

Elliptic Curves

D. Zack Garza

March 13, 2020

Contents

1	Wednesday January 8	3
2	Mordell-Weil Groups	3
3	Monday January 13th	5
3.1	Every Abelian Group is a Class Group	5
3.2	Proof Sketch	5
3.2.1	Step 1	5
3.2.2	Step 2	6
3.2.3	Step 3	6
3.3	Mordell-Weil	7
4	Wednesday January 15th	8
5	Friday January 17th	10
5.1	Continuing Step 3	10
5.2	Step 4	11
6	Wednesday January 22nd	12
6.1	Step 1:	12
6.2	Step 2	13
7	Friday January 24th	14
7.0.1	Step 3	15
7.0.2	Step 4: Number Theory	17
8	Monday January 27th	18
8.1	Weak Mordell-Weil: Finishing the Proof	18
8.2	Height Functions	19
9	Wednesday January 29th	20
9.1	Height Functions	20
10	Friday January 31st	22
10.1	Height Functions	23

11 Monday February 3rd	24
12 Friday February 7th	26
12.1 Weil Height Machine	26
13 Wednesday February 12th	28
13.1 Correction to Weil's Height Machine	28
13.2 Néron-Tate Canonical Height	29
13.3 10 Cents of Dynamics	30
13.3.1 Important Examples	32
14 Friday February 14th	32
14.1 Canonical Heights	32
14.2 Quadratic Functions	33
15 Monday February 17th	35
16 Monday February 24th	38
16.1 Classification of Locally K -Analytic Lie Groups	38
17 Wednesday February 26th	40
17.1 (Clark-Xarles) Local Bounds for Torsion Points on Abelian Varieties	40
17.2 Good Reduction	41
17.3 Potentially Good Reduction	42
17.4 General Reduction	43
18 Friday February 28th	43
18.1 The Chevalley Decomposition	44
19 Friday March 6th	45

List of Definitions

3.1 Definition	6
15.1 Definition	36
17.1 Definition	41
17.2 Definition	42
18.1 Definition	45

List of Theorems

3.1 Theorem – Claborn - Leedham - Green - Clark	5
3.2 Theorem – Mordell-Weil	7
14.1 Theorem	32
14.6 Theorem – Canonical Height Descent	35
14.7 Theorem	35
15.1 Theorem	35

15.2 Theorem	36
16.1 Theorem – C-Lacy	38
17.1 Theorem – Weil, Serre Improved Weil Bounds	41
17.3 Theorem – C-Xarles	42
18.1 Theorem – Lestra-Oort	45
18.2 Theorem – Clark-Xarles	45
19.1 Theorem – Tate, Part A	46
19.2 Theorem – Tate, Part B	46
19.3 Theorem – Tate, Part C	47
19.4 Theorem – Tate, Part D	47
19.5 Theorem – Tate, Part E	47

1 Wednesday January 8

Summary:

1. Mordell-Weil theorem
 - For elliptic curves over global fields (number fields, function fields, finite fields, etc)
 - Proof uses Galois cohomology and height functions, essentially one proof!
 - Holds for abelian varieties, but more difficult (need an analog of height functions, i.e. an x -coordinate)
2. Height functions (possibly)
3. Elliptic curves over \mathbb{Q}_p or complete discrete valuation fields (see Silverman for basics, possibly Chapter 5), particularly Tate curves
4. Weil-Chatelet groups E/k related to $H^1(k; E)$ with coefficients in the elliptic curve
5. Galois representation of E/k for char $k = 0$, for $\rho_n g_k \rightarrow \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$ which leads to $\hat{\rho} : g_k \rightarrow \mathrm{GL}(\hat{\mathbb{Z}})$.

2 Mordell-Weil Groups

Let E/k be an elliptic curve over a field k , i.e. a smooth, projective, geometrically integral curve of genus 1 with a k -rational point O .

Note: Silverman good for foundations, but assumes k is perfect! Here we'll assume k is arbitrary.

Remark: If k is not algebraically closed, such a point O may not exist.

By Riemann-Roch (easy computation) E embeds (non-canonically) into \mathbb{P}^2/k as a Weierstrass cubic

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \Delta \neq 0.$$

This is a smoothness condition, and this equation has a k -rational point at infinity $[0 : 1 : 0]$. The line at infinity is a flex line (?), and so only intersects this curve at one point.

If char $k \neq 2, 3$ then $y^2 = x^3 + Ax + B$.

Every elliptic curve is given by a Weierstrass equation, although not in a unique way.

An amazing fact: The k -rational points $E(k)$ forms an abelian group with zero as the identity.

Proof:

1. Given any plane cubic C/k and an origin $O \in C(k)$, the chord and tangent process yields a group structure. Note that there is a symmetry in connecting rational points a, b with a line intersecting at another rational point c which is not present in most groups, so an additional inversion about O is needed to actually make this into a group. Proving associativity: difficult!
2. Look at $\text{Pic}^0 E$, the degree 0 divisors on E mod birational equivalence (?), which is equal to the degree 0 line bundles on E mod bundle isomorphism.

Exercise: Show there is a map $C(k) \rightarrow \text{Pic}^1 C$ given by sending p to its equivalence class; this is a bijection by Riemann-Roch (straightforward exercise).

We can then compose this with a map $\text{Pic}^1 \rightarrow \text{Pic}^0 C$ given by $D \mapsto D - [O]$, which decreases the degree by 1. This gives a map $\Phi : C(k) \rightarrow \text{Pic}^0 C$, just need to check that $\Phi(P \oplus Q) = \Phi(P) + \Phi(Q)$.

Check that the groups are independent of the k -rational point chosen, i.e. changing rational points yields isomorphic groups. So the group law itself does actually depend on the rational point, although the structure doesn't.

Exercise: Let $(E, O)/k$ be an elliptic curve and define $E^0 = E \setminus \{O\}$ the (nonsingular, integral) affine curve given by removing the point at infinity. Then the affine coordinate ring $k[E^0]$ is defined as $k[x, y]/(y^2 - x^3 - Ax - B)$, which is a Dedekind ring.

The interesting thing about Dedekind domains: the ideal class group! (i.e. the Picard group)

This has ideal class group $\text{Pic}^0 E$, and one can show that

$$\begin{aligned} \text{Pic}^0 E &\longrightarrow \text{Pic}^0 k[E^0] \\ \sum_p n_p \deg(p)[p] &\mapsto \sum_{p \neq 0} n_p [p] = \prod_p p^{n_p} \end{aligned}$$

with the sum ranging over all closed points is an isomorphism.

Just note that the RHS can't have a point at infinity, so we just forget it. The isomorphism follows from some exact sequence with correction terms that vanish.

So the Mordell-Weil group of $E(k)$ is isomorphic to $\text{Pic}^0 E$, the class group of a Dedekind domain (?).

Definitions: Let G be a commutative group.

- G is a *class group* iff there exists a Dedekind domain R such that $G \cong \text{Pic} R$.
- G is an (*elliptic*) *Mordell-Weil group* iff there exists a field k and an elliptic curve E/k such that $G \cong E(k)$.

Questions:

1. Which G are class groups?
2. Which G are Mordell-Weil groups?

An answer to question 1:

Theorem (Clayborn, 1966): Every commutative G is a class group.

Subsequent proofs: Leetham-Green (1972) and Clark (2008) following Rosen, and uses elliptic curves. See the end of Pete's Commutative Algebra notes!

An answer to question 2:

Consider E/\mathbb{C} , then $E(\mathbb{C}) \cong S^1 \times S^1$, so the torsion subgroup is $T(1) := (\mathbb{Q}/\mathbb{Z})^2 = \bigoplus_{\ell} (\mathbb{Q}_{\ell}/\mathbb{Z}_{\ell})^2$.

This in fact holds for any algebraically closed field of characteristic zero.

Fact: For any E/k , the Mordell-Weil group $E(k)$ is “ $T(1)$ -constrained”, i.e. $E(k)[\text{tors}] \hookrightarrow T(1)$.

Theorem (Clark, 2012): G is a Mordell-Weil group $\iff G$ is $T(1)$ -constrained.

Note: the analogous statement for abelian varieties, i.e being $T(g)$ constrained for some other genus $g \neq 1$, is open. Fixing $k = \mathbb{Q}$ still yields very interesting problems. Computing the rank and torsion subgroups is currently open, and the subject of modern research.

3 Monday January 13th

3.1 Every Abelian Group is a Class Group

Theorem 3.1 (Claborn - Leedham - Green - Clark).

Any commutative group is the class group of some Dedekind domain.

Also see: partial re-proof by Rosen that uses elliptic curves. This theorem: mostly a proof in commutative algebra, see end of Pete's commutative algebra notes.

3.2 Proof Sketch

Let E/k be an elliptic curve over a field.

3.2.1 Step 1

Note that $\text{End}_k(E) \cong_{\mathbb{Z}} \mathbb{Z}^{a(E)}$ where $a(E) \in \{1, 2, 4\}$.

Could be \mathbb{Z} as a \mathbb{Z} -module, could be an order in the imaginary quadratic field (e.g. a quaternion algebra)

There is a short exact sequence

$$0 \longrightarrow E(k) \longrightarrow E(k(E)) \longrightarrow \text{End}_K(E) \longrightarrow 0.$$

This splits because (as seen above), the RHS term is free and thus projective. So

$$E/k(E) \cong E(k) \oplus \mathbb{Z}^{a(E)}.$$

Note that $k(E)$ is an extension of E_k to $E_{k(E)}$ the field of rational functions over k ? (function field). To simplify, take $a(E) = 1$ and $E(k) = \{0\}$.

Taking $k = \mathbb{Q}$, this happens (probably, asymptotically) half of the time. It's easy to write down an elliptic curve that satisfies these conditions

Then $E/k(E) \cong \mathbb{Z}$.

Now pass to the field of rational functions over this field, taking $E(k(E)/k(E))$. Then $k^2(E) := k(E)(E/k(E))$, and inductively define $k^n(E)$ by passing to function fields. So $E(k^n(E)) \cong \mathbb{Z}^n$.

So we can construct elliptic curves that have any free commutative group as their Mordell-Weil group.

3.2.2 Step 2

Loosely speaking, we'll iterate this process transfinitely. Then for any set S , there exists a field k and an elliptic curve E/k such that $E(k) \cong \bigoplus_S \mathbb{Z}$. We now want to introduce a process that allows passing to quotients. And $R := k[E^0]$ is the affine coordinate ring of E , remove the point at infinity (?).

3.2.3 Step 3

Let R be a Dedekind domain. Note it has a fraction field with a certain ideal class group. Let $W \subset \max\text{Spec}(R)$, then

$$R^W := \bigcap_{\mathfrak{p} \in \max\text{Spec}(R) \setminus W} R_{\mathfrak{p}}.$$

Then R^W is Dedekind (and every overring of a Dedekind domain is of this form) and $\max\text{Spec}(R^W) = \max\text{Spec}(R) \setminus W$.

Then

$$\text{Pic}(R^W) = \text{Pic}(R) / \langle [\mathfrak{p}] \mid \mathfrak{p} \in W \rangle.$$

Note that if $(A, +)$ is a commutative group, writing $A = \bigoplus_S \mathbb{Z}/H$, we have a Dedekind domain $R = k[E^0]$ such that $\text{Pic}(R) = \bigoplus_S \mathbb{Z}$.

Note: $\text{Pic}(R)$ is the class group.

Definition 3.1.

A Dedekind domain R is **replete** iff every element of the class group $\text{Pic}(R)$ is the class group $[\mathfrak{p}]$ of some ideal $\mathfrak{p} \in \max\text{Spec}(R)$.

Is every ideal class the class of a prime ideal? For k a field, $R = \mathbb{Z}_k$. This follows from Chebotom (?) Density (most important theorem for arithmetic geometers!)

Definition: A Dedekind domain R is **weakly replete** iff every subgroup $H \subset \text{Pic}(R)$ is generated by classes of prime ideals.

Exercise (Easy) $K[E^0]$ is weakly replete, and an easy application of Riemann-Roch shows that if $0 \neq p \in E(k) = \text{Pic}(k[E^0])$, then $[p] \in \text{Pic}(k[E^0])$ is generated by a prime ideal.

Note: most applications of Riemann-Roch to elliptic curves are easy! In this case, it gives you an identification $E \cong \text{Pic}^1(E)$.

So there exists a subset $W \subset \max\text{Spec } k[E^0]$ such that $\langle [p] \mid p \in W \rangle = H$. Then

$$\text{Pic } k[E^0]^W \cong \bigoplus_S \mathbb{Z}/H \cong A.$$

■

Note that Dedekind domains don't have to be replete or even weakly replete. The class group of a Dedekind domain could be \mathbb{Z} , and the class of every prime ideal could be $1 \in \mathbb{Z}$

Proof (Claborn).

Start with an arbitrary Dedekind domain R and attach one that's replete.

Can ask for a similar result for abelian varieties, there are conjectures here, few clear results. Need to get $\mathbb{Z}/(m) \times \mathbb{Z}/(n)$, since these occur as Mordell-Weil groups. Take a modular curve and a generic point. Look at universal elliptic curves over elliptic curves and take their Mordell-Weil groups (?)

If k is algebraically closed and $\text{char } k = p$, can't have $\mathbb{Z}(p) \times \mathbb{Z}/(p)$. Consider the p -primary torsion $E_k[p^\infty]$. It is zero iff E is supersingular (no points of order p). It is $\mathbb{Q}_p/\mathbb{Z}_p = \varinjlim_n \mathbb{Z}/(p^n)$ iff E is ordinary.

Can sometimes reduce to cases where $k = \mathbb{C}$ and do things analytically.

■

3.3 Mordell-Weil

Theorem 3.2 (Mordell-Weil).

Let k be a global field (extension of \mathbb{Q} or function field over \mathbb{F}_p) and E/k an elliptic curve. Then $E(k) \cong \mathbb{Z}^r \oplus T$ (by classification of abelian groups) where T is finite, and $T \cong \mathbb{Z}/(m) \oplus \mathbb{Z}/(n)$ for $m \mid n$. So T is generated by at most two elements.

Proof (3 steps).

Step 1: Weak Mordell-Weil theorem.

Take any $n \geq 2$ and $\text{char } k$ not dividing n . Show that $E(k)/nE(k)$ is finite.

Step 2: Define a height function $h : E(k) \rightarrow \mathbb{R}$ satisfying 3 properties (see next time). This is approximately a quadratic form.

Decompose at places of a number field, see Number Theory II.

Step 3: For any commutative group A , there is a notion of a height function $h : A \rightarrow \mathbb{R}$. Show the Height Descent Theorem: if A admits a height function and A/nA is finite for some $n \geq 2$, then A is finitely generated.

Also how you'd prove this theorem for abelian varieties, more difficulty defining h .

■

4 Wednesday January 15th

Recall that we're trying to prove the Mordell-Weil theorem. Let K be a global field, so it's the field of functions over some nice curve. Then the Mordell-Weil group $E(K)$ is finitely generated.

Step 1: The weak Mordell-Weil theorem for all $n \geq 2$ with $\text{char } k$ not dividing n , $E(k)/nE(k)$ is finite.

Step 2: Construction of a height function $h : E(K) \rightarrow \mathbb{R}$ that is "trying" to be a quadratic form.

Step 3 (Today): The Height Descent Theorem, i.e. if $(A, +)$ is a commutative group such that A/nA is finite for some $n \geq 2$ and it admits a height function $h : A \rightarrow \mathbb{R}$, then A is finitely generated.

Question: What does the weak Mordell-Weil group $E(K)/nE(K)$ tell us about $E(K)$?

Note that we'll inject this into a larger group, which we'll show is finite, but this isn't great for learning about the size.

Example: Consider E/\mathbb{C} , then $E(\mathbb{C}) = S^1 \times S^1$ and $E(\mathbb{C})/nE(\mathbb{C}) = 0$, so the map $x \rightarrow nx$ is a surjective map and $E(K)$ is n -divisible here. In general, whenever $K = \overline{K}$ is algebraically closed, then $x \mapsto nx$ is again surjective and the weak Mordell-Weil group is trivial. So knowing this is small doesn't tell us much about $E(K)$ at all.

Example: For E/\mathbb{R} , $E(\mathbb{R})$ is either S^1 (cubic with one real root, $\Delta = 0$) or $S^1 \times \mathbb{Z}/(2)$ (cubic with three real roots, $\Delta > 0$) are the two possible group structures.

Then

$$\begin{cases} 0 & n \text{ odd} \\ 0 & n \text{ even and } \Delta < 0 \\ \mathbb{Z}/(2) & n \text{ even and } \Delta > 0 \end{cases}$$

Example: Consider E/\mathbb{Q}_p , then for all $\ell \gg 0$ $E(\mathbb{Q}_p) \xrightarrow{[\ell]} E(\mathbb{Q}_p)$ with $E(\mathbb{Q}_p)/\ell E(\mathbb{Q}_p) = 0$ while $E(\mathbb{Q}_p)/pE(\mathbb{Q}_p)$ is not zero.

Note: here is an example of a Boolean space, that ends up being homeomorphic to a Cantor set.

Suppose $E(K)$ is finitely generated, so $E(K) \cong \mathbb{Z}^r \oplus T$ with T finite. Then knowing $E(K)/nE(K)$ gives an upper bound on r .

Example: Take $n = 2$, then $E(K)/nE(K) \cong (\mathbb{Z}/(2))^s$ for some $s \in \mathbb{N}$. Then $(\mathbb{Z}^r \oplus T)/2(\mathbb{Z}^r \oplus T) \cong (\mathbb{Z}/(2))^r \oplus T/2T$ for $r \leq s$. Then either

- $r = 2$ and $E(K[2]) = (0)$.
- $r = 1$ and $E(K[2]) \cong \mathbb{Z}/(2)$,
- $r = 0$ and $E(K[2]) \cong (\mathbb{Z}/(2))^2$.

Note that we don't need the Mordell-Weil theorem to compute the torsion subgroups of $E(k)$. It is often easier to compute these directly. For all non-archimedean places v of K , $E(K_v)[\text{tors}]$ is finite (see Silverman?) and embeds into a number of finite things.

To compute $E(K_v)[\text{tors}]$,

1. Find $N \in \mathbb{Z}^+$ such that $E(k)[\text{tors}] \subset E[N]$.
 - Choose 2 different places v_0, v_1 of good reduction (from Weierstrass equation) with different residue characteristics $\ell_1 \neq \ell_2$
 - Consider the map $E(K_{v_i})[\text{tors}] \rightarrow E(\mathbb{F}_{v_i})$
 - The kernel is a finite p_i -primary group.
 - Comes down to torsion and formal groups, see first course.
2. Compute $E[N](K)$ (several algorithms, just checking for rational points on a zero-dimensional variety?)

See division polynomials, can check for roots of polynomials over any global field. Easy to check for rational points on finite fields.

Suppose $E(K) \cong \mathbb{Z}^r \oplus T$ is finitely generated and we know $E(K)/nE(K)$ for some n and we know T . Then we explicitly know r .

See Tate Shafarevich group – important! But difficult, a piece of information that helps compute the rank (?).

Definition: Fix $n \geq 2$. An n -height function on $(A, +)$ is a map $h : A \rightarrow \mathbb{R}$ satisfying

1. For all $R \geq 0$, the set $h^{-1}((-\infty, R])$ is finite.
2. For all $Q \in A$, there exists a $C_2 = C_2(A, Q)$ such that for all $P \in A$, $h(P + Q) \leq 2h(P) + C_2$.
(?)
3. There exists a $C_3 = C_3(A, n)$ such that for all $P \in A$, $h(nP) \geq n^2h(P) - C_3$

Note: (3) would be an equality for an honest quadratic function, so this deviates in a controlled way.

Theorem (Height Descent): Let $(A, +)$ be a commutative group with an n -height function $h : (A, +) \rightarrow \mathbb{R}$. If A/nA is finite, then A is finitely generated.

Proof: Let r be the size of A/nA . Choose coset representatives Q_1, \dots, Q_r of nA in A . Let $p \in A$ and define a sequence $\{P_k\}_{k=0}^\infty$ in A by $P_0 = P$ and for $k \geq 1$, choose P_k such that $P_{k-1} = nP_k + Q_{i_k}$.

Then for all $k \in \mathbb{Z}^+$, it's true that $P = n^k P_k + \sum_{j=1}^k n^{j-1} Q_{i_j}$.

Claim: There exists a constant $c > 0$ depending only on A, n such that for all $P \in A$, there exists a $K = K(P)$ such that for all $k \geq K$, we have $h(P_k) \leq 0$.

Note that this is sufficient – if so, A is generated by $\{Q_1, \dots, Q_r\} \cup h^{-1}((-\infty, C])$, which are both finite.

Next time: proof of claim.

Note: similar setup goes through for abelian varieties, see Néron–Tate height canonical height, which yields an honest “quadratic form”.

5 Friday January 17th

5.1 Continuing Step 3

Recall the Height Descent Theorem (see previous notes). Most important property of height function: the collection of elements under a given height is finite.

Note that A/nA is the cokernel of multiplication by n .

Proof: Let r be the size of A/nA and choose coset representatives Q_1, \dots, Q_r . For $P \in G$ (?) define $P_0 = P$ and P_k such that $P_{k-1} = nP_k + Q_i$ for any i .

For all positive $k \in \mathbb{Z}$, we have $P = n^k P_k + \sum n^j Q_i$.

Claim: There exists a $c > 0$ such that for all $P \in A$ there exists a $K = K(P)$ such that for all $k \geq K$, $h(P_k) \leq C$. If this holds, A is generated by $\{Q_i\} \cup h^{-1}((-\infty, C])$.

Proof of claim: Let $c_2 = \max_{1 \leq i \leq r} c_2(-Q_i)$.

Then

$$\begin{aligned} h(P_k) &\leq \frac{1}{n^2}(h(nP_k) + c_3) \\ &= \frac{1}{n^2}(h(P_{k-1} - Q_i) + c_3) \\ &\leq \frac{1}{n^2}(2h(P_{k-1}) + c_2 + c_3) \\ &\leq \frac{1}{n^2} \left(\frac{2}{n^2}(2h(P_{k-1}) + c_2 + c_3) + c_2 + c_3 \right) \quad \text{by repeating} \\ &= \left(\frac{2}{n^2} \right)^2 h(P_{k-2}) + \left(1 + \frac{2}{n^2} \right)(c_2 + c_3) \\ &= \left(\frac{2}{n^2} \right)^k h(P) + \frac{1}{n^2} \left(1 + 2/n^2 + (2/n^2)^2 + \dots + (2/n^2)^{k-1} \right)(c_2 + c_3) \\ &\leq \left(\frac{2}{n^2} \right)^k h(P) + \left(\frac{1}{1 - \frac{2}{n^2}} \right)(c_2 + c_3), \end{aligned}$$

where the last inequality follows because $n \geq 2$ implies the leading term is bounded by 1 and the middle term contains a convergent series.

This proves the claim for any n . ■

Definition: A function $h : A \rightarrow \mathbb{R}$ from a commutative group is *quadratic* if the associated function $h(x + y) - h(x) - h(y) := B_h : A^2 \rightarrow \mathbb{R}$ is bilinear. The function h is *linear* iff B_h is constant.

The function h is a *quadratic form* iff h is quadratic and for all $m \in \mathbb{Z}$ and for all $x \in A$, $h(mx) = m^2 h(x)$.

I.e. a degree 2 homogeneous function.

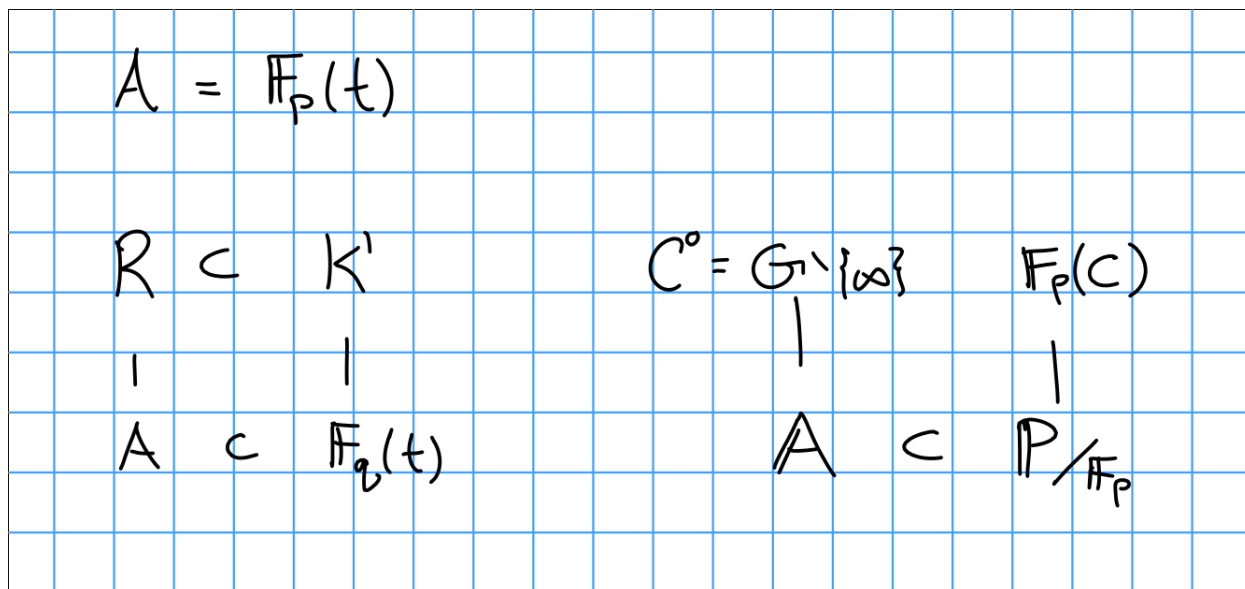


Figure 1: Image

Theorem (Canonical Height Descent): Suppose $(A, +)$ is commutative and $h : A \rightarrow \mathbb{R}$ is a quadratic form. Suppose

1. A/nA is finite, and
2. $h^{-1}((-\infty, R])$ is finite for all R ,

then letting $y_1, \dots, y_r \in A/nA$ be coset representatives and taking $C = \max h(y_i)$, we can conclude that A is generated by $\{x \in A \mid h(x) \leq C\}$.

5.2 Step 4

Theorem (Abstract Weak Mordell-Weil):

Let k be a field, E/k an elliptic curve, choose n such that $\text{char } k$ doesn't divide n , and let $k' := k(E[n])$ be k with the n -torsion points of E adjoined. Note that this adjoins finitely many algebraic points to k .

Suppose there exists a Dedekind domain R with fraction field k' with finite class group, so $\text{Pic}(R) < \infty$, and R^\times is finitely generated. Then $E(k)/nE(k)$ is finite.

Corollary: Let k be a global field $n \geq 2$, then $E(k)/nE(k)$ is finite.

Proof: k is a number field, so is k' . Pick $k' = \mathbb{Z}_k$, which is a Dedekind domain. By Number Theory I, the hypotheses above are satisfied.

If k is a function field, $k/\mathbb{F}_p(t)$ is finite and separable, so $k'/\mathbb{F}_p(t)$ is finite and separable. For $A = \mathbb{F}_p(t)$, $A \subset \mathbb{F}_q(t)$, then take $R/A \subset k'/\mathbb{F}_q(t)$ the integral closure of A in k' . By Number Theory I, R is a Dedekind domain.

Then $R = \mathbb{F}_p[C^0]$, and by Number Theory II, $\text{Pic}(R)$ is finite.

Removing primes makes unit group larger and the class group smaller.

Localizing at a prime ideal yields a DVR? This kills the Picard group (since it's a PID?) but blows up the units group.

Note that the proof for abelian varieties adapts very easily.

■

Sketch of proof:

Step 1: Reduce to the case that E has full n -torsion, i.e. $k' = k$. If L/k is finite Galois (as is k'/k), and $E(L)/nE(L)$ is finite, then $E(k)/nE(k)$ is finite.

Remark: For any extension L/k , there is an injection $E(k) \hookrightarrow E(L)$, but $E(k)/nE(k)$ need not inject into $E(L)/nE(L)$. For counterexamples, take $k = \mathbb{R}$ and \mathbb{C}/k , then $E(\mathbb{C})/nE(\mathbb{C})$ can be trivial.

Step 2: Let $L := k([n]^{-1}E(k))$ be the compositum $k[\{P\}]$ over the $P \in E/\bar{k}$ such that $[n]P \in E(k)$ is k -rational. It's straightforward to show that L is separable and Galois (it is an étale covering). That it's Galois: if $[n]P$ is rational, so is $[n]\sigma(P)$ for any σ in the Galois group. We'll show that this is a finite extension.

Step 3: Construct a Kummer pairing to show that finiteness of $[L : k]$ is equivalent to $E(k)/nE(k)$ being finite.

Step 4: Reduce finiteness of $[L : k]$ to algebraic number theory.

6 Wednesday January 22nd

Theorem (Stronger Weak Mordell-Weil:) Let $n \geq 2$, k a field, $\text{char}(K)$ not dividing n , E/k an elliptic curve $K := K(E[n])$.

Suppose there exists a Dedekind domain R with fraction field K such that

- $\text{Pic } R[n]$ is finite
- The cokernel of $x \mapsto nx$ is finite

Then $E(K)/nE(K)$ is finite.

Exercise: Take $k = \bar{k}$, C/k a “nice” affine curve, $R = k[C]$, $K = k(C)$, $\text{char}(k)$ not dividing n . Show that if E/k is any elliptic curve, then the hypotheses of Stronger Weak Mordell-Weil hold, as does the conclusion, and in fact $E(K)$ need not be finitely generated.

Uses ANT II.

6.1 Step 1:

Let L/K be a Galois extension and consider $\iota : E(K)/nE(K) \rightarrow E(L)/nE(L)$. This is not injective in general, and in fact $\ker(\iota) = (E(K) \cap nE(L))/nE(K)$.

Proposition:

- a. There exists a map $\ker \iota \rightarrow \text{Maps}(g_{L/K}, E[n])$, where $g_{L/K}$ is the Galois group of L/K .
- b. If L/K is finite, then $\ker \iota$ is finite

So if $E(L)/nE(L)$ is finite, then $E(K)/nE(K)$ is finite.

Proof: Let $p \in E(K) \cap nE(K)$. Choose $Q_p \in E(L)$ (only determined up to an n -torsion point) such that $[n]Q_p = p$. For all $\sigma \in g_{L/K}$ we have

$$[n](\sigma(Q_p) - Q_p) = \sigma([n]Q_p) - [n]Q_p = \sigma(p) - p = 0.$$

Thus $\sigma(Q_p) - Q_p \in E[n]$.

Note: this resembles a certain coboundary map in a cohomology theory.

We then associate a map

$$\begin{aligned} \lambda_p : g_{L/K} &\longrightarrow E[n] \\ \sigma &\mapsto \sigma(Q_p) - Q_p. \end{aligned}$$

Suppose that for $p, p' \in E(K) \cap nE(L)$, so $\lambda_p = \lambda_{p'}$. Then for all $\sigma \in g_{L/K}$, we have

$$\sigma(Q_p - Q_{p'}) = \sigma(Q_p) - Q_p - (\sigma(Q_{p'}) - Q_{p'}) + (Q_p - Q_{p'}) = \lambda_p(\sigma) - \lambda_{p'}(\sigma) + Q_p - Q_{p'} = Q_p - Q_{p'}.$$

So $Q_p - Q_{p'} \in E(K)$, and thus $p - p' = [n](Q_p - Q_{p'}) \in nE(K)$. Thus $\ker \iota = \frac{E(K) \cap nE(L)}{nE(K)}$.

From now on, we'll assume $K = K' = K(E[n])$.

6.2 Step 2

Define the Kummer pairing.

Let $L = K^{\text{sep}}$ and take $p \in E(K)$ such that $[n]Q_p = p$, and define

$$\begin{aligned} \lambda_p : g_K &\leq \text{Aut}(K^{\text{sep}}/K) \longrightarrow E[n] \\ \sigma &\mapsto \sigma(Q_p) - Q_p. \end{aligned}$$

Note that since $E[n] = E[n](K)$, this no longer depends on the choice of Q_p .

Define a Kummer pairing

$$\begin{aligned} \kappa : E(K) \times g_K &\longrightarrow E[n] \\ (p, \sigma) &\mapsto \sigma Q_p - Q_p. \end{aligned}$$

Proposition: This pairing satisfies the following properties:

1. For all $p, q \in E(K)$ and $\sigma \in g_K$, $\kappa(p + q, \sigma) = \kappa(p, \sigma) + \kappa(q, \sigma)$
2. For all $p \in E(K)$ and $\sigma, \xi \in g_K$, $\kappa(p, \sigma\xi) = \kappa(p, \sigma) + \kappa(p, \xi)$.
3. For all $p \in E(K)$, we have $\kappa(p, \sigma) = 0$ for all σ iff $p \in nE(K)$.
4. For all $\sigma \in g_K$, we have $\kappa(p, \sigma) = 0$ for all $p \in E(K)$ iff $\sigma \in g_L$ where $L := K([n]^{-1}E(K)) = K(Q_p/P \in E(K))$. So κ induces group homomorphisms

$$g_K/g_L = g_{L/K} \hookrightarrow \text{hom}(E(K)/nE(K), E[n])$$

$$E(K)/nE(K) \hookrightarrow \text{hom}(g_{L/K}, E[n]).$$

Thus $E(K)/nE(K)$ is finite iff $g_{L/K}$ is finite iff $[L : K]$ is finite.

Thus $g_{L/K}$ is abelian of exponent dividing n . So we can study this using Kummer theory and class field theory.

Proof of 1: Can take $Q_{p+p'} = Q_p + Q_{p'}$, which is a fine choice, and then $\kappa(p+p', \sigma) = \kappa(p, \sigma) + \kappa(p', \sigma)$.

Proof of 2:

$$\begin{aligned} \kappa(p, \sigma\xi) &= \sigma\xi Q_p - Q_p - \sigma\xi Q_p - \sigma Q_p + \sigma Q_p - Q_p \\ &= \sigma(\xi Q_p - Q_p) + \kappa(p, \sigma) = \sigma(\kappa(p, \xi) + \kappa(p, \sigma)) \\ &= \kappa(p, \xi) + \kappa(p, \sigma). \end{aligned}$$

Proof of 3: For $\sigma \in g_K$, then $\kappa(E(K), \sigma) = (0)$ iff $\sigma Q_p - Q_p = 0$ for all $P \in E(K)$ iff σ pointwise fixes L iff $\sigma \in g_L$.

Exercise: Replace E/k with A/k a commutative group scheme such that $[n] : A \rightarrow A$ is etale and $A[n]$ is finite. The proof goes through without modification if $\text{char } k$ doesn't divide n and A/k is an algebraic group, reduced, and of finite type.

Exercise: Take $A = \mathbb{G}_m$, the multiplicative group of K . Then $A(K)/nA(K) = K^\times/K^{\times n}$. Suppose K contains n th roots of unity, then regular Kummer theory gives a map $K^\times/K^{\times n} \cong \text{hom}(g_K, \mu_n)$ where μ_n are n th roots of unity.

This says that $K^\times/K^{\times n} = \chi(g_{L/K})$ where L is the maximal abelian extension of K of exponent dividing n , and $\chi(\cdot) = \text{hom}(\cdot, \mathbb{Z}/n\mathbb{Z})$, i.e. these are Pontryagin duals.

So far, works for any algebraic group, but we'll need properness later.

7 Friday January 24th

Let K be a field, $n \geq 2$ with $\text{char } k$ not dividing n , and A/K a commutative algebraic group (includes abelian varieties, additive/multiplicative groups, etc). Assume that K contains all n th roots of unity (we showed that this can be assumed).

Let $L := K([n]^{-1}A(K)) = K(\{Q \in A(K^{\text{sep}}) \mid [n]Q \in A(K)\})$. We've shown that L/K is Galois, and moreover abelian of exponent dividing n and L/K is finite iff $A(K)/nA(K)$ is finite.

Take $K = \mathbb{Q}$, then $\mathbb{Q}[p]$ for every p gives infinite extensions.

We want to show that if $A = E$ is an elliptic curve (or an abelian variety) and K is the fraction field of some Dedekind domain R with some finiteness condition on $\text{Pic}(R)$ and R^\times , then L/K is finite.

7.0.1 Step 3

Let $\mathfrak{p} \in \max\text{Spec}(R)$ with \mathfrak{p} not dividing n such that E has good reduction at \mathfrak{p} .

Take an R -integral Weierstrass equation W/R for E , then the discriminant satisfies $\Delta(W) \neq 0$. So just exclude the (finitely many) primes where $\mathfrak{p} \mid \Delta(W)$. For abelian varieties, reducing the equations mod p can result in singularities for only finitely many p .

Then L/K is unramified at \mathfrak{p} (i.e. it's ramified at only finitely many primes).

Proof: We have

$$L = \prod_{Q \mid n[Q]=P \in E(K)} L(Q)$$

as a compositum of extensions, so it's enough to show that

$$L_p := \prod_{[n]Q=p, p \in E(K)} K(Q)$$

is unramified over K .

Take integral closures:

Take the inertia group

$$I := I(\mathfrak{p} \mid p) = \left\{ \sigma \in g_{L_p/k} \mid \sigma(\mathfrak{p}) = \mathfrak{p}, \sigma \curvearrowright S_p/\mathfrak{p} = \text{id} \right\} \in \text{Aut}(L_p/K).$$

We want to show that $\forall \sigma \in I, \sigma(Q) = Q$. We have

$$0 = \sigma(P) - P = \sigma([n]Q) = [n]Q = [n](\sigma Q - Q)$$

and thus $\sigma Q - Q \in E[n] = E[n](K)$.

We now introduce the reduction map

$$r : E(L_p) \longrightarrow \tilde{E}(S/\mathfrak{p}),$$

where we use the fact that we can complete at \mathfrak{p} and then take a reduction to obtain a map $E(L_p) \longrightarrow E(\hat{L}_p) \longrightarrow \tilde{E}(S/p)$, which is where we use the fact that the reduction is good.

We know $\sigma Q - Q$ is n -torsion. Then r is a homomorphism, so $r(\sigma Q - Q) = r(\sigma Q) - r(Q) = 0$ by the definition of the inertia group. So $\sigma Q - Q$ is an n -torsion point in the kernel of the reduction map.

Fact from elliptic curves I (Silverman Ch. 7), the only torsion in the kernel of the reduction map is $\text{char}(S/p)$ -primary torsion. Since $\text{char}(S/p)$ does not divide n here, $\ker r = 0$, so $\sigma Q = Q$. ■

In the case of abelian varieties: The kernel of a good reduction is a formal group law of g dimensions. Reference: Prop 3.1, Clark and Xales (?) 2001. Here is where it doesn't work for \mathbb{G}_m . Projective variety: clear denominators for the fraction field, now need to look at integral points?



Figure 2: Image

7.0.2 Step 4: Number Theory

Let $S \subset \max\text{Spec } (R)$ be the finite set of p such that $p \mid n$ (using global characteristic assumption here) or E has bad reduction at p . Then take $L = K([n]^{-1}E(K))$. We know L/K is abelian of exponent dividing n , and is a compositum of extensions L_Q , each of bounded degree at most n^2 , each unramified outside of S .

Q is an n division point of something k rational. Multiplication by n has degree n^2 , so $[K_Q : K] < n^2$.

Theorem (Hermite - Minkowski): Let $d \in \mathbb{Z}^+$, K a number field, $s \subset \max\text{Spec } \mathbb{Z}_l$ finite. Then $|\{ L/K \text{ of degree } d \text{ unramified outside of } S \}| < \infty$.

One of a few finiteness theorems in elliptic curves/NT, probably the hardest one. Galois extension like branched cover, too few preimages. Take surface with marked points (corresponding to prime) and take all branched covering spaces that fix the degree and only ramify at those points. I.e. take unramified coverings. Then π_1 is free and f.g., which is the analogy here.

Proof: See Neukirch Ch. 3, 2.13, or Milne's ANT Theorem 8.42. Use Hermite's theorem that any given $\Delta \in \mathbb{Z}$ can only be the discriminant $\Delta(K)$ for finitely many K .

If K is a number field, then take $R = \mathbb{Z}_K$ and we're done.

Otherwise, let $R_s := \bigcap_{\mathfrak{p} \in \max\text{Spec } (R \setminus S)} R_{\mathfrak{p}}$. Then R_s is a Dedekind domain, $\max\text{Spec } R_s = \max\text{Spec } (R \setminus S)$. Also $\text{Pic } (R_s)$ is a quotient $\text{Pic } (R) / \langle [\mathfrak{p}] \mid \mathfrak{p} \in S \rangle$.

Assume $\text{Pic } R$ is finitely generated, then so is $\text{Pic } R_s$. If so, by enlarging S , we can make R_s a PID.

Note R_s is not necessarily a localization, although it could be, so we expect the unit group to get bigger.

Theorem (Pete's CA Notes Lemma 23.4): Let R be a Dedekind domain and $R \subset T \subset K$. Then

- a. T^\times / R^\times is torsion-free.
- b. Let $\mathfrak{p} \in \max\text{Spec } ?$ and define $T := \bigcap_{q \neq \mathfrak{p}} R_q$. TFAE:
 - $T^\times / R^\times = \mathbb{Z}$.
 - $T^\times \supsetneq R^\times$.
- c. $[p] \in \text{Pic } R[?]$.

So killing off primes either adds factors of \mathbb{Z} or does nothing at all.

By the lemma, passing from R to R_s by killing finitely many maximal ideals, if $\text{Pic } R$ and R^\times are both finitely generated, then they are still finitely generated for R_s . Thus we can assume R_s is a PID.

Proof of theorem next time. Need ramification and taking n th roots in local fields.

8 Monday January 27th

8.1 Weak Mordell-Weil: Finishing the Proof

Recall that $n \geq 2$, K a field with char K not dividing p , E/K an elliptic curve, R a Dedekind domain with fraction field $K(E[n])$ such that $\text{Pic } R$ and R^\times are finitely generated. Then $E(K)/nE(K)$ is finite.

We've shown:

- May take $K = K(E[n])$, so K contains the n -torsion and all n th roots of unity $\mu_n \in K$.
- R a PID with fraction field K ,
- $E(K)/nE(K)$ is finite iff $L := K([n]^{-1}E(K))$ is a finite degree extension over K .
- L/K is abelian of exponent dividing n
- L/K is only ramified over $\mathfrak{p} \in \text{Spec}(R)$ if $p \mid n$ or E has bad reduction at \mathfrak{p} (so bad reduction at only finitely many primes).

Last step of the proof: We'll apply Kummer theory to show L/K is finite.

Lemma: Let K be a field with a discrete valuation $v : K \rightarrow \mathbb{Z} \cup \{\infty\}$ such that $v(n) = 0$. When are Kummer extensions unramified? Every Kummer extension L is a compositum $L := K(a^{1/n})$. Then L/K is unramified at v iff n divides $v(a)$.

Proof:

\implies : We can extend v to L , and v is unramified iff $v(L^\times) = \mathbb{Z}$. Noting that $v(a^{1/n}) = \frac{1}{n}v(a)$, if we suppose $v(L^\times) = \mathbb{Z}$, we're done.

\impliedby :

Can check being unramified by passing to completion.

Pass from K to the completion K_v and let π be a uniformizer, so $v(\pi) = 1$. Then define $a' = a/\pi^{v(a)}$, so $v(a') = v(a) - v(a) = 0$ and thus $a \in R_v^\times$. Writing $a/a' = \pi^{v(a)} \in (K^\times)^n$, so $K(a^{1/n}) = K((a')^{1/n})$. So we reduce to the case $v(a) = 0$.

Since R_v is integrally closed, we have $x \in K_v^{\times n} \iff x \in R_v^{\times n}$, so there is an isomorphism

$$R_v^\times / R_v^{\times n} \cong k_v^\times / k_v^{\times n}$$

which follows from Hensel's Lemma.

Thus $K_v(a^{1/n})/K$ is unramified.

Standard argument from NT II.

■

Now let $S \subset \text{Spec } R$ be the set

$$S = \left\{ \mathfrak{p} \in \text{Spec } R \mid \mathfrak{p} \mid n \text{ or } E \text{ has bad reduction at } \mathfrak{p} \right\},$$

and

$$T_S = \left\{ a \in K^\times / K^{\times n} \mid \forall \mathfrak{p} \in \text{Spec}(R \setminus S), n \mid \text{Ord}_{\mathfrak{p}}(a) \right\}.$$

We will be done if T_S is finite.

Claim: There exists a surjective group homomorphism $\psi : R^\times \longrightarrow T_S$. Then since R^\times is finitely generated, so is its image, but if $T_S = T_S[n]$ is an n -torsion group, this forces T_S to be finite.

$$\begin{array}{ccccc}
 & & \psi & & \\
 & \nearrow & & \searrow & \\
 R^\times & \xrightarrow{\quad} & K^\times & \hookrightarrow & K^\times / K^{\times n} \\
 & \searrow & & \uparrow & \\
 & & & & T_S
 \end{array}$$

Take $\bar{a} \in T_S$ and lift it to $a \in K^\times$, and consider (a) as a fractional R_S ideal; it is an n th power. So write $(a) = I^n$ for I another fractional R_S ideal.

Really only need to assume that the class group of R_S does not have n -torsion.

Since R_S is a PID, $I = (b)$, so $(a) = (b)^n = (b^n)$ so there is some $u \in R_S^\times$ with $a = ub^n$. But then $\bar{a} = \psi(a) = \psi(u)\psi(b^n) = \psi(u)$, so ψ is surjective.

This finishes the proof of weak Mordell-Weil. ■

Remark: We could weaken the assumptions to R with fraction field $K(E[n])$ such that $(\text{Pic } R)[n]$ is finite and $R^\times / R^{\times n}$ is finite.

Application: Let $k = \bar{k}$ and C/k be a “nice” affine curve. Let R be the affine coordinate ring of C , i.e. $R = k[C]$, and $K = k(C)$ with $\text{char}(k)$ not dividing n . Show that if E/K is an elliptic curve then $E(K)/nE(K)$ is finite.

n -torsion on an abelian group is finite. Note that the Mordell-Weil group here may not itself be finite! Also note that proof almost goes through for abelian varieties, since we didn’t use anything particular to elliptic curves.

8.2 Height Functions

Definition: A product formula field is a triple (K, Σ_K, A) where K is a field, Σ_K is a set of places on K , and A is a set of normalizing constants.

A place v on a field K is an equivalence class of absolute values $|\cdot| : K \longrightarrow [-, \infty) \subset \mathbb{R}$, where e.g. the equivalence is given by absolute values inducing the same topology.

Here we don’t mind if raising to some power invalidates the triangle inequality, as long as raising to *some* power preserves it. See ultrametric, Archimedean.

Σ_K is a set of equivalence classes of absolute values (not necessarily all) such that

(PF1) $\Sigma_K^{\text{Arch}} \subset \Sigma_K$.

(PF2) For all $x \in K^\times$, the set $\{v \in \Sigma_K \mid |x|_v \neq 1\}$ is finite.

A non-Archimedean valuation in Σ_K satisfies $|x|_v = c_v^{-v(x)}$ for some rank 1 valuation $v : K \longrightarrow \mathbb{R} \bigcup \infty$ with $c_v > 1$, and A is that data of a choice of c_v for each non-Archimedean v .

(PF3) For all $x \in K^\times$, we have $\prod_{v \in \Sigma_K} |x|_v = 1$.

Note that we don't care about the c_v s necessarily, but we do need to choose them to preserve this product formula.

All global fields are PFFs, so we'll use this to define height functions on projective spaces.

9 Wednesday January 29th

A remark on weak Mordell-Weil:

Definition: A profinite group (e.g. group occurring as an absolute Galois group) is *small* if for all $n \in \mathbb{Z}^+$, the set of open subgroups of g of index n is finite.

Proposition: For any $g = g_K = \text{Aut}(K^{\text{sep}}/K)$, g is small iff K has only finitely many separable extensions of any fixed degree d .

Definition: A field K is *big* iff its Galois group g_K is small.

Warning: In general not related to cardinality.

If K is big and contains n th roots of unity $\mu_n \in K$, then for all $n \geq 2$, the maximal abelian extension of exponent dividing n is finite (by Kummer theory) Therefore, if A/K is any commutative algebraic group (plus conditions?), then $A(K)/nA(K)$ is finite.

Fields that are big:

- Finite fields
- Algebraically closed fields
- \mathbb{R} and any real closed field \iff
- p -adic fields

But $\mathbb{F}_q((A))$ is *not* big.

The Weak Mordell Weil proof goes through if you look at integral points instead of just rational points. Dirichlet unit theorem gives WMW for the multiplicative group.

9.1 Height Functions

Let (K, Σ_K, A) be a product formula field where K is a number field and $K = k(C)$ for C/K is a nice curve for k any field.

Don't need to assume separability, but we will!

A height function is a function $H : \mathbb{P}^n(K) \longrightarrow \mathbb{R}$. We assume the product formula field K has the *Northcott property*, i.e. $\{p \in \mathbb{P}^n(K) \mid H(P) \leq R\}$ is finite for every n and every R .

Remark: A number field K has the Northcott property, and $k(C)$ has this property iff k is finite.

1. This gives an estimate for change in H under finite morphisms $f : \mathbb{P}^n \rightarrow \mathbb{P}^m$.
2. For E/K with $y^2 = P_S(x)$, then $H : E(K) \rightarrow \mathbb{R}$ given by $p \mapsto H([X(p) : 1])$.

View $X : E \rightarrow \mathbb{P}^1$ is a 2:1 map given by taking x coordinates.

Sticking point: The “near-quadraticity” of H , i.e. the second property of height functions. We won’t have Weierstrass equations for abelian varieties, so we don’t want to do this. Instead, we’ll develop

1. Weil’s height machine
2. Néron-Tate canonical heights on abelian varieties A/K .

Note that if $(x_0, \dots, x_n) \in \mathbb{P}^n(\mathbb{Q})$, where \mathbb{Q} is the fraction field of \mathbb{Z} , a UFD, so this is a UFD. Appropriately clearing denominators, we can get $\gcd(x_0, \dots, x_n)$. So $H(x_0, \dots, x_n) = \max_{0 \leq i \leq n} |x_i|$, and (check!) the Northcott property holds.

Let (K, Σ_K, A) where Σ_K is a set of inequivalent places $|\cdot|_v$.

PFF1: The Archimedean places Σ_K^{Arch} have valuations $v : K \rightarrow \mathbb{R} \cup \infty$ where $|\cdot|_v = c_v > 1$.

PFF2: For all $x \in k^\times$, $|x|_v = 1$ for all v .

PFF3: Height is invariant under scaling, i.e. for all $x \in k^\times$, $\prod_{v \in \Sigma_K} |x|_v = 1$.

Example: Take $K = \mathbb{Q}$, then

- $|x|_p = p^{-\text{Ord}_p(x)}$
- $|x|_\infty = |x|$ the standard real absolute value
- $|x|_\infty = \left(\prod_p |x|_p \right)^{-1}$ for all $x \in \mathbb{Z}^\bullet$.

Example: k any field, $R = k[t]$, and $K = k(t)$. Then it’s not quite true that $\Sigma_K = \{v_p, p \text{ monic irreducible polynomial}\}$.

Question: what is C_{v_p} .

For $c > 1$, we can write $|\cdot|_p := c^{-v_p}$. Write $x = \varepsilon p_1^{a_1} \cdots p_r^{a_r}$ with the p_i monic irreducibles and $\varepsilon \in k^\times$. Then $\prod_p |x|_p = \prod_p c^{-v_p(x)} = c^{-\sum a_i}$. But this isn’t one! We don’t have the “counterbalance” here, so we may want to add an infinite place to compensate.

Remark: If k is algebraically closed, then $p_i = t - x_i$ and $\sum a_i = \deg v$.

Adding a place: Define $v_\infty(f/g) = v_\infty(f) - v_\infty(g)$, and $|\cdot|_{v_\infty} = c^{-v_\infty(f/g)} = c^{\deg f - \deg g}$. This yields

$$\begin{aligned} |x|_\infty \prod_p |x|_p &= \prod_p C^{-v_p(x)} C^{\deg x} \\ &= c^{-\sum a_i} C^{\deg x} \\ &= C^{-\deg x} C^{\deg x}. \end{aligned}$$

In general, $\deg(\prod_{i=1}^r p_i^{a_i} \cdots p_r^{a_r}) = \sum_{i=1}^r a_i \deg(p_i)$.

Then $k_v := \deg p_v \cdot c$ and $|x|_p := C^{-\deg(p)v_p(x)}$.

10 Friday January 31st

Given a product formula field (PFF) (K, Σ_K, A) , recall that we want the product formula:

$$\forall x \in K^\times, \quad \prod_{v \in \Sigma_K} |x|_v = 1.$$

We want to show that given any finite separable extension L/K , endow it with a PF structure where the places of L are given by $\Sigma_L =$ all extensions of $v \in \Sigma_K$ to L (?)

Note that separability is not necessary but does simplify things, c.f. Serre.

The structure for A : to be decided.

A technical remark: A global field is given by $K = \mathbb{F}_q(C)$ where C/\mathbb{F}_q is a nice curve.

Then \mathbb{Q} has a PF structure, $K(t)$ has a PF structure. Note that the extensions over \mathbb{Q} will be separable, since we're in characteristic zero, so the question is about separable extensions over $K(t)$.

If C/K is a nice curve over any field, then there exists a finite degree extension $K(C)/K(t)$ iff $C \xrightarrow{f} \mathbb{P}^1$.

Reminder: Noether's normalization, integral affine variety over any field, can geometrically map it down to affine d-space via an algebraic (finite) map. So we end up with a finitely generated module over a polynomial ring.

We want a separable extension, and from field theory, since \mathbb{F}_q is perfect we can find $\mathbb{F}_q(t) \subset \mathbb{F}_q(C)$ which is separable.

If k is any perfect field, then we can find a separable Noether normalization. If K/k is a finitely generated field extension of transcendence degree d . Moreover, we can find an extension $K \xrightarrow{\text{finite, separable}} k(f_1, \dots, f_d) \rightarrow k$.

So let L/K be degree d and separable. There is a surjective map $\Sigma_L \twoheadrightarrow \Sigma_K$ with fibers of size $\leq d$. For $v \in \Sigma_K$, this is defined by $L_v := L \otimes_K K_v$, and if L/K is separable then $L \cong k[t]/(f)$ where f is separable and irreducible. Thus $L_v \cong K_v[t]/(f)$ where $f = f_1 \cdots f_r$ which are irreducible over K_v .

By the Chinese Remainder Theorem, $L_v \cong \prod_{i=1}^r K_v[t]/(f_i) \cong \prod_{w|v} L_w$.

Primitive element theorem: finite separable extensions of fields are generated by one element.

How do we extend the norm? For $x \in C_w$, define $|x|_w := |N_{L_w/K_v}(x)|_v^{\frac{1}{d}}$ where d is the global degree $d = [L : K]$.

Note that the exponent here is not necessary to get the product formula, but it works anyway and is useful when we later look at heights.

Lemma: For $x \in C$, $\prod_{w|v} |x|_w = |N_{L/K}(x)|_v^{\frac{1}{d}}$.

This yields the normalization A_L .

Theorem: The product formula holds, i.e. (L, Σ_K, A) is a PFF.

For all $x \in L^\vee$, we have $\prod_{w \in \Sigma_L} |x|_w = \prod_{v \in \Sigma_K} \prod_{w|v} |x|_w$. This equals $\prod_{v \in \Sigma_K} |N_{L/K}(x)|_v^{\frac{1}{d}} = 1$ by the product formula on K . ■

10.1 Height Functions

For (K, Σ_K, A_K) a PFF, define $x := (x_0, \dots, x_n) \in \mathbb{A}^{n+1}(K)$ and $H(x) := \prod_{v \in \Sigma_K} \max_{0 \leq i \leq n} |x_i|_v$. Then $H(x) = 0$ iff $x = (0, 0, \dots, 0)$.

Lemma: For all $\lambda \in K^\times$, $H(\lambda x_1, \dots, \lambda x_n) = H(x_1, \dots, x_n)$, so H descends to $H : \mathbb{P}^n(K) \rightarrow \mathbb{R}$.

Thus for any $p \in \mathbb{P}^n(K)$, can write $p = [x_0, \dots, x_n]$ where some $x_i = 1$. So each term appearing in the product is at least 1.

For $x \in K$, we define $H(x) = H([x : 1])$.

Example: Take $K = \mathbb{Q}$ and $n = 1$, we can compute $H([x : y]) = H([a : b])$ where $\gcd(a, b) = 1$. This equals $\prod_{p \leq \infty} \max(|a|_p, |b|_p)$, the p -adic norms. This equals $(\max(|a|, |b|)) \left(\prod_p \max(|a|_p, |b|_p) \right)$, where the second term collapses to 1 because every term is 1, because no p can divide both a and b . So $H([a : b]) = \max(|a|, |b|)$.

Example: Take $K = \mathbb{Q}$, n arbitrary. WLOG, we can consider $\{x_i\}$ with $\gcd(x_i) = 1$, then $H([x_0 : \dots : x_n]) = \max(|x_0|, \dots, |x_n|)$.

We in fact have a finite bound

$$\#\{P \in \mathbb{P}^n(\mathbb{Q}) \mid H(P) \leq R \in \mathbb{Z}\} \leq (2R + 1)^{n+1}.$$

Note that the probability that two numbers are prime is $1/\zeta(2)$; look at Euler product expansion.
Idea of proof: don't want both to be divisible by 2, by 3, by 5, etc.

Example: Let $K = k(t) \supset k[t]$ for k arbitrary. Write $H([x_0 : x_1]) = H([a : b])$ where $a, b \in k[t]$ with $\gcd(a, b) = 1$. Recall that the infinite-adic norm is given by $|a|_\infty = C^{\deg(a)}$. Then $H([a : b]) = \prod_{p \leq \infty} \max(|a|_p, |b|_p) = (\max(|a|_\infty, |b|_\infty)) \prod_p \max(|a|_p, |b|_p) = \max(C^{\deg a}, C^{\deg b})$, where the same argument goes through. Thus $\log_C H([a : b]) = \max(\deg a, \deg b)$, literally the maximum degree of these two polynomials.

Note that there are only finitely many polynomials of a given degree d iff the field is finite. So the PFF formalism doesn't care about the field, but the Northcott property depends on the cardinality of the field in a key way.

Fact: The Northcott property holds for all $R > 0$ and for all n , i.e. $\#\{P \in \mathbb{P}^n \mid H(P) \leq R\} < \infty$ iff K is finite. This holds iff $\#\{P \in \mathbb{P}^n \mid \log_C H(P) \leq R\}$ is finite. Note that if $K = \mathbb{F}_q$, then for $R \in \mathbb{Z}^+$, $\#\{P \in \mathbb{P}^n(\mathbb{F}_q) \mid \log_C H(P) \leq R\} = (q^{r+1})^{n+1}$ by counting choices for coefficients.

We'll show that the Northcott property passes to finite extensions.

Theorem: Let K be a Northcott PFF, then for all $n \in \mathbb{Z}^+$, for all $R \in \mathbb{R}$, for all $d \in \mathbb{Z}^+$, $\#\{P \in \mathbb{P}^n(K^{\text{sep}}) \mid [K(P) : K] \leq d, H(P) \leq R\}$ is finite.

11 Monday February 3rd

We started with a product formula field (K, Σ_K, A) , then took L/K finite and separable and equipped it with a PFF structure: Σ_L is equal to the places extending $v \in \Sigma_K$, and for $v \in \Sigma_L$, we have $|x|_w = |L_w/K_v(x)|_v^{1/d}$.

We defined a height function $H : \mathbb{P}^n(K) \rightarrow [1, \infty)$ where $[x_0, \dots, x_n] \mapsto \prod_{v \in \Sigma_K} \max(|x_0|_v, \dots)$.

If L/K is separable of degree d , we can consider $p \in \mathbb{P}^n(K) \subset \mathbb{P}^n(L)$ and define H_K, H_L respectively. It is then a fact that $H_L(p) = H_K(p)$. For $\alpha \in \mathbb{A}^1$, we have $H_L(\alpha) = H_K(N_{L/K}(\alpha))^{1/d} = H_K(\alpha^d)^{1/d} = H(\alpha)$.

This allows us to extend height functions to the separable closure, $H : \mathbb{P}^n(K^{\text{sep}}) \rightarrow \mathbb{R}$.

Lemma: If $p \in \mathbb{P}^n(K^{\text{sep}})$ and $\sigma \in g_K = \text{Aut}(K^{\text{sep}}/K)$, then $\sigma(p) := [\sigma(x_0), \dots, \sigma(x_n)]$ does not change the height.

Proof: Exercise.

Check that the norms of points are the same as the norms of their Galois conjugates. So the height is Galois-equivariant.

For $v \in \Sigma_K$, let ε_v be the Artin constant: the smallest $\varepsilon_v \in \mathbb{R}$ such that $|x + y|_v \leq \varepsilon_v \max(|x|_v, |y|_v)$.

Artin constant: measures how much better a norm does than the triangle inequality. Note that $\varepsilon_v = 1$ for ?

Lemma: Let K be a PFF and $d \in \mathbb{Z}^+$. If there exists an $M(K, d) > 0$ such that for all separable $f(T) = T^d + a_{d-1}T^{d-1} + \dots + a_1T + a_0 \in K[T]$, i.e. $f(T) = \prod_{i=1}^d (T - \alpha_i)$ with $\alpha_i \in K^{\text{sep}}$, then

$$H(a_0, \dots, a_{n-1}, 1) \leq M(K, d) \prod_{i=1}^d H(\alpha_i).$$

Proof:

Step 1: Suppose $\alpha_i \in K$ for all i . If so, we can take $M(K, d) = \prod_{v \in \Sigma_K} \varepsilon_v^{d-1}$.

Why? We need to show that for all $v \in \Sigma_K$, we have $\max |a_i|_v \leq \varepsilon_v^{d-1} \prod_{i=1}^d \max(|\alpha_i|_v)$. If so, take the product over all v .

Proceeding by induction, where the $d = 1$ is clear, suppose $d \geq 2$ so result holds for $d - 1$. Choose k such that $|\alpha_k|_v \geq |\alpha_i|_v$ for all i . We can then write $f(T) = (T - \alpha_k)(T^{d-1} + b_{d-1}T^{d-2} + \dots + b_1T + b_0)$ where $b_{d-1} = 1$ and $b_{-1} = b_d = 0$. Then for all i , we have $\alpha_i b_{i-1} - \alpha_k b_j$.

We then apply the triangle inequality:

$$\begin{aligned} |a_i|_v &= \max_i |b_{i-1} - \alpha_j b_i| \\ &\leq \varepsilon_v \max |b_{i-1}|_v |\alpha_k b_i|_v \\ &\leq \varepsilon_v (\max_n |b_i|_v) \max(|\alpha_k|_v, 1) \\ &\leq_{IH} \varepsilon_v^{d-1} \max_i (|a_i|_v, 1). \end{aligned}$$

■

Step 2: Now suppose $\alpha, \dots, \alpha_d \in K^{\text{sep}}$. Then replace K with $K(\alpha_1, \dots, \alpha_d) := L$. This is an extension of K of degree at most $d!$.

Note that if we define $\varepsilon = \max \varepsilon_v$, and $|\Sigma_K^{\text{Arch}}| = A$, then $\prod_{v \in \Sigma_K} \varepsilon_v^{d-1} \leq (\varepsilon^A)^{d-1} = \varepsilon^{A(d-1)}$. We also have $|\Sigma_L^{\text{Arch}}| \leq d!A$ and for the argument over K , we can take $M(K, d) = \varepsilon^{Ad!(d-1)}$.

Theorem (Northcott implies Strong Northcott): Let K be a PFF satisfying the Northcott property. Then for all $d, n \in \mathbb{Z}^+$ and for all $R \in \mathbb{R}$, the set $\{P \in \mathbb{P}^n(K^{\text{sep}}) \mid [K(P) : K] \leq d, H(P) \leq R\}$ is finite. I.e. passing to finite separable extensions preserves the Northcott property, although this statement is stronger, since this is a *uniform* bound (hence the term “strong”).

Stated scheme-theoretically, we can write $P = [x_0, \dots, x_n]$ where some $x_i = 1$ be rescaling. Then $K(P) = K(x_0, \dots, x_n)$ is a finite separable extension.

Proof: Let $P \in \mathbb{P}^n(K^{\text{sep}})$ with $\deg P \leq d$, where $P = [x_0, \dots, x_n]$ with one $x_i = 1$.

$$\begin{aligned} H(P) &= \prod_{v \in \Sigma_K} \max_i |x_i|_v \\ &= \prod_{v \in \Sigma_K} \max_i (|x_i|_v, 1) \\ &\geq \max_i \prod_{v \in \Sigma_K} \max(|x_i|_v, 1) \\ &= \max_i H(x_i). \end{aligned}$$

So if $H(P) \leq C$ and $[K(P) : K] \leq d$, then $\max_i H(x_i) \leq C$ and $\max_i [K(x_i) : K] \leq d$.

Define $X(K, C, d) = \{x \in K^{\text{sep}} \mid H(x) \leq C, [K(x) : K] \leq d\}$, we'll show this is a finite set. Let $x \in X(K, C, d)$ and $d' := [K(x) : K] \leq d$, and $f(T) := \text{minpoly}_x = \prod_{i=1}^{d'} (T - x_i) = T^{d'} + \sum_{i=0}^{d'-1} a_i T^i$. Take $M := \max_{1 \leq i \leq d} M(K, i)$ from the previous lemma.

By the lemma, we have $H(a_0, \dots, a_{d'-1}, 1) \leq M \prod_{i=1}^{d'} H(x_i)$. But Galois conjugate points have the same height, so this is equal to $MH(x)^{d'} \leq MC^d$. By the Northcott property, there exist only finitely many such tuples $(a_0, \dots, a_{d'-1}, 1)$, and thus only finitely many possibilities for x . ■

Key Theorem: Let K be a PFF, and $f : \mathbb{P}^n \rightarrow \mathbb{P}^m$ be a degree d morphism over K (given by a collection of homogeneous polynomials of degree at most d). Then there exist constant $C_1, C_2 > 0$ depending only on K such that

$$C_1 H(P)^d \leq H(f(P)) \leq C_2 H(P)^d.$$

Proof: See Theorem 8.5.6 in Silverman I.

12 Friday February 7th

12.1 Weil Height Machine

What is the analog of the x -coordinate of an elliptic curve for a general abelian variety? Answer: an ample base point divisor.

Let K be an NPFF (Northcott Product Formula Field), V/k a projective variety and $\phi : V \rightarrow \mathbb{P}^n$, then define

$$h_\phi : V(K^{\text{sep}}) \rightarrow [0, \infty) \quad p \mapsto \log H(\phi(p)).$$

Key property: Take hyperplanes $\psi : V \rightarrow \mathbb{P}^m \supset H'$ and $\phi : V \rightarrow \mathbb{P}^n \supset H$, noting that the picard group of \mathbb{P}^n is \mathbb{Z} . Suppose $\phi^* \sim \psi^* H'$, then $h_\phi = h_\psi + O(1)$. Generally, we'll want to identify functions whose difference is a bounded function.

Highly recommended: Diophantine Geometry, Handry-Silvermann GTM

Theorem (Weil Height): Let K be a NPFF (e.g. a global field) and V/K a smooth projective variety. There exists a map $h_{V,\cdot} : \text{Div} V \rightarrow \mathbb{R}^{V(K^{\text{sep}})}$ from divisors on V to ? which is unique modulo bounded functions such that

- a. For $H \subset \mathbb{P}^n$ a hyperplane, the divisor $h_{\mathbb{P}^n H} = h + O(1)$ (for the previously defined h).
- b. Pullbacks: For $\phi : V \rightarrow W$ a smooth morphism and $D \in \text{Div} W$, we have $h_{V, \phi^* D} = h_{W, D} \circ \phi + O(1)$.
- c. Linearity: For all divisors $D_1, D_2 \in \text{Div} V$, $h_{V, D_1 + D_2} = h_{V, D_1} + h_{V, D_2} + O(1)$.

- d. If $D_1 \sim D_2$, then $h_{V,D_1} = h_{V,D_2} + O(1)$.
- e. Positivity: Let $D \in \text{Div} V$ be effective and B the base locus (common intersection of linearly equivalent effective divisors), then $h_{V,D}(p) \geq O(1)$ for all $P \in (V \setminus B)(K^{\text{sep}})$.
- f. Let $D, E \in \text{Div} V$ with D ample and E algebraically equivalent to 0. Then $\lim_{P \in V(K^{\text{sep}}), h_{V,D}(p) \rightarrow \infty} h_{V,E}(p)/h_{V,D}(p) = 0$.

Ample: Chern class of line bundle is zero.

- g. Finiteness: $D \in \text{Div} V$ is ample. For all map into L/K and $r \in \mathbb{R}$, the set $\{p \in V(L) \mid h_{V,0}(p) \leq R\}$ is finite.

Note every ample divisor has the Northcott property. Every abelian variety has an ample *symmetric* divisor.

Let $V = A/K$ be an abelian variety and $D \in \text{Div} A$ a divisor, see section A.7 in Silverman. Some properties of such divisors:

1. (A.7.25) For all $n \in \mathbb{Z}$, $[n]^*D \sim \frac{n^2+n}{2}D + \frac{n^2-n}{2}[-1]^*D$ (standard fact). If $[D]$ is symmetric, i.e. $[-1]^*D \sim D$, $[n]^*D \sim n^2D$. If $[D]$ anti-symmetric, i.e. $[-1]^*D \sim -D$, then $[n]^*D \sim nD$. i.e. $[-1]^*D \sim -D$, then $[n]^*D \sim nD$. i.e. $[-1]^*D \sim -D$, then $[n]^*D \sim nD$.
2. (A.7.210?) Let D be effective, then $2D$ is basepoint free and TFAE:
 - D is ample.
 - $\psi_\ell : A \rightarrow A^\vee$ where $x \mapsto \tau_x^*D - D$ (where τ_x is translation by x) has finite kernel.
 - $A \rightarrow \mathbb{P}(L(2D))$ is finite.
3. (A.7.33) Define 4 maps, $\sigma, \delta, \pi_1, \pi_2 : A \times A \rightarrow A$,

$$\sigma(P, Q) = P + Q \quad \delta(P, Q) = P - Q \quad \pi_1(P, Q) = P \quad \pi_2(P, Q) = Q,$$

Then

- a. For $D \in \text{Div} A$, $[D]$ is symmetric iff $\sigma^*D + \delta^*D \sim 2\pi_1^*D + 2\pi_2^*D$.
- b. $[D]$ is antisymmetric iff $\sigma^* \sim \pi_1^*D + \pi_2^*D$ iff $[D] \in \text{Pic}^0 A$.

Proof: see Silverman, uses “Theorem of the Square” and the “Seesaw Principle”.

Corollary: For A/K an abelian variety over K a NPFF and $D \in \text{Div} A$, then

- a. $p \in A(K^{\text{sep}})$ and $h_{A,0}([n]p) = \frac{n^2+n}{2}h_{A,D}(p) + \frac{n^2-n}{2}h_{A,D}(-p) + O(1)$. If D is symmetric, then $h_{A,D}([n]p) = n^2h_{A,D}(p) + O(1)$. If D is antisymmetric, then $h_{A,D}([n]p) = nh_{A,D}(p) + O(1)$.

This follows from properties of the Weil height machine.

- b. If $[D]$ is symmetric, then we get the *quadraticity* relation: for all $P, Q \in A(K^{\text{sep}})$, $h_{A,D}(P + Q) + h_{A,D}(P - Q) = 2h_{A,D}(P) + 2h_{A,D}(Q) + O(1)$.

Proof: We have $h_{A \times A, D}(\sigma(P, Q)) + h_{A \times A, D}(\delta(P, Q)) = 2h_{A \times A, D}(\pi_1^*D) + 2h_{A \times A, D}(\pi_2^*D) + O(1)$.

For $\phi : V \rightarrow W$ and $D \in \text{Div} W$, we have $h_{C, \phi^*(D)}(p) = h_{W, D}(\phi(p)) + O(1)$. So $h_{A \times A, D}(\sigma(P, Q)) = h_{A, D}(\sigma(P, Q)) = h_{A, D}(P + Q)$, and applying it to the other terms works the same way.

Abelian variety has attached *polarization*, and are projective group varieties. Every projective variety has an ample divisor, by definition?

Proof of Mordell-Weil for A/K a global field:

1. Weak MW
2. Choose an ample symmetric $D \in \text{Div} A$, by definition A carries an ample divisor D_0 ; then $D := D_0 + [-1]^* D_0$ is ample and symmetric.
3. Work with $h_{A,D}$ instead of h_X for elliptic curves

Then the proof goes through as before.

Note h is trying to be a quadratic form (we'll review such forms on groups) except for the $O(1)$. Maybe we can modify h by a bounded function to make it quadratic – this is the Neron-Tate canonical height. Regulator: defined in terms of the Neron-Tate canonical height on the Mordell-Weil group of an elliptic curve.

13 Wednesday February 12th

13.1 Correction to Weil's Height Machine

Let K be a NPFF (from now onwards: just a global field) and X/K a nice variety. Let $D \in \text{Div}(X)$ be ample and consider the points of bounded height $\{p \in V(K) \mid h(p) \leq R\}$; by the Northcott property this is finite for every $R \in \mathbb{R}$.

Counterexample: Let $X = E$ an elliptic curve and $D = [0]$. Then $\ell(D) = \dim f \in K(X) \mid \text{Div} f \geq -D$, the rational functions with poles no worse than order D . Then $\ell[0] = 1$.

Then there is a corresponding morphism to projective space $\phi_D : X \rightarrow \mathbb{P}(L(D)) = \mathbb{P}^{\ell(D)-1}$. Here $\phi_D : E \rightarrow \mathbb{P}^{\ell[0]-1} = \mathbb{P}^0 = \{\{\text{pt}\}\}$.

Thus if $E(K)$ is infinite, which is possible, then $\forall R \geq 1$ the set $\{p \in E(K) \mid h(p) \leq R\} = E(K)$ is infinite as well.

How to fix this? Replace “ D is ample” with “ D is ample and $\ell(D) \geq 2$ ”.

Note: not listed as a correction in Silverman's book.

Theorem (C.1.9 Of Hindry-Silverman): Let K be a number field (perhaps works with global function fields) and $n \geq 2$, with A/K an abelian variety of dimension g . Suppose $A[n] = A[n](K)$ (so a large extension of K), and let S be a set of finite non-Archimedean places of K containing places dividing n and places of bad reduction. Suppose all that the ring of S -integers, $\mathbb{Z}_{K,S}$, is a PID.

Then $\text{rank} A[k] \leq 2g \text{rank} \mathbb{Z}_{K,S}^\times$. We can then apply the Dirichlet unit theorem, the RHS is $2g(r_1 + r_2 + \#S - 1)$ where r_1 is the number of real places and r_2 is the number of complex places.

This is an explicit upper bound, but a pretty bad one!

13.2 Néron-Tate Canonical Height

Let K be a global field. We'll get a good canonical representative of the height functions studied previously, provided we get one additional piece of data.

Theorem (Néron-Tate): Let V/K be a nice variety and $D \in \text{Div} V$, and suppose there exists a morphism $\phi : V \rightarrow V$ such that there exists an $a \in \mathbb{Q}^{>1}$ with the induced map on $\text{Pic } V$ satisfies $\phi^* D \sim \alpha D$. (So D is an “eigendivisor”).

Then there exists a unique function

$$\hat{h}_{V,\phi,D} : V(K^{\text{sep}}) \rightarrow \mathbb{R}$$

such that

1. (CH1) $\hat{h}_{V,\phi,D} = h_{V,D} + O(1)$
2. (CH2) $\hat{h}_{V,\phi,D} \circ \phi = \alpha \hat{h}_{V,D}$

Moreover, for all $p \in K^{\text{sep}}$, there is a stabilization

$$\hat{h}_{\phi,D}(p) = \lim_n \frac{1}{\alpha^n} h_{V,D}(\phi^n(p)).$$

Proof: We first need to show that the stated limit exists. Applying Weil's Height Machine to $\phi^* D \sim \alpha D$, there exists a c such that

$$|h_{V,D} \circ \phi - \alpha h_{V,D}| \leq c.$$

So take a separable point $p \in V(K^{\text{sep}})$.

Claim: $\alpha^{-n} h_{V,D}(\phi^n(p))$ is Cauchy in \mathbb{R} and thus convergent.

Proof:

Step 1: Let $m \leq n$, then we want to show

$$\begin{aligned}
|\alpha^{-n}h_{V,D}(\phi^n(p)) - \alpha^{-m}h_{V,D}(\phi^n(p))| &= \left| \sum_{i=m+1}^n \alpha^{-i} (h_{V,D}(\phi^i(p)) - \alpha h_{V,D}(\phi^{i-1}(p))) \right| \\
&= \sum_{i=m+1}^n \alpha^{-i} |h_{V,D}(\phi^i(p)) - \alpha h_{V,D}(\phi^{i-1}(p))| \\
&\leq \sum_{i=m+1}^n \alpha^{-i} C \\
&< C \sum_{i=m+1}^{\infty} \alpha^{-i} \\
&= \frac{\alpha^{-m-1}1 - \alpha}{C} \\
&\xrightarrow{m \rightarrow \infty} 0.
\end{aligned}$$

Step 2: Write

$$\begin{aligned}
\hat{h}_{V,D}(\phi(p)) &= \lim_{n \rightarrow \infty} \alpha^{-n} h_{V,D}(\phi^n(\phi(p))) \\
&= \alpha \lim_{n \rightarrow \infty} \frac{1}{\alpha^{n+1}} h_{V,D}(\phi^n(\phi(p))) \\
&= \alpha \hat{h}_{V,\phi,D}(p).
\end{aligned}$$

Step 3: Suppose \hat{h} and \hat{h}' both satisfy CH1 and CH2. Let $g := \hat{h} - \hat{h}'$. By CH1, $|g| \leq C$ for some C . Then by CH2, $g \circ \phi = \alpha g$, and for all $n \in \mathbb{Z}^+$, $g \circ \phi^n = \alpha^n g$. We thus get

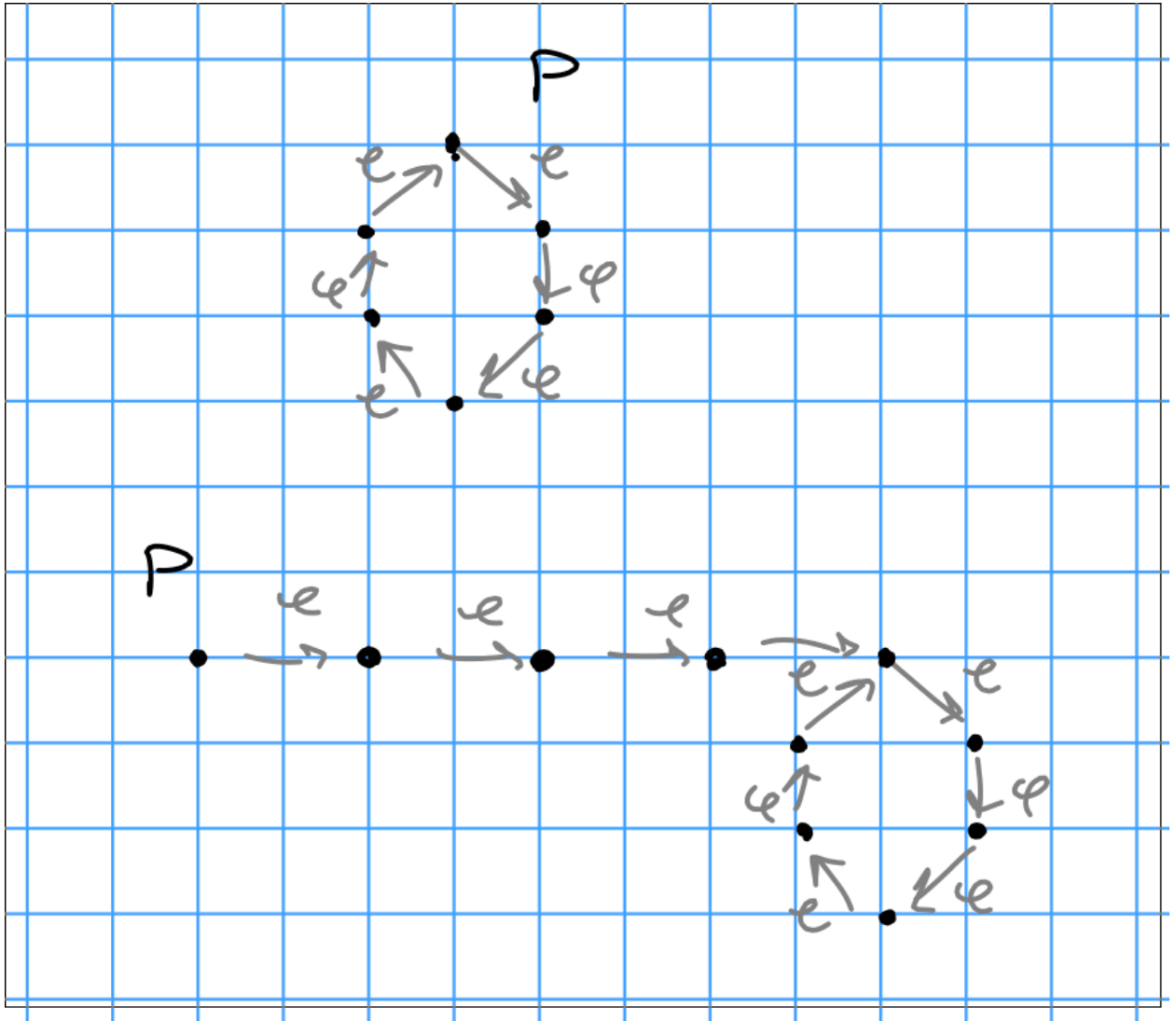
$$g = \frac{g \circ \phi^n}{\alpha^n} \implies |g| \leq \frac{C}{\alpha^n} \xrightarrow{n \rightarrow \infty} 0.$$

■

13.3 10 Cents of Dynamics

Anytime we have an endomorphism, we can iterate it and consider the associated dynamical system.

Let S be a set, $\phi : S \rightarrow S$ a function, $\phi^n = \phi \circ \phi \circ \cdots \circ \phi$ with $\phi^0 = \text{id}_S$. Then $p \in S$ is ϕ -periodic if there exists an $n \in \mathbb{Z}^+$ such that $\phi^n(p) = p$. We say p is ϕ -preperiodic iff the set $\{\phi^n(p) \mid n \in \mathbb{N}\}$ is finite. In this case, there exists some $n \in \mathbb{N}$ such that $\phi^n(p)$ is ϕ -periodic:



Proposition: Setup as in the last result, $\phi : V \rightarrow V$, $D \in \text{Div} V$ and $\phi^* D \sim \alpha D$ for $\alpha \in \mathbb{Q}^{\geq 1}$. For $\ell(D) \geq 2$ and D ample, we have

- For all $p \in V(K^{\text{sep}})$, $\hat{h}_{V,D,\phi}(p) \geq 0$. Moreover, $\hat{h}_{V,D,\phi}(p) = 0$ iff p is ϕ -preperiodic.
- The set $\{p \in V(K) \mid p \text{ is } \phi\text{-preperiodic}\}$ is finite.

Proof of (a):

We know positivity by the Weil Height Machine. Let $p \in A(K^{\text{sep}})$, then $K \rightarrow K(p)$ for ?. Suppose $\hat{h}_{V,D,\phi}(p) = 0$, then

$$\begin{aligned} h_{V,D}(\phi^n(p)) &= \hat{h}_{V,\phi,D}(\phi^n(p)) + O(1) \\ &= \alpha^n \hat{h}_{V,\phi,D}(p) + O(1) \\ &= O(1). \end{aligned}$$

Then the set of forward orbits $\{\phi^n(p) \mid n \in \mathbb{N}\}$ has bounded height. By the finiteness property of the Weil Height Machine, this set is finite and p is thus ϕ -preperiodic.

If p is ϕ -preperiodic, then $\{h_{V,D}(p)\}$ bounded, so

$$\widehat{h}_{V,\phi,D}(p) = \lim_n \frac{1}{\alpha^n} h_{V,D}(\phi^n(p)) = 0.$$

Proof of (b):

By part (a), if $p \in V(K)$ then p is ϕ -preperiodic, so $\widehat{h}_{V,\phi,D} = 0$ and thus $h_{V,D}(p) = O(1)$. By the Weil Height Machine, this set of points is finite. ■

13.3.1 Important Examples

Example 1: Let $\phi : \mathbb{P}^n \rightarrow \mathbb{P}^n$ of degree $d \geq 2$ and $H \subset \mathbb{P}^n$ the hyperplane divisor, $\phi^*H \sim dH$. So take $\alpha = d$, this is an eigendivisor, now applying this theory, a consequence is that $\{p \in V(K) \mid p \text{ is } \phi\text{-preperiodic}\}$ is finite. (Theorem by Northcott, properties of heights were established to show this statement!)

Example 2: Let A/K an abelian variety with $D \in \text{Div} A$ ample, $\ell(D) \geq 2$ with $[-1]^*D \sim D$. Take $\phi = [n]$ for some $n \geq 2$, then $\phi^*(D) \sim n^2 D$ where $\alpha = n^2 > 1$. The ϕ -preperiodic points of $A(K^{\text{sep}})$ are precisely the torsion points.

Note that this proves that the set of torsion points on an abelian variety is finite.

14 Friday February 14th

14.1 Canonical Heights

Last time: the Néron-Tate Canonical Height. Simple if you buy the Weil Height Machine! Recall the statement of the theorem:

Theorem 14.1.

Let K be a global field, V/K a nice variety, $D \in \text{Div}(V)$. Suppose there exists $\phi : V \rightarrow V$ such that D is an “eigendivisor”, i.e. $\phi^*D \sim \alpha D$ for some $\alpha \in \mathbb{Q}$.

Then there exists a unique function $\widehat{h}_{V,\phi,D} : V(K^{\text{sep}}) \rightarrow \mathbb{R}$ such that

- (CH1) $\widehat{h}_{V,\phi,D} = h_{V,D}O(1)$
- (CH2) $\widehat{h}_{V,\phi,D} \circ \phi = \alpha \widehat{h}_{V,\phi,D}$, which is constructed in the following way: For all $p \in K^{\text{sep}}$,

$$\widehat{h}_{V,\phi,D}(p) = \lim_n \frac{1}{\alpha^n} h_{V,D}(\phi^n(p)).$$

Two important examples:

Example 14.1.

Morphism from $\mathbb{P} \rightarrow \mathbb{P}$, then $\text{Pic } \mathbb{P} = \mathbb{Z}$ so everything’s an eigendivisor. So just take a degree ≥ 2 map and a hyperplane divisor.

Example 14.2 (Key example).

A/K an abelian variety, D ample, $\ell(D) \geq 2$ (so at least 2 sections of the line bundle), and symmetric in the sense that $[-1]^*D \sim D$. Then for all $n \in \mathbb{Z}$, $[n]^*D \sim n^2D$, so take ϕ to be multiplication by n for $|n| \geq 2$.

In this case $\hat{h}_{A,D} = \hat{h}_{A,[n],D}$. It agrees with the usual Weil height, and moreover $\hat{h}_{A,D}([n]p) = n^2\hat{h}_{A,D}(p)$. Note that this is at least one property we'd want from a quadratic form.

The geometry associated to the height function on other types of varieties can become more interesting, e.g. K_3 surfaces and Calabi-Yau.

Next up: Showing $\hat{h}_{A,D} : A(K^{\text{sep}}) \rightarrow \mathbb{R}$ is a “quadratic form”, but what is a quadratic form on an abelian group?

14.2 Quadratic Functions

Let A, B be abelian groups written additively. Then a map $f : A \rightarrow B$ is *quadratic* if the associated function

$$B_f : A \times A \rightarrow B$$

$$(x, y) \mapsto f(x + y) - f(x) - f(y) + f(0)$$

is bilinear.

A function is *homogeneous quadratic* iff f is quadratic and $f(0) = 0$. A *quadratic form* is homogeneous, quadratic, and symmetric in the sense that $f(-x) = f(x)$ for all $x \in A$.

Note: multiplication on \mathbb{R} by 2 is an isomorphism, i.e. \mathbb{R} is *uniquely 2-divisible*. If B doesn't have this property, things can get slightly more complicated.

Lemma 14.2.

$f : A \rightarrow B$ is quadratic iff for all $x, y, z \in A$ we have

$$f(x + y + z) - f(x + y) - f(x + z) - f(y + z) + f(x) + f(y) + f(z) - f(0) = 0.$$

In other words, knowing what it does on values and pairs determines what it does on triples.

Proof.
Straightforward computation. ■

Lemma 14.3.

Let $f : A \rightarrow B$ such that

1. f is a quadratic form.
2. f satisfies the *parallelogram law* (also: quadraticity) $f(x+y) + f(x-y) = 2f(x) + 2f(y)$.

Then 1 implies 2, and if the 2-torsion $B[2]$ is trivial, then 2 implies 1.

Lemma 14.4.

Suppose f is a quadratic function, then f is a quadratic form iff $\forall n \in \mathbb{Z}, \forall x \in A, f(nx) = n^2 f(x)$.

Note that $n = 0$ implies homogeneity, and $n = 1$ implies symmetric. Proceed by strong induction.

Lemma 14.5.

Let $f : A \rightarrow B$ be a quadratic function. Define the even and odd parts of f in the following way:

$$\begin{aligned} q : x &\mapsto (f(x) - f(0)) + (f(-x) - f(0)) \\ l : x &\mapsto (f(x) - f(0)) - (f(-x) - f(0)) \end{aligned}$$

Then

- a. q is a quadratic form, l is a group morphism, and $2f = q + l + 2f(0)$.
- b. If B is uniquely 2-divisible, then dividing by 2 yields $f = \frac{1}{2}q + \frac{1}{2}l + f(0)$ where q is a quadratic form, l is a linear morphism, and $f(0)$ is constant. This decomposition is unique.

Exercise Show that if $f : A \rightarrow B$ a quadratic function,

- a. $f(A[\text{tors}]) \subseteq B[\text{tors}]$.
- b. For n odd, $f(A[n]) \subset B[n]$.
- c. The map $f : \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z}$ where $0 \mapsto 0, 1 \mapsto 1$ is a quadratic form. Thus the n odd condition above is necessary.

This comes up in Galois cohomology of abelian varieties? See Pete's paper. It takes an n torsion to an element that is no worse than $2n$ torsion.

From now on, take $B = \mathbb{R}$. Note that if $B = \mathbb{R}$, height functions kill all torsion.

Define a pairing

$$\begin{aligned} \langle \cdot, \cdot \rangle : A \times A &\rightarrow B \\ \langle x, y \rangle &= \frac{1}{2}(f(x+y) - f(x) - f(y)). \end{aligned}$$

If f is a quadratic form, $\langle x, x \rangle = f(x)$, so this reduces to the usual bilinear form associated to a quadratic form.

Exercise a. Show that for all $x \in A, y \in A[\text{tors}]$, we have $f(x+y) = f(x)$. Thus f factors through a morphism $\hat{f} : A/A[\text{tors}] \rightarrow \mathbb{R}$ through the torsion-free quotient.

This is stronger than just killing torsion, since f isn't necessarily linear.

b. If f is a quadratic form, \hat{f} is as well.

Theorem 14.6 (Canonical Height Descent).

Let $h : A \rightarrow \mathbb{R}$ be a quadratic form and suppose $\exists n \geq 2$ such that

1. $\text{coker } A \xrightarrow{\times 2} A = A/nA < \infty$,
2. The Northcott property holds, i.e. $\{x \in A \mid h(x) \leq R\} < \infty$ for each $R \in \mathbb{R}$,

Letting y_1, \dots, y_r be coset representatives for $nA \subset A$ and $C_0 := \max h(y_i)$, then A is generated by the finite set $\{x \in A \mid h(x) \leq C_0\}$.

Proof: Omitted.

Next up: the Néron-Tate height is indeed a quadratic form.

Theorem 14.7.

Let K be a global field, A/K an abelian variety, D ample and $\ell(D) \geq 2$ with $[D]$ symmetric. Then there exists a unique function $\hat{h}_{A,D} : A(K^{\text{sep}}) \rightarrow \mathbb{R}$ such that

1. $\hat{h}_{A,D} = h_{A,D} + O(1)$
2. $\hat{h}_{A,D}$ is a *quadratic form* (stronger conclusion), and in particular $\hat{h}_{A,D}([n]p) = n^2 \hat{h}_{A,D}(p)$.

Proof.

We have 1, we'll show 2 by establishing the parallelogram law and use a previous lemma.

Note ϕ is suppressed here, since by uniqueness, multiplication by n always yields the same function. So we'll take multiplication by 2.

For all $P, Q \in A(K^{\text{sep}})$, we can compute

$$\begin{aligned} \hat{h}_{A,D}(P+Q) + \hat{h}_{A,D}(P-Q) &= \lim 4^{-n} (h_{A,D}([2^n]P + [2^n]Q) + h_{A,D}([2^n]P - [2^n]Q)) \\ &= \lim 4^{-n} (2h_{A,D}([2^n]P) + 2h_{A,D}([2^n]Q) + O(1)) \\ &= 2\hat{h}_{A,D}(P) + 2\hat{h}_{A,D}(Q). \end{aligned}$$

■

15 Monday February 17th

Theorem 15.1.

If A/K is an abelian variety, $D \in \text{Div}(A)$, ample, $\ell(D) \geq 2$, $[D]$ symmetric, then there exists a canonical height $\hat{h}_{A,D} : A(K^{\text{sep}}) \rightarrow \mathbb{R}$ such that

1. $\hat{h}_{A,D} = h_{A,D} + O(1)$
2. $\hat{h}_{A,D}$ is a *quadratic form* (defined last time).

In particular, $\hat{h}_{A,D} \circ [n] = n^2 \hat{h}_{A,D}$. We can define an associated bilinear form

$$\langle P, Q, \rangle = \frac{1}{2} \left(\hat{h}_{A,D}(P + Q) - \hat{h}_{A,D}(P) - \hat{h}_{A,D}(Q) \right),$$

so consider the linear extension

$$\begin{aligned} \hat{h}_{A,D} A(K^{\text{sep}}) \otimes \mathbb{R} &\longrightarrow \mathbb{R} \\ \sum_{i=1}^n [P] \otimes \alpha_i &\mapsto \sum_{i=1}^n \alpha_i \hat{h}_{A,D}. \end{aligned}$$

Exercise This yields a quadratic form on the domain.

Question: What is $\ker(A(K^{\text{sep}}) \longrightarrow A(K^{\text{sep}}) \otimes \mathbb{R})$?

Answer: It contains the torsion, but turns out to be precisely this. Note that $\ker(M \longrightarrow M \otimes \mathbb{Q}) = M[\text{tors}]$, and we can tensor up in two steps: $A(K^{\text{sep}}) \otimes_{\mathbb{Z}} \mathbb{R} = (A(K^{\text{sep}}) \otimes_{\mathbb{Z}} \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{R} = A(K^{\text{sep}})[\text{tors}] \otimes_{\mathbb{Q}} \mathbb{R}$.

Theorem 15.2.

With the same setup as the previous theorem, the linear extension is *positive definite*, i.e.

$$q(x) \geq 0 \ \forall x \quad \text{and} \quad q(x) = 0 \iff x = 0$$

Definition 15.1.

If $P_1, \dots, P_n \in A(K^{\text{sep}}) \otimes \mathbb{R}$ are \mathbb{R} -linearly independent, then we can define the *regulator*

$$\text{Reg}(P_1, \dots, P_n) := \det(\langle P_i, P_j \rangle) > 0.$$

Note that this is the determinant of the Gram matrix, forms can be diagonalized into $\sum a_i x_i^2$, and positive-definite implies $a_i \geq 0$?

If $\{P_i\}$ is a \mathbb{Z} -basis for $A(K^{\text{sep}})/A(K^{\text{sep}})[\text{tors}]$, then we define $\text{Reg}(A, K, D) := \det(\langle P_i, P_j \rangle) > 0$.

This is well-defined for exactly the same reason that the discriminant of a number field is well-defined.

Proof.

Mostly algebra, mostly omitted here. Uses the following lemma. ■

Lemma 15.3.

Let $A \cong \mathbb{Z}^n$ and $q : A \longrightarrow \mathbb{R}$ be a quadratic form such that

1. For all $x \in A$, $q(x) \geq 0$ and $q(x) = 0 \iff x = 0$,
2. The Northcott Property holds, i.e. $\forall R \in \mathbb{R}, \# \{x \in A \mid q(x) \leq R\} < \infty$.

Then $q \otimes \mathbb{R} : A \otimes \mathbb{R} \longrightarrow \mathbb{R}$ is still positive-definite.

Example: See Cassels-Silverman. Let K be a real quadratic field, e.g. $K = \mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$. Define $q : A \rightarrow \mathbb{R}, x \mapsto x^2$; this is positive-definite but for $q \otimes \mathbb{R}$, there exist $x \neq 0$ such that $q(x) = 0$.

Note: There exists a **canonical** canonical height which is used for the BSD conjecture.

Step 1: For elliptic curves E/K , $D = 2[O] \iff D_x$ where $x : E \rightarrow \mathbb{P}^1$ is taking the x -coordinate, note that if $y^2 = f(x)$, then $x([-P]) = x([P])$ making this an even function. So taking the quotient $E \xrightarrow{q} E/[-1]$ yields a 2-to-1 map, which factors through an isomorphism $E/[-1] \cong \mathbb{P}^1$. However, $2[-O] = [-1]^*D = D$, but we also have $2[O] = x^*([\infty])$. Then $K(x) \subset K(E)$ contains all of the even functions, i.e. every even function is a function of the x -coordinate. So take any rational function $f \in K(x) \setminus K$ yields a composition $F : E \xrightarrow{x} \mathbb{P}^1 \xrightarrow{f} \mathbb{P}^1$ where $\deg(F) = 2 \deg(f)$.

Define $D_f = F^*([\infty])$, which is a pullback of a symmetric function (since x is only a function of one coordinate), so $[-1]^*D_f = D_f$, so D_f is a symmetric divisor. Moreover, $\deg D_f = 2 \deg f$. Take $\hat{h}_{E,f} = \hat{h}_{E,D_f}$, since by Riemann-Roch the number of sections is at least 2. How does this depend on f ? Does the regulator depend on f ?

There is a dependence, but it's understandable enough to be removed at the end.

We can apply the Weil Height Machine, and a comparison shows $h_{E,D_f} = (\deg f)h_{E,D_x} + O(1)$. Therefore $\hat{h}_{E,D_f} = (\deg f)\hat{h}_{E,D_x}$ on the nose. By a computation, $\text{Reg}(E, D_f) = \deg(f)^n \text{Reg}(E, D_x)$ where $n = \text{rank}(E(K))$. So there is a dependence, but nothing too scary.

Silverman defines the canonical height in the curve case as

$$\hat{h}_E := \frac{\hat{h}_{E,D_f}}{2 \deg f}.$$

Step 2: For abelian varieties, define a height pairing $\hat{h} : A(K^{\text{sep}}) \times A^\vee(K^{\text{sep}}) \rightarrow \mathbb{R}$, where the dual variety is defined such that the functor of points $A^\vee \iff \text{Pic}^0(A)$, where $A^\vee(K) = \text{Pic}^0(A)$.

There is a (well-defined up to linear equivalence) *Poincare divisor* $\mathcal{P} \in \text{Div}(A \times A^\vee)$ which is ample and symmetric. We can then define $\hat{h}_{A \times A^\vee, \mathcal{P}}$ and take the associated bilinear form

$$\langle \cdot, \cdot \rangle_{A \times A^\vee, \mathcal{P}} : (A(K) \times A(K^{\text{sep}}))^2 \rightarrow \mathbb{R}.$$

So choose bases P_1, \dots, P_R for the Mordell-Weil group mod torsion $A(K)/\text{tors}$, and by isogeny, a basis Q_1, \dots, Q_R of $A^\vee(K)/\text{tors}$. Then define $\text{Reg}(A, K) := |\det \langle P_i, Q_j \rangle| > 0$.

Note that swapping signs in the basis changes the determinant by ± 1 , hence the absolute value. This is the regulator that appears in the BSD conjecture.

Recall Mumford's formula: If $D \in \text{Div}(A)$, then

$$[n]^*D \sim \left[\frac{n^2 + n}{2} \right] D + \left[\frac{n^2 - n}{2} \right] [-1]^*D.$$

If D is symmetric, then $[n]^*D \sim n^2D$, i.e. the quadratic eigendivisor condition. In this case $\hat{h}_{A,D}$ is a quadratic form.

If D is skew-symmetric, i.e. $[-1]^*D = -D \iff D \in \text{Pic}^0(A)$, then $[n]^*D = nD$ and we obtain a linear eigendivisor condition.

Note: $D \in \text{Pic}^0(A)$ means algebraically equivalent to zero.

If $D \in \text{Pic}^0(A)$, then $\hat{h}_{A,D} : A(K^{\text{sep}}) \rightarrow \mathbb{R}$ is a linear form. By the Weil Height Machine, up to $O(1)$ we have $\hat{h}_{A,D_1+D_2} = \hat{h}_{A,D_1} + \hat{h}_{A,D_2}$. So we do have a bilinear pairing

$$\langle \cdot, \cdot \rangle : A(K^{\text{sep}})^2 \rightarrow \mathbb{R}$$

$$(P, Q \iff D \in \text{Div}(A) \text{ after extending bases }) \mapsto \hat{h}_{A,D}(P) \in \mathbb{R}.$$

Note: we could equivalently define it on $A(L)$ for every finite separable extension L/K .

This explains the regulator appearing in BSD. This concludes the discussion of height functions and the Mordell-Weil group.

16 Monday February 24th

16.1 Classification of Locally K -Analytic Lie Groups

Let K be a locally compact field with discrete valuation, R a valuation ring with $\mathfrak{m} = (\pi)$ its maximal ideal where $R/\mathfrak{m} \cong \mathbb{F}_q = \mathbb{F}_{p^a}$. There are two cases:

- If $\text{char } K = 0$, then $\mathbb{Q}_p \subset K$ and $d = [L : \mathbb{Q}_p]$
- If $\text{char } K = p > 0$, then $K \cong \mathbb{F}_q((t))$.

Fact (Lie Theoretic) Let G be a compact commutative g -dimensional K -analytic lie group (i.e. locally looks like k^n with transition harts given by convergent power series) which is 2nd countable.

- There exists a filtration by open subgroups $G = G^0 \supset G^1 \supset \dots \supset G^n \supset \dots$ such that
 - G^0/G^i is finite and discrete for all i ,
 - $G^i \cong (\mathfrak{m}^i)^g$, with addition given by a g -dimensional formal group law,
 - $\bigcap G^i = (0)$, so the filtration is exhaustive,
 - G/G^{i+1} is p -torsion,
 - $G^1[\text{tors}] = G^1[p^\infty]$
- If $\text{char } (K) = 0$, then there exists an open subgroup U of G such that $U \cong (R^g, +)$ as K -analytic Lie groups.

Analog in Lie theory: Lie groups with isomorphic Lie algebras yield isomorphic universal covers. Can then recover the formal group from the Lie algebra. Wildly false in characteristic p , since we lose information about the height of the formal group.

Theorem 16.1 (C-Lacy). a. If $\text{char } (K) = 0$ (i.e. in a p -adic field), then $G \cong (R, +)^g \oplus G[\text{tors}]$ as topological groups, where $G[\text{tors}]$ is finite, which is in turn isomorphic to

$$\mathbb{Z}_p^{dg} \oplus G[\text{tors}].$$

- b. If $\text{char}(K) = p$, then there exists a countable set I such that $G \cong \prod_{i \in I} \mathbb{Z}_p \oplus G[\text{tors}]$ as topological groups, where each of the groups on the RHS are closed subgroups. Moreover, $G[\text{tors}] < \infty \iff G[p] < \infty$, and when these conditions hold, I is infinite.


Lemma 16.2.

If H is a commutative torsionfree pro- p group, then $H \cong \prod_{i \in I} \mathbb{Z}_p$. If H is 2nd countable, then I is countable.

Proof (of Lemma, sketch).

We'll take *Pontryagin duals*. Recall that if G is an locally compact abelian (LCA) group, then $G^\vee := \text{hom}(G, \mathbb{R}/\mathbb{Z})$ is an LCA group. Note that the dual of a profinite group (inverse limit) is an ind-finite group (direct limit), which are discrete torsion groups.

H^\vee is a discrete p -primary torsion group. Example: $\mathbb{Z}_p^\vee = \mathbb{Q}_p/\mathbb{Z}_p$, which flips the following exact sequence:

$$0 \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Q}_p \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0$$


Then $H^\vee = [p]H^\vee$, and thus H^\vee is divisible. We then apply the structure theory of divisible group to get a direct sum, then applying duality again yields a direct product, which proves the lemma. ■

Proof (of Theorem).

Assume that $G[\text{tors}]$ is finite. We have a SES of commutative profinite groups:

$$0 \longrightarrow G[\text{tors}] \longrightarrow G \longrightarrow G/G[\text{tors}] \longrightarrow 0,$$

and taking Pontryagin duals yields

$$0 \longrightarrow (G/G[\text{tors}])^\vee \longrightarrow G^\vee \longrightarrow G[\text{tors}]^\vee.$$

Then $G/G[\text{tors}]$ is torsionfree and has a finite index pro- p subgroup, so $G/G[\text{tors}]$ is itself a pro- p group. By the lemma, $G/G[\text{tors}] \cong \prod_{i \in I} \mathbb{Z}_p$, so

$$(G/G[\text{tors}])^\vee \cong \bigoplus_{i \in I} \mathbb{Q}_p/\mathbb{Z}_p.$$

But this is divisible, and hence injective since we're over a PID, so the dual sequence above splits. So the original sequence splits.

We thus have an isomorphism of topological groups

$$G \cong G/G[\text{tors}] \oplus G[\text{tors}] \cong \prod_{i \in I} \mathbb{Z}_p \oplus G[\text{tors}],$$

where $G[\text{tors}]$ was assumed finite.

Suppose $\text{char}(K) = 0$. We have two open subgroups of G , $\prod_{i \in I} \mathbb{Z}_p \leq G$ (open since its complement is finite) and $(R, +)^g \cong \mathbb{Z}_p^{dg}$ by Serre. It follows that $|I| = dg$.

Suppose instead that $\text{char}(K) > 0$. The claim is that $[G : pG]$ is infinite and thus $|I|$ is infinite. This is because the cokernel of multiplication by p on $\prod \mathbb{Z}_p \oplus G[\text{tors}]$ is infinite iff I is infinite, so it suffices to check the size of this cokernel.

Consider the formal group law in characteristic p given by

$$[p] \in R[[X_1^p, \dots, X_g^p]]^g.$$

It suffices to restrict to $G^1 = (t\mathbb{F}_q[[t]]^g, \text{fgl})$. Then $pG_1 \subseteq t\mathbb{F}_q[[t]]^g \cap \mathbb{F}_q[[t^p]]^g$. But $[\mathbb{F}_q[[t]] : \mathbb{F}_q[[t^p]]]$ is infinite, so $[G : pG_1]$ is infinite, so $[G : pG]$ is infinite and thus I is infinite. ■

If we know the torsion is finite, can we find bounds on their size? We'll need to revisit Néron models (as covered in the abelian varieties course), and introduce Tate curves.

17 Wednesday February 26th

Example 17.1 (regarding generalization from last time).

Let $G = \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$, which is a commutative pro- p group. Then

$$\oplus \mathbb{Z}_p^n \mathbb{Z} (?) \subsetneq G[\text{tors}] \subsetneq G$$

with proper containments, but the direct sum is dense in the direct product, so $G[\text{tors}]$ is proper and dense and thus not closed.

17.1 (Clark-Xarles) Local Bounds for Torsion Points on Abelian Varieties

Recommended reading! Introduces a lot of tools in their most basic form.

Let K/\mathbb{Q}_p be a p -adic field with $[K : \mathbb{Q}_p] = d$, R a valuation ring, \mathfrak{m} a maximal ideal, $\mathbb{F}_q = R/\mathfrak{m}$.

Recall previously: finiteness on torsion subgroups in certain cases. Mordell-Weil works for global fields, but what is that finite group? No positive results bounding the torsion for a Laurent series field, can be arbitrary large.

Let A/K be a g -dimensional abelian variety and recall

$$A(K) \cong_{\text{TopGrp}} (R, +)^g \oplus T \cong \mathbb{Z}_p^{dg} \oplus T,$$

where $|T| < \infty$

We'll prove bounds in three steps:

1. Good reduction
2. Potentially good reduction
3. General reduction and results in the case of *anisotropic reduction*.

17.2 Good Reduction

Definition 17.1.

A/K has *good reduction* if there exists a smooth group scheme A/R with generic fiber A/K .

Noting that $\text{Spec}(R) = \{(0), (\pi)\}$ is a two point space, we have the fibers

$$\begin{array}{ccc} A & A/K & A/\mathbb{F}_q \\ \downarrow & \downarrow & \downarrow \\ \text{Spec}(R) & (0) & (\pi) \end{array}$$

We get a SES

$$0 \longrightarrow A' \longrightarrow A(R) \xrightarrow{\text{reduction}} A(\mathbb{F}_q) \longrightarrow 0$$

and the fact that it is surjective is due to **Hensel's lemma**. Here $A' = \mathfrak{m}^g$ endowed with a formal group law. Since we have a projective variety, we can clear denominators to replace $A(R)$ with $A(K)$ in the above sequence. Note that the quotient is precisely a Mordell-Weil group, so using the Weil conjectures, we can say quite a bit about its size.

Thus $A' \hookrightarrow A(K)$ is an open finite-index subgroup. Moreover, all of the torsion is p -primary, and $A'[\text{tors}] = A'[p^\infty]$. Define $G[\text{tors}]'$ to be the torsion that is prime to p . If the kernel is p -primary torsion, then the reduction map induces an isomorphism

$$r : A(K)[\text{tors}]' \xrightarrow{\cong} A(\mathbb{F}_q)[\text{tors}]'.$$

Theorem 17.1 (Weil, Serre Improved Weil Bounds).

$\#A(\mathbb{F}_q) \leq \left\lfloor (1 + \sqrt{q})^2 \right\rfloor^g$. (Note that Weil's original bound is just this without the floor function.)

Therefore, for A/K and K/\mathbb{Q} a number field of degree d , choose $\mathfrak{p}_1, \mathfrak{p}_2$ in $\text{Spec}\mathbb{Z}_k$ points of good reduction. Then

$$\#A(K)[\text{tors}] \leq \left\lfloor \left(1 + p_1^{\frac{d}{2}}\right)^2 \right\rfloor^g \left\lfloor \left(1 + p_2^{\frac{d}{2}}\right)^2 \right\rfloor^g.$$

Note: potentially “blah” always means “blah” after some base extension.

17.3 Potentially Good Reduction

Definition 17.2.

Let K be a p -adic field, then A/K has *potentially good reduction* iff there exists a finite degree extension L/K such that base extending to L , A/L , has good reduction.

Proposition 17.2.

$$\#A(K)[\text{tors}]' \leq \left\lfloor (1 + \sqrt{q})^2 \right\rfloor^g.$$

Remark If $\text{End}(A)$ is “large enough”, e.g. if A has X -multiplication for $X = \mathbb{C}, \mathbb{H}$ (complex or quaternionic) then A must have potentially good reduction (see Pete’s thesis).

Proof.

Serre-Tate observed that if you have potentially good reduction, it can always be obtained via a totally ramified extension L/K . That is, if S is the valuation ring of L and \mathfrak{m}_S is its maximal ideal, then $S/\mathfrak{m}_S \cong \mathbb{F}_q$, so it doesn’t change the size of the residue field. Applying step 1 over L yields a bound. ■

Application If E/\mathbb{Q} is an elliptic curve with potentially good reduction over 2, 3 (i.e. the j -invariant doesn’t have 2 or 3 in the denominator). Applying the bound yields

$$\begin{aligned} \#E(\mathbb{Q})[\text{tors}] &\leq \left\lfloor (1 + \sqrt{2})^2 \right\rfloor \left\lfloor (1 + \sqrt{3})^2 \right\rfloor \\ &= (5)(7) \\ &= 35. \end{aligned}$$

Note that a much harder theorem yields a tighter bound at 15, but this is much easier and not much worse of a bound.

Taking now A/\mathbb{Q} with $\dim A = 2$ with the same conditions yields $\#A(\mathbb{Q})[\text{tors}]' \leq (35^2) = 1225$.

Note that without this minor observation, the known bound is astronomically larger!

Theorem 17.3 (C-Xarles).

Fix A/\mathbb{Q} with $\dim A = 2$ and everywhere potentially good reduction. Then

$$\#A(\mathbb{Q})[\text{tors}] \in [1, 16] \cup [18, 20] \cup \{22, 24, 25, 28, 30, 36, 48, 60, 72\}$$

Conversely, $[1, 10] \cup \{12, 16, 18, 19, 20, 24, 36\}$ are known to occur.

Note that for elliptic curves over \mathbb{Q} , it’s $\{1, 2, 4, 6\}$.

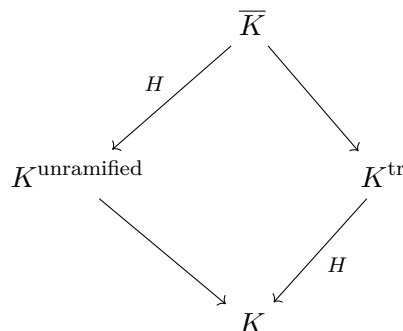
Proof (Sketch).

For K a p -adic field, the absolute unramified extension has galois group $\widehat{\mathbb{Z}}$, then extend to \overline{K} with galois group H to obtain a SES

$$1 \longrightarrow H \longrightarrow g_K \longrightarrow \widehat{\mathbb{Z}} \longrightarrow 0$$

Since $\widehat{\mathbb{Z}}$ is a free profinite group, thus a projective object in that category of profinite groups, so this sequence splits and $g_K \cong \widehat{\mathbb{Z}} \oplus H$. ■

What does this buy us? We can think of the subgroup H now as a quotient, so there is a $K^{\text{tr}} \leq \overline{K}$ such that $\text{Aut}(K^{\text{tr}}/K) = H$, i.e. we have a compositum



Thus $\overline{K} = K^{\text{unramified}} \times K^{\text{tr}}$.

17.4 General Reduction

Let A/K be an abelian variety, A/R the Néron model, which is a smooth finite type group R -group scheme with generic fiber A/K and $A(K) = A(R)$. There is a reduction map $A' \rightarrow A(R) \xrightarrow{r} A(\mathbb{F}_1) \rightarrow 0$ given by reduction, which is again surjective by Hensel's lemma.

Here the kernel A' is exactly as before, obtained by evaluating a g -dimensional formal group law on \mathfrak{m}^g . The difference here is that $A(\mathbb{F}_q)$ is no longer an abelian variety, and instead the group of \mathbb{F}_q rational points of a commutative algebraic group over \mathbb{F}_q .

There is structure theory of commutative algebraic groups, which may be disconnected, so we'll need to consider things like the component group – but this can be arbitrarily large, which can be an issue.

18 Friday February 28th

Continuing Clark-Xarles paper on torsion points of abelian varieties A/k , where $[k : \mathbb{Q}_p] = ef$ and $q = p^f$. If A/k has potentially good reduction, the prime to p torsion injects into the torsion of the residue field, which gave an estimate

$$\#A(k)[\text{tors}]'(\text{prime to } p) \leq \left\lfloor (1 + \sqrt{q})^2 \right\rfloor^g = \lfloor q + 2\sqrt{q} + 1 \rfloor^g$$

Can also get a bound on $\#A(k)[p^\infty]$ in terms of p, g, e , and if $p \gg e$, the bound is precisely 1.

We want to generalize this: let R be a valuation ring, then there exists a finite type smooth commutative (not necessarily proper) R -group scheme A/R with generic fiber A/k , the Néron model, such that $A(R) = A(K)$ and

$$0 \rightarrow A'(R) \rightarrow A(R) = A(k) \xrightarrow{r} A(\mathbb{F}_q) \rightarrow 0.$$

Note that $A'(R)$ here comes from a formal group law.

For A/\mathbb{F}_q a smooth commutative algebraic group, and A/k has good reduction $\iff A/\mathbb{F}_q$ is an abelian variety.

We obtain

$$0 \longrightarrow A^0/\mathbb{F}_q \longrightarrow A/\mathbb{F}_q \longrightarrow \Phi \longrightarrow 0,$$

where the first entry is the component group and the third is a finite etale \mathbb{F}_q -group scheme. Identify Φ with $\Phi(\overline{\mathbb{F}}_q)$ as a $g_{\mathbb{F}_q}$ -module, then $\Phi(\mathbb{F}_q) = \Phi^{g_{\mathbb{F}_q}}$ coming from a Galois action.

Note that A^0/\mathbb{F}_q is a connected commutative smooth algebraic group over the perfect field \mathbb{F}_q , so we can apply some classification theory.

18.1 The Chevalley Decomposition

Let k be any perfect field and G/k be a commutative connected algebraic group, then there exists a unique SES of such groups

$$0 \longrightarrow T \oplus U \longrightarrow G \longrightarrow B \longrightarrow 0.$$

Plugging in \bar{k} points would yield a SES of Galois modules. Plugging in k points may not work, because a surjection of elliptic curves (isogeny) is not necessarily surjective on k -points. Say $\dim G = g, \dim B = \beta$ be the abelian ranks.

Since B/k is an abelian variety, T/k is a linear torus and $T/\bar{k} = \mathbb{G}_m^\mu$, so define $\dim T = \mu$ the “toric rank”. Then U/k is a commutative unipotent *linear algebraic group*, so it embeds in some $\mathrm{GL}(n, k)$ with eigenvalues only 1. Note that $\mathbb{G}_a = \{[1, x; 0, 1] \mid x \in k\}$, and anything here will be a repeated extension of the additive group. Let $\alpha = \dim U$ be the additive rank.

If A/\mathbb{F}_q is an abelian variety of dimension β , we have the bound $\#A(\mathbb{F}_q) \leq [q + 2\sqrt{q} + 1]^\beta$, if $T_{\mathbb{F}_q}$ is a torus of dimension u , then $\#T(\mathbb{F}_q) \leq (q + 1)^\mu$. Note that if $\dim T = 1$, then T is isomorphic to either \mathbb{G}_m or $N = \ker(\mathbb{G}_m/\mathbb{F}_{q^2} \longrightarrow \mathbb{G}_m/\mathbb{F}_q)$ (Weyl restriction) over \mathbb{F}_q . Moreover, $N(\mathbb{F}_q) = \ker(\mathbb{F}_{q^2}^\times \longrightarrow \mathbb{F}_q^\times)$ which is cyclic of order $q + 1$.

Note that if we have a nodal cubic, and the group splits to \mathbb{G}_m if the slopes of the two tangents at the node do (??) lie in \mathbb{F}_q , and lands in the second case if the slopes are Galois conjugate.

If U/\mathbb{F}_q is a commutative unipotent algebraic group of dimension α , then $\#U(\mathbb{F}_q) = q^{[\alpha]}$, the number of points of \mathbb{G}_m^α (?).

We'll find a filtration

$$0 = G^3 \subset G^2 \subset G^1 \subset G^0 = A(k).$$

Take G^1 to be the points reducing into $A^0(\mathbb{F}_q)$, i.e. $\ker(A(k) \xrightarrow{r} A(\mathbb{F}_q) \xrightarrow{?} \Phi(\mathbb{F}_q))$. Then $G^0/G^1 \hookrightarrow \Phi(\mathbb{F}_q)$. Take $G^2 = \ker(A(k) \xrightarrow{r} A(\mathbb{F}_q))$, then $G^1/G^2 \hookrightarrow A^0(\mathbb{F}_q)$. Note that G^2 comes from the formal group law.

Now let $T^i = G^i \cap A(k)[\mathrm{tors}]$, then

$$\#A(k)[\mathrm{tors}]' \leq \#\Phi(\mathbb{F}_q)\#A^0(\mathbb{F}_q), ,$$

and since we know everything about $A^0(\mathbb{F}_q)$, we have

$$\#A(k)[\text{tors}]' \leq \#\Phi(\mathbb{F}_q) \lfloor q + 2\sqrt{q} + 1 \rfloor^\beta (q+1)^\mu.$$

Note that q^α is p -torsion, so we don't need the unipotent piece here.

Theorem 18.1 (Lestre-Oort).

Suppose $\mu = 0$, so no toric part. Then $\#\Phi' \leq 2^{2\alpha} \leq 2^{2g}$.

Thus if $\mu = 0$, we have

$$\#A(k)[\text{tors}]' \leq \#\Phi(\mathbb{F}_q) \lfloor q + 2\sqrt{q} + 1 \rfloor^\beta (q+1)^\mu 2^{2\alpha}.$$

Noting that $\alpha + \mu + \alpha = g$, this can give a better bound than in the case of good reduction.

Definition 18.1.

Let T/k be a torus, then T is *anisotropic* iff there does not exist an embedding $\mathbb{G}_m \hookrightarrow T$ over k .

A/k has *anisotropic reduction* (or AR) iff the toric part is anisotropic.

Theorem 18.2 (Clark-Xarles).

If A/k has anisotropic reduction, then

$$\begin{aligned} \#A(k)[\text{tors}]' &\leq \#\Phi(\mathbb{F}_q) \lfloor q + 2\sqrt{q} + 1 \rfloor^\beta (q+1)^\mu 2^\alpha \\ &\leq \lfloor q + 2\sqrt{q} + 1 \rfloor^g. \end{aligned}$$

This generalizes the potentially good reduction case, since p.g.r. implies anisotropic.

Next up: need to understand p -adic uniformization of abelian varieties, and particularly for abelian varieties.

19 Friday March 6th

Analytic uniformization, beginning of discussion about Tate curves. Gives us a way to use analysis to understand a variety.

Tate curves: let $(K, |\cdot|) = \mathbb{R}, \mathbb{C}$ or a complete nonarchimedean field. Recall that if K is p -adic, then $(K, +)$ has no nontrivial lattices (closed, discrete subgroups). For \mathbb{C} we have an infinite-dimensional covering map $\exp : \mathbb{C}/\mathbb{Z} \xrightarrow{z \mapsto e^{2\pi iz}} (\mathbb{C}^\times, \cdot)$ which is an isomorphism of \mathbb{C} -lie groups.

If $\tau \in \mathbb{H}$ and $\Lambda_s = \langle 1, \tau \rangle$, then taking the exponential yields $C/\Lambda_s \xrightarrow{\exp} \mathbb{C}^\times / \langle q_\tau \rangle$ where $q_\tau = e^{2\pi i\tau}$ and $0 < |q_\tau| < 1$, which is a type of “additive uniformization”.

Thus if E/\mathbb{C} is any elliptic curve, then there exists such a $q \in \mathbb{C}$ such that $E(\mathbb{C}) \cong C^\times / \langle q \rangle$.

Remark: The map $q \mapsto j(q)$ is generally not injective. Note that j factors through the quotient

$$\begin{array}{ccc}
 j\mathbb{H} & \xrightarrow{\quad} & \mathbb{C} \\
 & \searrow \text{dashed} & \uparrow \cong \\
 & & \mathfrak{sl}(2, \mathbb{Z}) \backslash \mathbb{H}
 \end{array}$$

In other words, for $(a, b; c, d) \in \mathfrak{sl}(2, \mathbb{Z})$ we have $j(\tau) = j\left(\frac{a\tau + b}{c\tau + d}\right)$. The indeterminacy here is given by $e^{2\pi i\tau_1} = e^{2\pi i\tau_2}$ iff $j_2 = j_1 + b$ for some $b \in \mathbb{Z}$ and $(1, b; 0, 1)\xi = \xi + b$.

Last time we saw that $(K, |\cdot|)$ is locally compact and $q \in K$ with $0 < |q| < 1$, then $\langle q \rangle = q^{\mathbb{Z}}$ is a full lattice in K^\times . Proof last time, a one-liner using compactness of the unit ball.

Exercise If $\Lambda \in K^\times$ is a full lattice (discrete, closed, compact quotient/cocompact), then $\Lambda = q^{\mathbb{Z}}$ for a unique q with $0 < |q| < 1$. The content: can't take $|q| = 1$. Think about what happens if you take a p -adic field and start taking powers, see what it is dense in.

Modding out by finite group doesn't lose compactness.

Exercise What are the full lattices in $(K^\times)^g$? Higher dimensional abelian varieties are also uniformized by lattices in \mathbb{C}^g . Claim: all isomorphic to \mathbb{Z}^g .

Exercise For $K = \mathbb{R}$, $0 < |q| < 1$, then

$$R^\times / \langle q \rangle \cong \begin{cases} \mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & q > 0 \\ \mathbb{R}/\mathbb{Z} & q < 0 \end{cases}.$$

Primary source material for Tate Curves: Silverman Chapter 5

In fact, for all E/\mathbb{R} there exists a $0 < |q| < 1$ such that $E(\mathbb{R}) \cong E_q$ as \mathbb{R} -lie groups, where $E_q \cong \mathbb{R}^\times / \langle q \rangle$. So the Tate parameter q is telling you whether or not 2-torsion exists. Also relates sign of q to sign of discriminant. Can take q series in the sense of modular forms, starting next week.

Note: these q series will still converge in K .

For our purposes, take $(K, |\cdot|)$ a complete nonarchimedean field, $0 < |q| < 1$ in K , $E_q := K^\times / \langle q \rangle$ is a compact commutative 1-dimensional K -analytic lie group.

How all of this will end up working:

Theorem 19.1 (Tate, Part A).

For $(K, |\cdot|)$ a complete nonarchimedean field and q a Tate parameter, there exists an elliptic curve E_q/K and a K -analytic group isomorphism

$$\phi : K^\times / \langle q \rangle \xrightarrow{\cong} E_q(K)$$

Moreover, E_q has split multiplicative reduction.

Theorem 19.2 (Tate, Part B).

Moreover, for all finite extensions L/K , note that we can extend the norm to the algebraic

closure uniquely (by Number Theory II), and the following diagram commutes

$$\begin{array}{ccc} K^\times / \langle q \rangle & \longrightarrow & E_q(K) \\ \downarrow & & \downarrow \\ L^\times / \langle q \rangle & \longrightarrow & E_q(L) \end{array}$$

Taking the \varinjlim over finite L/K , $\phi : \overline{K}^\times / \langle q \rangle \xrightarrow{\cong} E_q(\overline{k})$. Moreover, ϕ is equivariant for $\text{Aut}(\overline{K}/K)$, i.e. for all $\sigma \in \text{Aut}(\overline{k}/k)$ and $x \in \overline{K}^\times / \langle q \rangle$, $\phi(\sigma x) = \sigma(\phi x)$. For $N \in \mathbb{Z}^+$ with $\text{char } K \nmid N$, we have $E_q[N] \cong (K^{\text{sep}})^\times / \langle q \rangle [N]$ as g_K -modules. Note that μ_N is a subgroup of the RHS, which is fixed under the galois action.

Punch line: every elliptic curve comes with a unique order N subgroup which is galois-invariant. Thus we reduce the question of computing the galois module structure of torsion points to a qual-level algebra problem of computing galois extensions.

Theorem 19.3 (Tate, Part C).

Suppose K is discretely valued, $|x| = C^{-v(x)}$, $v(K^\times) = \mathbb{Z}$. Then E_q has **split** multiplicative reduction (by A), and $v(j(E_q)) = v\left(\frac{1}{q}\right) = -v(q) \in \mathbb{Z}^+$. This implies that the component group of the Néron special fiber is *constant* and isomorphic to $\mathbb{Z}/v(q)\mathbb{Z}$.

See Kodaira-Néron classification

Major difference: only uniformizing curves with split multiplicative reduction, as opposed to all curves in \mathbb{R}, \mathbb{C} case.

Theorem 19.4 (Tate, Part D).

For all $j \in K$ with $|j| > 1$, there exists a unique $q \in K$ such that $0|q| < 1$ and $j(E_q) = j$. So the Tate parameter is uniquely recovered.

For every q , we build a curve E_q , and get a galois structure on its torsion points. They must have split multiplicative reduction, and every such curve is isomorphic to E_q for a unique q . Pretty strong result!

Theorem 19.5 (Tate, Part E).

Assume $\text{char } K \neq 2$. If E/K is any elliptic curve with $|j(E)| > 1$ (so not integral), then there exists a unique q such that E/K is a *quadratic twist* of E_q/K . For $K(\sqrt{\alpha})/K$, we have $E/K(\sqrt{\alpha}) \cong E_q/K(\sqrt{\alpha})$. Moreover,

$$E/K \text{ has } \begin{cases} \text{split multiplicative reduction} & K(\sqrt{\alpha}) = K \sim \mathbb{G}_m \\ \text{non-split multiplicative reduction} & K(\sqrt{\alpha})/K \text{ is unramified} \sim T \text{ a nonsplit torus} \\ \text{additive reduction} & K(\sqrt{\alpha})/K \text{ is ramified} \end{cases} .$$

Remark: the torsion can be arbitrarily large.

Example 19.1.

Take $K = \mathbb{Q}_p$ and $q = p^n$ so $|p^n| < 1$. Then $E_q(\mathbb{Q}_p) \cong \mathbb{Q}_p^\times / \langle p^n \rangle$. What is the torsion subgroup? Note that roots of unity in \mathbb{Q}_p inject into the quotient, and $\mu(\mathbb{Q}_p) \cong \mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)$ (by Number Theory II). The class of p is order n , and thus also torsion, so $T \cong \mathbb{Z}/(p) \times \mathbb{Z}/(p-1)$, where the containment is obvious and staring at this calmly will show that this in fact the entire torsion subgroup.

In general, for $(K, |\cdot|)$ discretely valued, it's easy to give an upper bounds. We have $E_q(K)[N] \hookrightarrow \mu_N(K) \times Z$, where Z is cyclic of order $v(q)$. Equality occurs if (not iff) q is a perfect $v(q)$ th power.

Taking $E_q(\overline{K})[N]$ is generated by ζ_n , a primitive n th root of unity, and any n th root of q , $q^{\frac{1}{n}}$. Thus this is literally a Kummer extension, and this is no big deal to work out.

The culprit: the component group can be arbitrarily large!