L, we define E^σ to be the elliptic curve obtained by applying σ to the coefficients of a Weierstrass equation for E. (This is a more general version of the construction of the Frobenius twist). One checks that this is independent of the Weierstrass equation defining E. Since $j(E)$ is a rational function of the coefficients of a Weierstrass equation for E, we have $j(E^\sigma) = \sigma(j(E))$.

We finish this section by stating the link with our complex analytic constructions from two weeks ago. We saw that given $\tau \in \mathfrak{h}$, the points of the complex torus can be identified with the the points of projectivisation of the curve $y^2 = x^3 - g_2(\tau)x - g_3(\tau)$ which we will denote by E_τ. Given what we now know, we can prove the following.

Theorem 0.3. *(Complex Uniformisation of Elliptic curves) The association*

$$\mathbb{C}/\Lambda_\tau \mapsto E_\tau$$

induces a bijection between the ismorphism classes of complex tori and isomorphism classes of elliptic curves over $\mathbb{C}$.

Proof. First note that any complex torus is isomorphic to $\mathbb{C}/\Lambda_\tau$ for some $\tau \in \mathfrak{h}$. The elliptic curve E_τ has j-invariant given by $j(\tau)$, since $\mathbb{C}/\Lambda_{\tau_1}$ and $\mathbb{C}/\Lambda_{\tau_2}$ are isomorphic if and only if τ_1 and τ_2 are conjugate by $\Gamma = SL_2(\mathbb{Z})$, but j is invariant under the action of Γ, hence this map is well defined.

If $\mathbb{C}/\Lambda_{\tau_1}$ and $\mathbb{C}/\Lambda_{\tau_2}$ map to the same elliptic curve, we have $j(\tau_1) = j(\tau_2)$, but j induces a bijection $\Gamma\backslash\mathfrak{h}$, hence τ_1 and τ_2 are conjugate under Γ.

Finally the map is surjective since for an elliptic curve E, it has j-invariant j_0. But there exists $\tau \in \mathfrak{h}$ such that $j(\tau) = j_0$ in which case E_τ is ismorphic to E and E_τ is in the image.

□

0.1. **Algebraic interpretation of the group law.** The complex torus E_τ is equipped with a group structure, how is this realised in the projective curve E_τ?

The bijection between $\mathbb{C}/\Lambda_\tau$ and E_τ is given by the map

$$\alpha \mapsto (\wp(\alpha), \wp'(\alpha))$$

Since $\wp$ and $\wp'$ have poles at Λ, this bijection takes 0 to the point 0 at ∞ of E_τ. Now suppose $P_i = (\wp(\alpha_i), \wp'(\alpha_i))$ are colinear for $i = 1, 2, 3$ are colinear, then there exists $A, B, C \in \mathbb{C}$ such that

$$f(z) = A\wp(z) + B\wp'(z) + C = 0$$

for $z = \alpha_i$. But this is an elliptic function whose only pole is a triple pole at 0. Therefore the only zeros of f are the α_i. Now consider the integral

$$\frac{1}{2\pi i}\int_C z\frac{f'(z)}{f(z)}dz$$

where C is a fundamental parallelogram for the lattice Λ. It follows from the residue theorem that this is just $\sum_{w\in\mathbb{C}\Lambda} w v_w(f)$. However if we consider the integral on each leg of the paralleogram, one sees that after cancellation the integral becomes

$$\frac{1}{2\pi i}\int_{\gamma_1}\frac{f'(z)}{f(z)}dz + \frac{\tau}{2\pi i}\int_{\gamma_2} z\frac{f'(z)}{f(z)}dz$$

where γ_1 is the path from 0 to 1 and γ_2 the path from 0 to τ. Since $\frac{f'}{f}$ is an elliptic function, this must lie in Λ. Thus we have $\alpha_1 + \alpha_2 + \alpha_3 \in \Lambda$, i.e. in the group structure on $\mathbb{C}/\Lambda$, $\alpha_1 + \alpha_2 + \alpha_3 = 0$. In particular, we can take $P_2 = 0$ and then P_3 is the unique point of intersection of the line through P_1 and 0. Then P_3 corresponds to $-P_1$ under the group structure of $\mathbb{C}/\Lambda$.

This gives us a clue how to translate the group structure to the projective curve E_τ. Suppose we have $P, Q \in \mathbf{E}_\tau(\mathbb{C})$, corresponding to $\alpha, \beta \in \mathbb{C}/\Lambda_\tau$. The line L through P and Q intersect at a unique third point R by Bezout's theorem. And R corresponds to to $-\alpha - \beta \in \mathbb{C}/\Lambda_\tau$. Thus by the last remark in the previous paragraph, we have $\alpha + \beta$ corresponds to the third intersection point of the line L' between R and 0.

The upshot of this approach is that this algorithm allows us to define a group structure on an elliptic curve over any field.

Geometric definition of group structure: Suppose E is a an elliptic curve defined by a Weierstrass equation. Let $P, Q \in E$, we wish to define a point $P + Q$.

Step 1: Draw the line L in $\mathbb{P}^2$ which passes through P and Q, (If $P = Q$, take L to be the tangent line through E at P).

Step 2: Bezout's theorem tells us that L intersects E three times with multiplicity, so that $L \cap E = \{P, Q, R\}$.

Step 3: Let L' be the line through the point 0 and R.

Step 4: L' meets E in three point $R, 0$ and another point which we will define to be $P + Q$.

Proposition 0.4. *The composition law defined above satisfies the following properties:*

i) $P + 0 = P$

ii) $P + Q = Q + P$

iii) $\forall \in E$, $\exists(-P) \in E$ *such that* $P + (-P) = 0$

iv) $(P + Q) + R = P + (Q + R)$ *This basically says* $+$ *defines an abelian group structure on* E *such that*) *is the identity. Moreover we have the following:*

v) If E *is defined over* K *then* $E(K)$ *is a subgroup of* $E(\overline{K})$ *under this group structure.*

Proof. This is proposition 2.2 in Silverman. The only hard part is the associativity part iv), this can be checked by an explicit computation. It can be proved in a much simpler way using the Riemann-Roch theorem. □

Exercise: Check the other parts of the above proposition.

In essence this proposition just says that the composition law defines an abelian group structure on E.

Example 0.5. Consider the elliptic curve E defined by the Weierstrass equation $y^2 = x^3 + x$ and let $f = y^2 - x^3 - x$. Then consider the two points $P = (i, 0), Q = (-i, 0) \in E$. The line through these points is given by the set of points

$$\{(x, 0) + (i, 0) : x \in \mathbb{C}\} = \{(x, 0) : x \in \mathbb{C}\}$$

To find the third intersection point, we plug this into the equation for E and find that the three intersection points are P, Q and $(0, 0)$, hence $R = (0, 0)$. Now the line between $(0, 0)$ and O is given by

$$\{(0, y) : y \in \mathbb{C}\}$$

Plugging this into the equation for E we find that this line intersects E at O and at $(0,0)$ with multiplicity 2, hence $P+Q=(0,0)$.

The explicit computations shows that the maps defined by

$$+ : E \times E \to E \text{ and } - : E \to E$$

are morphisms of algebraic varieties. Morphism if E is defined over K, then so are this morphisms. This important result means we have successfully transferred all the complex analytic theorey into a purely algebraic one. To convince yourself of this result it was worth writing down the explicit polynomials defining the map $- : E \mapsto E$. You should find that in the case $a_1, a_3 = 0$ this map is given by

$$(x,y) \mapsto (x,-y)$$

which is clearly a morphism of algebraic varieties.

What we have shown can be more succinctly stated in the following way.

Definition 0.6. A group variety over a field K is an algebraic variety V over K together a K rational point $e \in V(K)$ and morphisms of varieties (also defined over K):

$$m : V \times V \to V$$

$$i : V \to V$$

which satisfy the usual relations for a group. (m is multiplication, e is the identity, i is the inverse).

Given any group variety V and a field extension L/K, the maps m, i and the point e define the structure of a group on the set of L rational points $V(L)$. Thus we have shown that any elliptic has the natural structure of a group variety where the identity is the point 0. Moreover (although we cannot prove this) there is only one possible group structure on an elliptic curve once the point 0 is fixed.

Example 0.7. (The multiplicative group $\mathbb{G}_m$) Let $V = \mathbb{A}^1_K - \{0\}$, this is a variety since it is the complement in $\mathbb{A}^1_K$ of the vanishing set of the polynomial x. Let $1 \in V(K) = K^\times$ be the point e. Then the morphisms m and i given by

$$m(x,y) = xy, i(x) = x^{-1}$$

define the structure of a group variety of V.

For any extension L/K, the group of L rational points $V(L)$ can be identified with $L^\times$. The multiplication given by usual multiplication in L. The torsion points of this group structure over $\overline{K}$ are just the roots of unity.

0.2. **Isogenies of elliptic curves.**

In this section we study maps from elliptic curves to each other. These will be maps of algebraic curves, however an elliptic curve has the extra structure of a marked point 0 so we require our maps to preserve this point.

Definition 0.8. Let (E_1, O_1) and (E_2, O_2) be elliptic curves over K, an isogeny $\phi : E_1 \to E_2$ is a morphism of algebraic curves such that $\phi(O_1) = O_2$. A isogeny is defined over K if it is defined over K as a morphism of algebraic curves.

Two elliptic curves E_1 are isogenous if there exists an non-constant isogeny between them.

Of course we have seen that E_1 and E_2 are endowed with algebraically defined group structures so one would think it should be more natural to consider morhpisms which preserve this group structure. However we have the following theorem:

Theorem 0.9. *An isogeny of elliptic curves $\phi : E_1 \to E_2$ is compatible with the group structure on these curves.*

Proof. This follows from the Riemann Roch theorem. □

This means that if $\phi : E_1 \to E_2$ is defined over K, then for any extension L/K the map induces a group homomorphism on $E_1(L) \to E_2(L)$ on L rational points.

Remark 0.10. Over $\mathbb{C}$ we defined a homomorphism of complex tori $C/\Lambda_1 \to \mathbb{C}/\Lambda_2$ as holomorphic maps which preserve the point $0 \in \mathbb{C}$. We classified these maps as being given by multiplication by $[\alpha]$ for some $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 \subset \Lambda_2$. It can be shown that this map is induced by a map of algebraic curves. Conversely any isogeny defined as above defines a holomorphic map of Riemann surfaces which preserve 0. Thus the complex uniformisation theorem can be refined to the statement that the category of complex tori and the category of elliptic curves over $\mathbb{C}$ are equivalent.

In general if we are working over characteristic 0 fields, the theory of complex tori provides a good source of intuition. Complex tori are very concrete objects and many of the results below are very evident for this case. However one should bear in mind that in positive characteristic, some very weird things can happen.

Recall from the theory of algebraic curves, an isogeny $\phi : E_1 \to E_2$ is either surjective or $\phi(E_1) = 0_2$.

Definition 0.11. An isogeny is separable, resp. inseparable, resp. purely inseparable if the corresponding map of algebraic curves is.

Define the degree of an isogeny to be the degree as a map of algebraic curves, i.e. the degree of the extension of function fields. By convention we set $\deg[0] = 0$, then $\phi = 0$ if and only if $\deg \phi = 0$.

It is a consequence of the definitions that if $\phi : E_1 \to E_2$, $\psi : E_2 \to E_3$ are isogenies, then $\deg \psi \circ \phi = \deg \psi \deg \phi$.

We denote by $\mathrm{Hom}(E_1, E_2)$ the group of isogenies from E_1 to E_2 and $\mathrm{End}(E)$ for the ring of endomorphisms of E. Similarly if E_1 and E_2 are defined over K, we define $\mathrm{Hom}_K(E_1, E_2)$ (resp. $\mathrm{End}(E)$) to be those isogenies which are defined over K. The structure of abelian group of E naturally induces groups structures on these sets. In addition $\mathrm{End}(E)$ is a ring with multiplication given by composition.

What is a non-trivial example of an isogeny? Well since an elliptic curve has the structure of an abelian group, or each $m \in \mathbb{Z}$ there is an algebraically defined multiplication by m map denoted $[m] : E \to E$.

Example 0.12. Consider the elliptic curve E with Weierstrass equation $y^2 = x^3+x$ and let $P = (x_1, y_1)$ be an arbitrary point on E. Let us compute the isogeny [2] on E, i.e. we want to find the coordinates of $P + P$. We have

$$\frac{\partial f}{\partial x} = -3x^2 - 1$$

$$\frac{\partial f}{\partial y} = 2y$$

Thus the tangent line through P is the line $(2y_1, 3x_1^2+1)\lambda + (x_1, y_1)$. Plugging this into the equation for E we obtain the equation

$$((3x_1^2+1)\lambda + y_1)^2 = ((2y_1\lambda + x_1)^3 + 2y_1\lambda + x_1)$$

In order to find the third intersection point, we must solve for λ, but exapnding out the equation we find that we end up solving:

$$\lambda^3 8y_1^3 + (12y_1^2 - 9x_1^4 - 6x_1^2 - 1)\lambda^2 = 0$$

Dividing out by λ^2 we obtain

$$\lambda = \frac{12y_1^2 - 9x_1^4 - 6x_1^2 - 1}{8y_1^2}$$

Therefore the third intersection point is

$$\left(x_1 + \frac{12y_1^2 - 9x_1^4 - 6x_1^2 - 1}{4y_1}, y_1 + \frac{(3x_1^2+1)(12y_1^2 - 9x_1^4 - 6x_1^2 - 1)}{8y_1^2}\right)$$

and hence $2P$ is the point

$$\left(x_1 + \frac{12y_1^2 - 9x_1^4 - 6x_1^2 - 1}{4y_1}, -(y_1 + \frac{(3x_1^2+1)(12y_1^2 - 9x_1^4 - 6x_1^2 - 1)}{8y_1^2})\right)$$

This works for a general point apart from when $y_1 = 0$, but one can show that it extends to a morphism defined everywhere. And defines the self isogeny [2] on the curve E.

This gives the so called [2] multiplication formula, generalising the map $t \mapsto t^2$ for the case of $K^\times$ with its multiplicative group structure. One therefore sees that the two torsion points are given by $y_1 = 0$ and $x = 0, i, -i$. Note that when the base field is $\mathbb{Q}$, these are all algebraic numbers, this follows from the fact that these formulas only involve polynomials defined over $\mathbb{Q}$. Such formulas exist in general for all $[n]$.

Proposition 0.13. *Let E be an elliptic curve over any field K. Then $[m]$ is a non-zero isogeny defined over K.*

Proof. [AEC] Proposition 4.2a). □

The ring End(E) is an important invariant of an elliptic curve. Over a field of characteristic O this ring will usually be $\mathbb{Z}$ (it contains it by the above Proposition). On the other hand if E is defined over a finite field, this ring will always strictly larger than this.

Definition 0.14. When $\mathbb{Z} \subsetneq \mathrm{End}(E)$ is a strict inclusion, we say E has complex multiplication or is CM.

Corollary 0.15. *The ring End(E) is torsion free as a $\mathbb{Z}$ module, and is an integral domain of characteristic 0.*

Proof. The structure of $\mathbb{Z}$ module is given by multiplication by $[m] \in \mathrm{End}(E)$. Then if $[m]\phi = 0$ we have $\deg[m] \deg\phi = 0$, hence $\deg\phi = 0$ so that $\phi = 0$.

Similarly if $\phi \circ \psi = 0$ we have $\deg\phi \deg\psi = 0$ so that either ϕ or ψ is 0.

□

Usually when the only endomorphisms are given by multiplication by $[m]$. These maps provided powerful tools for studying elliptic curves.

Definition 0.16. Let E be an elliptic curve, the m torsion subgroup denoted $E[m]$ is the kernel of $[m]$. In general if α is an isogeny of elliptic curves, we define $E[\alpha]$ to be the kernel of α.

It follows from the theory of algebraic curves that $E[\alpha]$ is a finite subgroup consisting of at most $\deg \alpha$ elements.

Over charactersitic 0, $E[m]$ will always have m^2 elements. This follows from the Leftschetz principle, the basic of which says that you can embed your field into $\mathbb{C}$, from which the theory shows that there are at most m^2 torsion points. But since $[m]$ is a an algebraically defined, one can show using the n multiplication formula that any torsion point is the root of some polynomial hence is algebraic, thus all torsion points can be defined over some algebraic extension of your base field.