TOPICS IN ALGEBRA 4/30 NOTES BY: NATHAN PIERCE

ELLIPTIC CURVES

Take a field K and a curve E over K

E is a — smooth projective curve of genus 1 with or point on E with co-ords in K

We can get: $E \subset \mathbb{P}^2_K$

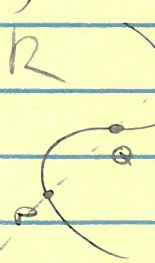
$O \to \infty$

E given by Weierstrass equation

We showed $E(\overline{K}) \cong Pic^0(E)$

Since $Pic^0(E)$ is Abel grp, we get an induced Abel. grp. structure on $E(\overline{K})$.

PROP: Suppose $P, Q, R \in E(\overline{K})$
Then $P+Q+R=O$ iff P, Q, R are collinear.



COR: $P+Q$ is algebraic
(Intersection of a line and a curve)

Cor: If $P, Q \in E(L)$, $L \subset \bar{K}$
Then $P+Q \in E(L)$

PROOF of PROP: X, Y, Z are coords on $\mathbb{P}^2_K$

Take $R' = PQ \cap E$

Look at $f(X,Y,Z) = aX+bY+cZ$
the line through P and Q and R'

Recall $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ are affine coordinates

which you get by removing the point at infinity.

Consider $\operatorname{div}\left(\frac{f}{Z}\right) = \operatorname{div}(ax+by+c)$

Suppose $b \neq 0$ ($b=0$ similar)

CLAIM: $\operatorname{div}\left(\frac{f}{Z}\right) = P+Q+R'-3(O)$

In $\mathrm{Pic}^0(E)$, this is $((P)-(O))$
$+((Q)-(O))$
$+((R')-(O)) = O$

which in $E(\bar{K})$ means $P+Q+R' = O$,
hence $R' = R$.

Proof of CLAIM: Certainly the line passes through P, Q, and R' and so vanishes at them.

So f/z has zeroes at P, Q, R.
If two of them are equal count them separately using multiplicity.

By Bezout's Thm f/z has no other zeros

And has a pole at (0), which by degree considerations (deg div $= 0$) must be degree 3.

Hence $\operatorname{div}(f/z) = (P)+(Q)+(R)-3(0)$

We can describe this very abstract group structure in terms of a nice geometric operation.

- Algebraic closure of pts in ell. curves
- Sum is an alg. operation

HOMEWORK

Def: An Isogeny is a morphism
$f: E_1 \to E_2$ s.t. $f(0_1) = 0_2$
f could be constant
or f must be surjective
If f is surj., f is finite

$\mathrm{Hom}(E_1, E_2) = (\text{isogenies})$ ← group under addition

$\mathrm{End}(E) = \mathrm{Hom}(E, E)$ ← can endow with a ring structure with "+" composition

The ring structure of $\mathrm{End}(E)$ is very restricted and informative.

THEOREM: $\mathrm{End}(E)$ is an integral domain with characteristic 0

Pf: $f \circ g = 0$ Consider the degrees.

$\deg(f \circ g) = \deg f \times \deg g = 0$

So one of $\deg f, \deg g = 0$

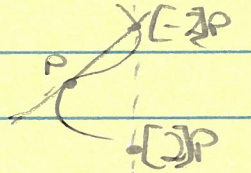
So one of f, g is 0 since a constant isogeny must be identically 0.

Pf: If $n \in \mathbb{Z} \subset \mathrm{End}(E)$

$[n](P) = P + P + \dots P$ n times

This is an isogeny of degree n^2

For instance $[2](P)$ is the line through P and P tangent



Check that for $n \neq 0$ $[n] \neq 0$

Observe that $\deg([n]) = n^2 \neq 0$

Work omitted: Proving $\deg[n] = n^2$

Examples of Isogenies:

Take $E = (y^2 = x^3 - x)$

$[\sqrt{-1}] : (x, y) \mapsto (-x, iy)$

Turns out $\mathbb{Z}[\sqrt{-1}] \subset End(E)$

Take $a+bi \longmapsto [a] + [b][\sqrt{-1}]$

Remark: Typically $End(E) = \mathbb{Z}$
(char $K = 0$)

The only other possibility is that $End(E)$ is a finite index lattice in the ring of integers of $\mathbb{Q}[\sqrt{-k}]$

In which case we say E has complex multiplication and is very Special.

$K = \mathbb{F}_q$

EXAMPLE: Let $char(K) = p$. Then the Frobenius morphism $\phi(x, y) = x^q, y^q$ is in fact an Isogeny from E/K to E/K of degree q.

THEOREM (DUAL ISOGENIES)

Let E_1, E_2 be elliptic curves

$\phi : E_1 \to E_2$ an isogeny

There exists an isogeny $\hat{\phi} : E_2 \to E_1$

s.t.

* $\hat{\phi} \circ \phi = [\deg \phi]$ on E_1
* $\hat{\hat{\phi}} = \phi$
* $\deg \hat{\phi} = \deg \phi$

Construction requires some machinery.

EXAMPLE: $\widehat{[n]} = [n]$

Check: $[n] \circ [n] = [n^2]$

$= [\deg [n]]$ ✓

FACT: If we take $f, g \in \mathrm{End}(E)$

$\widehat{f \circ g} = \hat{g} \circ \hat{f}$

$\widehat{f+g} = \hat{f} + \hat{g}$

ELLIPTIC CURVES over FINITE FIELDS

To show: $S_{E^{(s)}} = \dfrac{1 - a q^{-s} + q^{1-2s}}{(1-q^{-s})(1-q^{1-s})}$

$a = \#E(\mathbb{F}_q) - q - 1$

(1) $|a| < 2\sqrt{q}$

(2) Riemann hypothesis is satisfied

$$P(Z) = 1 - aZ + qZ^2$$

roots of $|a| = \sqrt{q}^{-1}$

(1) implies (2) immediately

PROOF: To show (1)

REMARK: $\phi(x,y) = (x^q, y^q)$

# of points on $E(\mathbb{F}_{q^n}) = \{\#(x,y) \in E \mid x,y \in \mathbb{F}_{q^n}$ i.e. $x^q = x, y^q = y\}$

in other words look at all points

$\{P \in E \mid \phi^n(P) = P\}$

$= \#\ker(1 - \phi^n)$

$= \deg(1 - \phi^n) = \#E(\mathbb{F}_{q^n})$

Show $|\#E(\mathbb{F}_q) - q - 1| < 2\sqrt{q}$

$= |\deg(1 - \phi) - q - 1|$ by DUAL ISOGENY

$= |(1 - \phi)(1 - \hat{\phi}) - q - 1|$

$= |(1 - \hat{\phi})(1 - \phi) - q - 1| = |(1 - \phi)(1 - \hat{\phi}) - q - 1|$

$= |1 - \hat{\phi}\phi - \hat{\phi} - \phi - q - 1| = |\phi + \hat{\phi}|$

$\deg \phi = q$

Pick $m, n \in \mathbb{Z} > 0$

$$0 \leq \deg(m - n\varphi)$$
$$= (m - n\hat{\varphi})(m - n\varphi)$$
$$= m^2 - mn(\varphi + \hat{\varphi}) + n^2 q$$
$$\varphi + \hat{\varphi} \leq \frac{m^2 + n^2 q}{mn} = \frac{m}{n} + \frac{n}{m} q$$

As $\frac{m}{n} \to \sqrt{q}$, $|\varphi + \hat{\varphi}| \leq \lim_{m/n \to \sqrt{q}} \frac{m}{n} + \frac{n}{m} q$

$$= 2\sqrt{q}$$

So $\varphi + \hat{\varphi} < 2\sqrt{q}$ □

We know $a = \#E(\mathbb{F}_q) - q - 1$

$|a| \leq 2\sqrt{q}$,

RH for $1 - aZ + qZ^2$

to show: $S_r(Z) = \frac{1 - aZ + qZ^2}{(1-Z)(1-qZ)}$

that this is the same a

For that, we have to do some indirect stuff

To do so, we introduce the number theory!

Def: If p is a prime, $E[p^n] = \{Q \in E \mid [p^n]Q = \mathcal{O}\}$

that is points on E that are p^n torsion

FACT: $E(p^n)$ is a rank 2 torsion-free $\mathbb{Z}/p^n\mathbb{Z}$-module

Def, can't If $Q \in E[p^n]$
then $\varphi(Q) \in E[p^n]$
for φ endomorphism

The TATE MODULE, denoted $T_p E$

$= \varprojlim E[p^n]$

And $\varphi \in End(T_p E)$ since φ acts on each object as you take the limit

FACT: $T_p E$ is a rank 2 free $\mathbb{Z}_p$: $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ - modules.

Suppose φ has eigenvalues α, β
Then φ^n has " α^n, β^n

Turns out: $\varphi^n + \hat{\varphi}^n = \alpha^n + \beta^n$
char poly. of $\varphi = (X-\alpha)(X-\beta)$
$\det \varphi = \deg \varphi = q$

Hence $\#E(\mathbb{F}_{q^n}) = 1 + q - (\alpha^n + \beta^n)$
Verify that $\zeta_E(Z) = \dfrac{1-(\alpha+\beta)Z+qZ^2}{(1-Z)(1-qZ)}$
by going to the def'n of ζ_E and using logarithms:

$$\log \zeta_E(z) = \sum_{n \geq 1} \frac{\#E(\mathbb{F}_{q^n}) z^n}{n}$$ and it works out...?

Turns out the Tate module also carries the action of Galois groups.