THE l-ADIC GALOIS REPRESENTATION ASSOCIATED TO AN ELLIPTIC CURVE

DINA ROUMIANTSEVA

1. Some Basic Definitions

We will begin with some basic definitions in order to develop the notion of an elliptic curve. We will show that there is a natural addition law on the points of an elliptic curve and then we will discuss n-torsion points and use them to construct a representation associated to an elliptic curve.

Definition 1. *Let k be a field, then projective n-space over k*

$$k\mathbb{P}^n = (k^{n+1} - \{0\})/(v \sim \lambda v, \forall \lambda \in k^*)$$

Lemma 1. *$E = \{(x, y, z) \mid y^2z = x^3 + axz^2 + bz^3, a, b \in k\}$ is well-defined as a subspace of $k\mathbb{P}^2$*

(Note: Any homogeneous cubic in x, y and z can be reduced to this form by an invertible change of coordinates as long as the characteristic of k is not 2 or 3, see for example [2, pp. 46–48, 63–64].)

Proof. It suffices to show that $(x, y, z) \in E$ implies $(\lambda x, \lambda y, \lambda z) \in E, \forall \lambda \in k^*$ because E is defined as a subspace of $k^3 - \{0\}$ and $(\lambda x, \lambda y, \lambda z) \in E$ implies $(\frac{1}{\lambda}\lambda x, \frac{1}{\lambda}\lambda y, \frac{1}{\lambda}\lambda z) = (x, y, z) \in E$ as well. But this statement is clear because $y^2z = x^3 + axz^2 + bz^3 \implies \lambda^3 y^2 z = \lambda^3(x^3 + axz^2 + bz^3) \implies (\lambda y)^2 \lambda z = (\lambda x)^3 + a\lambda x(\lambda z)^2 + b(\lambda z)^3$. □

Definition 2. *The discriminant of E as above is $D = -4a^3 - 27b^2$.*

Definition 3. *An elliptic curve is the set E as above such that $x^3 + ax + b = 0$ has distinct roots over $\overline{k}$, the algebraic closure of k.*

Lemma 2. *E is an elliptic curve $\iff D \neq 0$*

Proof. Write $x^3 + ax + b$ as $(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ and observe that $a = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3$, $b = -\alpha_1\alpha_2\alpha_3$, and $\alpha_1 + \alpha_2 + \alpha_3 = 0$. Then it is simply a direct calculation to verify that $D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$. But then it follows directly that D is nonzero if and only if the roots are distinct. □

Now let (x, y, z) be a representative of a class in E and suppose $z \neq 0$ then $(\frac{x}{z}, \frac{y}{z}, 1)$ is the unique representative of $[(x, y, z)]$, the class of (x, y, z), in the plane $z = 1$. So we can think of projective points on E with nonzero z-coordinate as corresponding bijectively to solutions (x, y) of $y^2 = x^3 + ax + b$. Now suppose $z = 0$, then $[(x, y, z)] \in E$ implies that $x^3 = 0$, so there is exactly one such class, it is $[(0, 1, 0)]$. When looking at the curve in affine coordinates, we will call this class $\mathcal{O}$, the point at infinity.

Definition 4. *Let $+: E \times E \to E$ such that $\mathcal{O}$ is the identity and $A+B = A^*B^*\mathcal{O}$, where X^*Y is the third point on the line $\overline{XY}$. We also define $\overline{XX}$ to be the line tangent to the curve at X, $\mathcal{O}^*\mathcal{O} = \mathcal{O}$, and say that a line intersects $\mathcal{O} \iff$ it is vertical.*

Given the notion of intersection multiplicity, this definition makes sense for all cases, but we will make it more precise without using algebraic geometry shortly. First, if $\overline{A\mathcal{O}}$ goes through no other points on the curve besides those two, we define $A^*\mathcal{O} = A$. Next, suppose $A = (x_1, y_1), B = (x_2, y_2)$, and $\overline{AB}$ is not a vertical line, then we write its equation as $y = mx + d$. To get the third point, we make the substitution $y^2 = (mx+d)^2 = x^3+ax+b$, so we have $x^3-m^2x^2-(2md-a)x+b-d^2 = (x - x_1)(x - x_2)(x - x_3) \implies x_3 = m^2 - x_1 - x_2$. So we can define A^*B to be the unique point on $\overline{AB}$ with x_3 as its x-coordinate.

Now we can compute explicit formulas for addition of two points: if $A + B \neq \mathcal{O}$,

$$A + B = (m^2 - x_1 - x_2, m(m^2 - 2x_1 - x_2) + y_1) \tag{1}$$

where $m = \frac{y_2-y_1}{x_2-x_1}$ if $A \neq B$, and $m = \frac{dy}{dx} = \frac{3x^2+a}{2y}$ if $A = B$. The fact that m is well defined in the second case means that if $y = 0$ then we need $A + A = \mathcal{O}$, therefore we need to show that if $y = 0$, then $3x^2 + a \neq 0$ since then $\frac{dx}{dy} = 0$, so $A^*A = \mathcal{O}$ and $A + A = \mathcal{O}$. However, a polynomial and its derivative have a root in common if and only if it is a double root of the polynomial, but we specified that it have all distinct roots. Now we can look at the points on the elliptic curve as a group under this operation, where $\mathcal{O}$ is the identity, $A^{-1} = (x_1, -y_1)$, and the associativity follows quite directly, albeit tediously, from the formulas (there is also a nice geometric argument for it on p. 21 of [3]). This group is abelian because the * operation is clearly commutative.

2. n-torsion points on E

The main goal of this section is to show that the group of n-torsion points over $\overline{k}$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. We present the outline of an elementary proof suggested in [3], we then give the description of a more standard but less elementary proof which uses complex analysis, however this proof has the disadvantage that it only works for subfields of $\mathbb{C}$.

Definition 5. *An n-torsion point of an elliptic curve is a point such that $nA = \overbrace{A + \cdots + A}^{n \text{ terms}} = \mathcal{O}$*

From here on we assume that the characteristic of k is 0.

Proposition 1. *$\exists P_n \in \mathbb{Z}[x]$ of degree $n^2 - 1$ such that $(x, y) \in E$ is an n-torsion point $\iff$ $P_n(x) = 0$. Additionally, P_n has a double root at x if $y \neq 0$ and a simple root otherwise.*

Proof. See [3, exercise 6.4, (a)–(f)]. Our P_n corresponds to ψ_n^2 in the book. Note also that the statement of part (e) is incorrect and should be changed to the statement given above. □

Corollary 1. *$E[n]$, the group of n-torsion points over $\overline{k}$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Proof. First, there are exactly n^2 n-torsion points because if x is a root of P_n, then there are two points on the curve with x as their x-coordinate unless their y-coordinate is 0, in which case there is one. Hence the number of points with x as their x-coordinate is the same as the order of the zero of P_n at x. Therefore, by Proposition 1, there are $n^2 - 1$ points (x, y) such that $P_n(x) = 0$ and hence there are $n^2 - 1$ nontrivial points in $E[n]$. Together with $\mathcal{O}$ we get n^2 points.

Now to show that $E[n]$is actually $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, let $n = p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}$ be the prime factorization of n. First, it is enough to show that no more than two $\mathbb{Z}/p_i^r\mathbb{Z}$ terms can appear in the abelian decomposition of $E[n]$for any i. This is because if s such terms appear with exponents $t_1, \dots, t_s$, we must have $\Sigma_j t_j = 2r_i$ but each $t_j \leq r_i$ because otherwise there would be a point of order not dividing n. But if $s \leq 2$, we immediately have that $s = 2$ and $t_1 = t_2 = r_i$. To finish the proof, choose generators $a_1, \dots, a_s$ of each copy of $\mathbb{Z}/p_i^{t_j}\mathbb{Z}$ and note that $p_i^{t_j - 1} a_j$ has order exactly p_i. Thus $\{p_i^{t_j - 1} a_j\}$ generate a subgroup of p_i-torsion points of order p_i^s. But the number of p_i-torsion points is p_i^2 so $s \leq 2$ as desired. □

We will now outline the complex-analytic proof of the goal stated earlier.

Theorem 1. *Every elliptic curve over $\mathbb{C}$ is isomorphic as an abelian group to $\mathbb{C}/L$ where L is some lattice in the complex plane.*

Proof. The proof that $\mathbb{C}/L$ is isomorphic to an elliptic curve requires no more than basic complex analysis and a particularly elegant approach is given in [1, pp. 14–35]. The fact that every elliptic curve is of this form is more difficult and there are several common approaches. One approach using j-invariants is given in [1, pp. 119–121]. □

Corollary 2. *Let k be a subfield of $\mathbb{C}$ and E defined over k. Then $E[n]$ is $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ over $\overline{k}$.*

Proof. It is clear from Theorem 1 that $E[n]$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ over $\mathbb{C}$ since if $\omega_1, \omega_2 \in \mathbb{C}$ generate L such that $\mathbb{C}/L$ is isomorphic to E, then it is clear that $\{c_1 \frac{\omega_1}{n} + c_2 \frac{\omega_2}{n}\}$ is exactly the set of n-torsion points. However, it follows from an argument identical to the one in Proposition 2 that if σ is an automorphism of $\mathbb{C}$ then the map $(x, y) \to (\sigma x, \sigma y)$ permutes the n-torsion points of E and since there are only finitely many n-torsion points, it follow that their coordinates generate an extension of finite degree over k. Therefore, all n^2 n-torsion points lie inside $\overline{k}$. □

3. The Galois Representation

Definition 6. *Given $\sigma \in \mathrm{Gal}(\overline{k}/k)$, we define an action of σ on $\overline{k}^2$ by $\sigma(x, y) = (\sigma x, \sigma y)$.*

Proposition 2. *$f_\sigma \colon (x, y) \to \sigma(x, y)$ induces an automorphism of E, where we define $f_\sigma(\mathcal{O}) = \mathcal{O}$.*

Proof. First, we will show that f_σ sends E to E, so say $y^2 = x^3 + ax + b$, $a, b \in k$, then $(\sigma(y))^2 = \sigma(y^2) = \sigma(x^3 + ax + b) = \sigma(x^3) + \sigma(a)\sigma(x) + \sigma(b) = (\sigma(x))^3 + a\sigma(x) + b$ because σ fixes k, so $(\sigma x, \sigma y) \in E$. By a similar argument, f_σ is a homomorphism simply because the addition map is given by rational functions with coefficients in k and is therefore preserved by f_σ. Finally, it is actually an automorphism since σ is invertible. □

(Note that here we mean automorphisms of E as an abelian group. $\mathrm{Aut}(E)$ often refers to group automorphisms given by an algebraic map, which f_σ isn't in general.)

This actually gives a homomorphism from $\mathrm{Gal}(\overline{k}/k) \to \mathrm{Aut}(E)$ since it is trivial to see that $(\sigma\tau)(x,y) = \sigma(\tau(x,y))$.

Since f_σ is an automorphism of E it sends $E[n]$ to $E[n]$. In order to take advantage of this to develop a representation of $\mathrm{Gal}(\overline{k}/k)$, we will construct a convenient module, called the Tate module.

Definition 7. *Let $G_1, G_2, \dots$ be any finite groups and $\varphi_i \colon G_{i+1} \to G_i$ any homomorphisms. The inverse limit, $G = \varprojlim G_i$ is the set of all sequences $g = \{g_i\}$ such that $g_i \in G_i$ and $\varphi_i(g_{i+1}) = g_i$.*

Definition 8. *$\mathbb{Z}_l$, the l-adic integers, are $\varprojlim \mathbb{Z}/l^i\mathbb{Z}$ with the φ_i just taking the residue modulo l^i.*

Definition 9. *The Tate module, T_l, is $\varprojlim E[l^i]$ with the φ_i being the multiplication by l maps.*

Lemma 3. *T_l is a free $\mathbb{Z}_l$-module of rank 2.*

Proof. First, T_l is a $\mathbb{Z}_l$-module since if $\mathcal{P} = (\mathcal{P}_1, \mathcal{P}_2, \dots) \in T_l$ and $m = (m_1, m_2, \dots) \in \mathbb{Z}_l$, we can define $m\mathcal{P} = (m_1\mathcal{P}_1, m_2\mathcal{P}_2, \dots)$. This is well-defined because the m_i are defined mod l^i and the $\mathcal{P}_i$ are l^i-torsion points. Furthermore, it is in T_l because $lm_i\mathcal{P}_i = m_i\mathcal{P}_{i-1} = m_{i-1}\mathcal{P}_{i-1}$ because $m_i \equiv m_{i-1} \mod l^{i-1}$. T_l is clearly a free module because if $\mathcal{P} \neq 0$ is in the Tate module, and $m \neq 0$ in $\mathbb{Z}_l$ then $m\mathcal{P} \neq 0$ directly from the definition. To show it is of rank 2, start by choosing any point $\mathcal{P} \in T_l$ such that $\mathcal{P}_i \neq 0, then \forall i$, for each i, choose a $\mathcal{P}'_i$ outside of $\{j\mathcal{P}_i\}$ such that $l\mathcal{P}'_i = \mathcal{P}'_{i-1}$. Then it is clear that $\mathcal{P}$ and $\mathcal{P}'$ are linearly independent and span T_l. □

Now we claim that given $\sigma \in \mathrm{Gal}(\overline{k}/k)$, f_σ defined above induces an invertible $\mathbb{Z}_l$-linear map from T_l to itself, by sending $(\mathcal{P}_1, \mathcal{P}_2, \dots)$ to $\rho(\sigma)(\mathcal{P}) = (f_\sigma(\mathcal{P}_1), f_\sigma(\mathcal{P}_2), \dots)$. First, we want to show that $\rho(\sigma)(\mathcal{P}) \in T_l$. But since f_σ is an automorphism, it takes $E[n]$to $E[n]$, so we only need to show that $l(f_\sigma(\mathcal{P}_{i+1})) = f_\sigma(\mathcal{P}_i)$, which is clear because l commutes with f_σ since f_σ is a homomorphism. Similarly, $\rho(\sigma)$ is $\mathbb{Z}_l$-linear because f_σ is a homomorphism and addition and scalar multiplication can be evaluated term by term. The above discussion gives us the following:

Proposition 3. *ρ is a homomorphism from $Gal(\overline{k}/k)$ to $GL(T_l)$.*

If we choose a basis $\{e_1, e_2\}$, we get an isomorphism between $GL(T_l)$ and $GL_2(\mathbb{Z}_l)$, the set of invertible 2×2 matrices with coefficients in $\mathbb{Z}_l$. Since $\mathbb{Z}_l \subset \mathbb{Q}_l$, we can think of the 2×2 matrices as invertible linear maps from $\mathbb{Q}_l^2$ to itself. This gives us:

Theorem 2. *Given a choice of basis of T_l, ρ is a 2-dimensional representation of $Gal(\overline{k}/k)$ over $\mathbb{Q}_l$.*

4. Cool Facts

The remarkable thing about this representation is that one can recover much of the information about the elliptic curve from it alone. First we show that

Proposition 4. *The field extension of k generated by the coordinates of $E[l^i]$ can be determined solely from the Galois representation of E.*

Proof. First, let k' be an extension of k, and suppose that $E[l^i]$ has coefficients in k', then take $\sigma \in \mathrm{Gal}(\overline{k}/k)$ such that σ fixes k'. So σ acts as the identity $E[l^i]$ which means that the first i terms of the coefficients of the matrix for $\rho(\sigma)$ are 1 on the diagonal and 0 otherwise. But this is actually if and only if. To determine what field is generated by coefficients of $E[l^i]$, this is simply the fixed field of $\{\sigma$ such that the first i terms of the coefficients of the matrix for $\rho(\sigma)$ are the same as the identity matrix $\}$. □

We will state two further examples, justification of which is far beyond the scope of this paper, which demonstrate the power of this representation. First, given an elliptic curve over $\mathbb{Q}$ we can look at the set of solutions to the same equation over $\mathbb{Z}/p\mathbb{Z}$ for any p. This will define an elliptic curve for all but finitely many p, since the discriminant vanishes mod p exactly when p divides the discriminant of E over $\mathbb{Q}$. Therefore in all the other cases, the discriminant mod p will be nonzero which by Lemma 2 means that we get an elliptic curve over $\mathbb{Z}/p\mathbb{Z}$. It is a theorem that one can actually recover the number of points of E over $\mathbb{Z}/p\mathbb{Z}$ for any p simply by examining the l-adic Galois representation of E over $\mathbb{Q}$ for any l.

Finally, one can define an l-adic Galois representation attached to a modular form of weight 2 in an analogous but substantially more technical manner. It has long been known that given an elliptic curve E and a modular form of weight 2, E is parametrized by a modular form if and only if they have the same l-adic Galois representation for some l. Therefore, when Andrew Wiles proved that every semistable elliptic curve can be parametrized by a modular form of weight 2, what he did was to show that given any semistable elliptic curve he could produce a modular form of weight 2 whose 3-adic Galois representation was the same as that of the elliptic curve.

References

1. Neal Koblitz, *Introduction to elliptic curves and modular forms*, 2nd ed., Springer-Verlag, New York, US, 1993.
2. Joseph Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, US, 1986.
3. Joseph Silverman and John Tate, *Rational points on elliptic curves*, Springer-Verlag, New York, US, 1992.