p-Divisible Groups and Reciprocity Laws

Ricky Magner

May 15, 2020

Overview

Table of Contents

Elliptic Curves

- We can think of an elliptic curve as the solutions to the equation $y^2 = x^3 + Ax + B$ for constants A and B.

Elliptic Curves

- We can think of an elliptic curve as the solutions to the equation $y^2 = x^3 + Ax + B$ for constants A and B.
- ex: $E : y^2 = x^3 - x$.

Elliptic Curves

- We can think of an elliptic curve as the solutions to the equation $y^2 = x^3 + Ax + B$ for constants A and B.
- ex: $E : y^2 = x^3 - x$.
- We have the addition law $P + Q = R$ with identity element 0 at ∞:

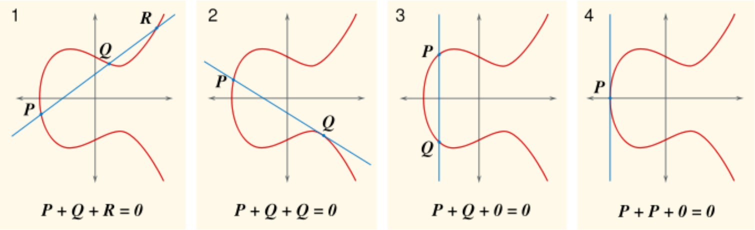

Figure: Group Law on E

Elliptic Curves and Tori

- We can think about the $\mathbb{C}$-points of E as forming a torus. In particular $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$.

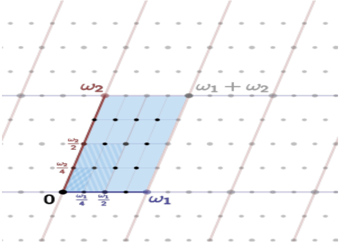

Figure: $E(\mathbb{C})$ as a torus

Elliptic Curves and Tori

- We can think about the $\mathbb{C}$-points of E as forming a torus. In particular $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$.

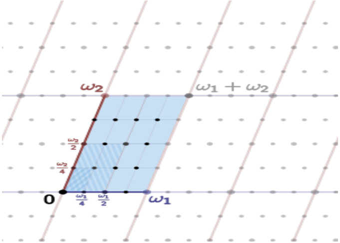

Figure: $E(\mathbb{C})$ as a torus

- We can visualize the *torsion points*, i.e. those of finite order, this way. We write $E[n]$ for the n-torsion. We see $E[n] \cong \mathbb{Z}/n \times \mathbb{Z}/n$.

Division Polynomials

- How do we find coordinates for the points in $E[n]$ given $y^2 = x^3 + Ax + B$?

Division Polynomials

- How do we find coordinates for the points in $E[n]$ given $y^2 = x^3 + Ax + B$?
- Use rational functions for addition formula to compute $[n](x, y) = (x, y) + \cdots + (x, y)$ and solve for $[n](x, y) = \infty$.

Division Polynomials

- How do we find coordinates for the points in $E[n]$ given $y^2 = x^3 + Ax + B$?
- Use rational functions for addition formula to compute $[n](x, y) = (x, y) + \cdots + (x, y)$ and solve for $[n](x, y) = \infty$.
- **Example:** $E : y^2 = x^3 - x$. Then $[2](x, y) = (X, Y)$ for

$$X = (x^4 + 2x^2 + 1)/(4x^3 - 4x)$$
$$Y = (8x^6 y - 40x^4 y - 40x^2 y + 8y)/(64x^6 - 128x^4 + 64x^2)$$

Division Polynomials

- How do we find coordinates for the points in $E[n]$ given $y^2 = x^3 + Ax + B$?
- Use rational functions for addition formula to compute $[n](x, y) = (x, y) + \cdots + (x, y)$ and solve for $[n](x, y) = \infty$.
- **Example:** $E : y^2 = x^3 - x$. Then $[2](x, y) = (X, Y)$ for

$$X = (x^4 + 2x^2 + 1)/(4x^3 - 4x)$$
$$Y = (8x^6y - 40x^4y - 40x^2y + 8y)/(64x^6 - 128x^4 + 64x^2)$$

- So $(x, y) \in E[2]\backslash\{\infty\}$ if and only if $4x^3 - 4x = 0$, or $x = 0, \pm 1 \implies E[2] = \{\infty, (0, 0), (\pm 1, 0)\}$.

Division Polynomials (cont.)

- **Example:** $E : y^2 = x^3 - x$. Then $[3](x, y) = (X, Y)$ for

$$X = (x^9 + 12x^7 + 30x^5 - 36x^3 + 9x)/ \\ (9x^8 - 36x^6 + 30x^4 + 12x^2 + 1)$$

$$Y = (6x^{12}y - 132x^{10}y - 990x^8y + 552x^6y - 1110x^4y + 540x^2 \\ (162x^{12} - 972x^{10} + 1782x^8 - 648x^6 - 594x^4 - 108x^2 - 6)$$

Division Polynomials (cont.)

- **Example:** $E : y^2 = x^3 - x$. Then $[3](x, y) = (X, Y)$ for

$$X = (x^9 + 12x^7 + 30x^5 - 36x^3 + 9x)/$$
$$(9x^8 - 36x^6 + 30x^4 + 12x^2 + 1)$$
$$Y = (6x^{12}y - 132x^{10}y - 990x^8y + 552x^6y - 1110x^4y + 540x^2$$
$$(162x^{12} - 972x^{10} + 1782x^8 - 648x^6 - 594x^4 - 108x^2 - 6)$$

- So $(x, y) \in E[3] \backslash \{\infty\}$ if and only if $9x^8 - 36x^6 + 30x^4 + 12x^2 + 1 = (3x^4 - 6x^2 - 1)^2 = 0$. Note this quartic is irreducible over $\mathbb{Q}$, so these points have coordinates over a finite extension of $\mathbb{Q}$.

Systems of p-Torsion

- From the picture, we see that $E[2] \subset E[4] \subset E[8] \subset \dots$, and that $\cup_{n \geq 1} E[2^n]$ is dense in $E(\mathbb{C})$. We write $E[2^\infty]$ for the union of the $E[2^n]$'s.

Systems of p-Torsion

- From the picture, we see that $E[2] \subset E[4] \subset E[8] \subset \dots$, and that $\cup_{n \geq 1} E[2^n]$ is dense in $E(\mathbb{C})$. We write $E[2^\infty]$ for the union of the $E[2^n]$'s.
- More generally, the p-divisible group associated to E is

$$E[p^\infty] = \bigcup_{n \geq 1} E[p^n].$$

Abelian Reciprocity for $\mathbb{Q}(i)$

- Let $K = \mathbb{Q}(i)$ be the field of $r + si$ with $r, s \in \mathbb{Q}$. Fix a prime p, and let $E : y^2 = x^3 - x$ as before. Set $L_n = K(x(E[p^n]))$, i.e. the extension by adjoining the x-coordinates of points in $E[p^n]$ and $L_\infty = K(x(E[p^\infty]))$.

Abelian Reciprocity for $\mathbb{Q}(i)$

- Let $K = \mathbb{Q}(i)$ be the field of $r + si$ with $r, s \in \mathbb{Q}$. Fix a prime p, and let $E : y^2 = x^3 - x$ as before. Set $L_n = K(x(E[p^n]))$, i.e. the extension by adjoining the x-coordinates of points in $E[p^n]$ and $L_\infty = K(x(E[p^\infty]))$.

Theorem

L_n/K is a Galois extension with group

$$\mathrm{Gal}(L_n/K) \cong (\mathbb{Z}[i]/p^n)^\times = \mathrm{GL}_1(\mathbb{Z}[i]/p^n).$$

Furthermore, if M/K is a finite Galois extension with abelian Galois group (unramified away from p), then $M \subseteq L_\infty$.

Abelian Reciprocity for $\mathbb{Q}(i)$

- Let $K = \mathbb{Q}(i)$ be the field of $r + si$ with $r, s \in \mathbb{Q}$. Fix a prime p, and let $E : y^2 = x^3 - x$ as before. Set $L_n = K(x(E[p^n]))$, i.e. the extension by adjoining the x-coordinates of points in $E[p^n]$ and $L_\infty = K(x(E[p^\infty]))$.

Theorem

L_n/K is a Galois extension with group

$$\mathrm{Gal}(L_n/K) \cong (\mathbb{Z}[i]/p^n)^\times = \mathrm{GL}_1(\mathbb{Z}[i]/p^n).$$

Furthermore, if M/K is a finite Galois extension with abelian Galois group (unramified away from p), then $M \subseteq L_\infty$.

- Under the Langlands philosophy, theorems relating Galois groups to Lie groups are called *reciprocity laws*.

Table of Contents

General p-Divisible Groups

- Suppose we start with an elliptic curve mod p, i.e. $E : y^2 \equiv x^3 + Ax + B \bmod p$. Then the group law still works on $\mathbb{Z}/p$ points, and we can talk about $E[p^n]$ as before. We get the p-divisible group $E[p^\infty]$.

General p-Divisible Groups

- Suppose we start with an elliptic curve mod p, i.e. $E : y^2 \equiv x^3 + Ax + B \bmod p$. Then the group law still works on $\mathbb{Z}/p$ points, and we can talk about $E[p^n]$ as before. We get the p-divisible group $E[p^\infty]$.
- In fact, if A is an abelian variety (a space defined by polynomial equations with a group law), then we can form $A[p^\infty]$ analogously.

General p-Divisible Groups

- Suppose we start with an elliptic curve mod p, i.e. $E : y^2 \equiv x^3 + Ax + B \bmod p$. Then the group law still works on $\mathbb{Z}/p$ points, and we can talk about $E[p^n]$ as before. We get the p-divisible group $E[p^\infty]$.
- In fact, if A is an abelian variety (a space defined by polynomial equations with a group law), then we can form $A[p^\infty]$ analogously.

Abstract p-divisible group

We can define an abstract p-divisible group $\mathbb{X}$ to be a sequence $\mathbb{X}_n$ behaving like the examples above; a bit more precisely, $\mathbb{X}_n$ should a group defined by polynomials with a surjective multiplication by p map $[p] : \mathbb{X}_{n+1} \to \mathbb{X}_n$.

Reduction mod p

- When working[1] mod p, these can be characterized succinctly. A general $\mathbb{X}$ can be made out of "simple" building blocks, i.e. $\mathbb{X} = \oplus_i \mathbb{X}_i$ for some simple p-divisible groups $\mathbb{X}_i$.

[1]We should technically work over $\overline{\mathbb{F}}_p$, the algebraic closure of $\mathbb{Z}/p$

Reduction mod p

- When working[1] mod p, these can be characterized succinctly. A general $\mathbb{X}$ can be made out of "simple" building blocks, i.e. $\mathbb{X} = \oplus_i \mathbb{X}_i$ for some simple p-divisible groups $\mathbb{X}_i$.

Theorem (Dieudonne-Manin)

The simple p-divisible groups mod p are of the form $\mathbb{X}_\lambda$ for $\lambda \in \mathbb{Q}$. The endomorphism ring of maps $\mathbb{X}_\lambda \to \mathbb{X}_\lambda$ is D_λ, the division algebra over $\mathbb{Q}_p$ of invariant λ.

[1] We should technically work over $\overline{\mathbb{F}}_p$, the algebraic closure of $\mathbb{Z}/p$

Reduction mod p

- When working[1] mod p, these can be characterized succinctly. A general $\mathbb{X}$ can be made out of "simple" building blocks, i.e. $\mathbb{X} = \oplus_i \mathbb{X}_i$ for some simple p-divisible groups $\mathbb{X}_i$.

Theorem (Dieudonne-Manin)

The simple p-divisible groups mod p are of the form $\mathbb{X}_\lambda$ for $\lambda \in \mathbb{Q}$. The endomorphism ring of maps $\mathbb{X}_\lambda \to \mathbb{X}_\lambda$ is D_λ, the division algebra over $\mathbb{Q}_p$ of invariant λ.

- **Example:** If $\mathbb{X} = E[p^\infty]$, then either $\mathbb{X} = \mathbb{X}_{1/2}$ or $\mathbb{X} = \mathbb{X}_0 \oplus \mathbb{X}_1$ depending on if E is supersingular or not. In the former case, $D_{1/2}$ is the p-adic quaternion algebra.

[1] We should technically work over $\overline{\mathbb{F}}_p$, the algebraic closure of $\mathbb{Z}/p$

Table of Contents

Deformations to Characteristic 0

- Let $\mathbb{X} = \mathbb{X}_\lambda$ be a simple p-divisible group mod p as before. We consider possible ways to "lift" $\mathbb{X}$ to characteristic 0.

[2] Technically this should be a quasi-isogeny

Deformations to Characteristic 0

- Let $\mathbb{X} = \mathbb{X}_\lambda$ be a simple p-divisible group mod p as before. We consider possible ways to "lift" $\mathbb{X}$ to characteristic 0.
- We say a pair (X, ρ) is a deformation of $\mathbb{X}$ if X is a p-divisible group over $\mathbb{Z}_p$, and $\rho : \overline{X} \to \mathbb{X}$ is an isomorphism[2].

[2] Technically this should be a quasi-isogeny

Deformations to Characteristic 0

- Let $\mathbb{X} = \mathbb{X}_\lambda$ be a simple p-divisible group mod p as before. We consider possible ways to "lift" $\mathbb{X}$ to characteristic 0.
- We say a pair (X, ρ) is a deformation of $\mathbb{X}$ if X is a p-divisible group over $\mathbb{Z}_p$, and $\rho : \overline{X} \to \mathbb{X}$ is an isomorphism[2].
- One can think of X over $\mathbb{Z}_p$ as a sequence of p-divisible groups X_n over $\mathbb{Z}/p^n$ compatible with reduction.

[2] Technically this should be a quasi-isogeny

Rapoport-Zink Spaces

Theorem

The set of deformations

$$\mathcal{M}_\lambda = \{(X, \rho) : \text{ a deformation of } \mathbb{X}_\lambda\}$$

can be given the structure of a p-adic manifold. In particular, if $\lambda = 1/h$, then $\mathcal{M}_\lambda$ is an $(h-1)$-dimensional p-adic disk.

Rapoport-Zink Spaces

Theorem

The set of deformations

$$\mathcal{M}_\lambda = \{(X, \rho) : \text{ a deformation of } \mathbb{X}_\lambda\}$$

can be given the structure of a p-adic manifold. In particular, if $\lambda = 1/h$, then $\mathcal{M}_\lambda$ is an $(h-1)$-dimensional p-adic disk.

- We see there's a natural action of $D_\lambda^\times$ on $\mathcal{M}_\lambda$ given by $\gamma \cdot (X, \rho) = (X, \gamma \circ \rho)$ for $\gamma \in D_\lambda^\times$. This action is compatible with the geometric structure.

Level Structure

- Let $n \geq 1$. Then if X is a deformation of $\mathbb{X}$ with $\lambda = d/h$, we have $X[p^n] \cong (\mathbb{Z}/p^n)^h$.

Level Structure

- Let $n \geq 1$. Then if X is a deformation of $\mathbb{X}$ with $\lambda = d/h$, we have $X[p^n] \cong (\mathbb{Z}/p^n)^h$.
- Let $\mathcal{M}_\lambda^n = \{(X, \rho, \phi) : (X, \rho)$ a deformation of $\mathbb{X}$ and $\phi : X[p^n] \cong (\mathbb{Z}/p^n)^h\}$.

Level Structure

- Let $n \geq 1$. Then if X is a deformation of $\mathbb{X}$ with $\lambda = d/h$, we have $X[p^n] \cong (\mathbb{Z}/p^n)^h$.
- Let $\mathcal{M}_\lambda^n = \{(X, \rho, \phi) : (X, \rho)$ a deformation of $\mathbb{X}$ and $\phi : X[p^n] \cong (\mathbb{Z}/p^n)^h\}$.
- Then $\mathcal{M}_\lambda^n$ also has the structure of a p-adic manifold, with maps $\mathcal{M}_\lambda^{n+1} \to \mathcal{M}_\lambda^n$ via reduction.

Level Structure

- Let $n \geq 1$. Then if X is a deformation of $\mathbb{X}$ with $\lambda = d/h$, we have $X[p^n] \cong (\mathbb{Z}/p^n)^h$.
- Let $\mathcal{M}_\lambda^n = \{(X, \rho, \phi) : (X, \rho)$ a deformation of $\mathbb{X}$ and $\phi : X[p^n] \cong (\mathbb{Z}/p^n)^h\}$.
- Then $\mathcal{M}_\lambda^n$ also has the structure of a p-adic manifold, with maps $\mathcal{M}_\lambda^{n+1} \to \mathcal{M}_\lambda^n$ via reduction.
- Now we have an action of $\mathrm{GL}_h(\mathbb{Z}/p^n)$ on $\mathcal{M}_\lambda^n$ via $g \cdot (X, \rho, \phi) = (X, \rho, g \circ \phi)$.

Local Langlands Correspondence

- The maps $\mathcal{M}_\lambda^{n+1} \to \mathcal{M}_\lambda^n$ induce maps on cohomology $H^*(\mathcal{M}_\lambda^n) \to H^*(\mathcal{M}_\lambda^{n+1})$, and the direct limit, denoted $H^*(\mathcal{M}_\lambda^\infty)$, has an action of $\mathrm{GL}_h(\mathbb{Q}_p) \times D_\lambda^\times \times W_{\mathbb{Q}_p}$, after "passing to generic fiber."

Local Langlands Correspondence

- The maps $\mathcal{M}_\lambda^{n+1} \to \mathcal{M}_\lambda^n$ induce maps on cohomology $H^*(\mathcal{M}_\lambda^n) \to H^*(\mathcal{M}_\lambda^{n+1})$, and the direct limit, denoted $H^*(\mathcal{M}_\lambda^\infty)$, has an action of $\mathrm{GL}_h(\mathbb{Q}_p) \times D_\lambda^\times \times W_{\mathbb{Q}_p}$, after "passing to generic fiber."
- For a "nice" representation π of $\mathrm{GL}_h(\mathbb{Q}_p)$, we can take π-isotypic components to get:

Local Langlands Correspondence

- The maps $\mathcal{M}_\lambda^{n+1} \to \mathcal{M}_\lambda^n$ induce maps on cohomology $H^*(\mathcal{M}_\lambda^n) \to H^*(\mathcal{M}_\lambda^{n+1})$, and the direct limit, denoted $H^*(\mathcal{M}_\lambda^\infty)$, has an action of $\mathrm{GL}_h(\mathbb{Q}_p) \times D_\lambda^\times \times W_{\mathbb{Q}_p}$, after "passing to generic fiber."
- For a "nice" representation π of $\mathrm{GL}_h(\mathbb{Q}_p)$, we can take π-isotypic components to get:

Theorem

Let $\lambda = 1/h$. Then

$$H^*(\mathcal{M}_\lambda^\infty)[\pi] \cong \rho_\pi \boxtimes \sigma_\pi$$

where ρ_π and σ_π are representations of $D_\lambda^\times$ and $W_{\mathbb{Q}_p}$ respectively associated to π with arithmetic compatibilities.

LLC

- In other words, the cohomology of $\mathcal{M}_{\lambda}^{\infty}$ gives a geometric reason for the existence of a reciprocity law $\pi \rightleftarrows \sigma_{\pi}$ relating representations of the Lie group $\mathrm{GL}_h(\mathbb{Q}_p)$ and the Galois group $W_{\mathbb{Q}_p}$!

Table of Contents

Mixed Characteristic Shtukas

- In general, given an h-tuple $\mu = (1, 1, \ldots, 0, 0)$ of 0's and 1's, and $\lambda = 1/h$, one can define a space $\mathcal{M}^{\infty}_{\lambda,\mu}$ so that $\mu = (1, 0, \ldots, 0)$ agrees with above.

Mixed Characteristic Shtukas

- In general, given an h-tuple $\mu = (1, 1, \ldots, 0, 0)$ of 0's and 1's, and $\lambda = 1/h$, one can define a space $\mathcal{M}_{\lambda,\mu}^{\infty}$ so that $\mu = (1, 0, \ldots, 0)$ agrees with above.
- Scholze and Weinstein reinterpreted the space $\mathcal{M}_{\lambda,\mu}^{\infty}$ in terms of a space of "shtukas" $\mathrm{Sht}_{\lambda,\mu}$ on the Fargues-Fontaine curve, i.e. certain maps of rank h vector bundles on the curve compatible with a linear algebraic condition depending on μ.

Mixed Characteristic Shtukas

- In general, given an h-tuple $\mu = (1, 1, \ldots, 0, 0)$ of 0's and 1's, and $\lambda = 1/h$, one can define a space $\mathcal{M}^{\infty}_{\lambda,\mu}$ so that $\mu = (1, 0, \ldots, 0)$ agrees with above.
- Scholze and Weinstein reinterpreted the space $\mathcal{M}^{\infty}_{\lambda,\mu}$ in terms of a space of "shtukas" $\mathrm{Sht}_{\lambda,\mu}$ on the Fargues-Fontaine curve, i.e. certain maps of rank h vector bundles on the curve compatible with a linear algebraic condition depending on μ.
- The condition on μ makes sense for any tuple, so $\mathrm{Sht}_{\lambda,\mu}$ generalizes the old Rapoport-Zink spaces with infinite level structure.

Mixed Char Shtukas (cont.)

- Let $r_\mu : \mathrm{GL}_h \to \mathrm{GL}(V)$ be the representation of GL_h corresponding to the tuple μ.

Mixed Char Shtukas (cont.)

- Let $r_\mu : \mathrm{GL}_h \to \mathrm{GL}(V)$ be the representation of GL_h corresponding to the tuple μ.
- One expects a generalization of the Kottwitz conjecture:

Conjecture

For π a "nice" representation of $\mathrm{GL}_h(\mathbb{Q}_p)$,

$$H^*(\mathrm{Sht}_{\lambda,\mu})[\pi] \cong \rho_\pi \boxtimes r_\mu \circ \sigma_\pi,$$

with ρ_π and σ_π representations of $D_\lambda^\times$ and $W_{\mathbb{Q}_p}$ as before.

Thanks for listening!