Elliptic Curves

D. Zack Garza

February 24, 2020

Contents

1 Wednesday January 8 **2**

2 Mordell-Weil Groups **2**

3 Monday January 13th **4**

4 Wednesday January 15th **6**

5 Friday January 17th **8**
5.1 Continuing Step 3 8
5.2 Step 4 9

6 Wednesday January 22nd **10**
6.1 Step 1: 10
6.2 Step 2 11

7 Friday January 24th **12**
7.0.1 Step 3 13
7.0.2 Step 4: Number Theory 15

8 Monday January 27th **16**
8.1 Weak Mordell-Weil: Finishing the Proof 16
8.2 Height Functions 17

9 Wednesday January 29th **18**
9.1 Height Functions 18

10 Friday January 31st **20**
10.1 Height Functions 21

11 Monday February 3rd **22**

12 Friday February 7th **24**
12.1 Weil Height Machine 24

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 $\rho_n g_k \longrightarrow \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$ which leads to $\widehat{\rho} : g_k \longrightarrow \mathrm{GL}(\widehat{\mathbb{Z}})$.

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 an 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 $\mathrm{Pic}^0 E$, 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 $C(k) \longrightarrow \mathrm{Pic}^1 C$ given by sending p is its equivalence class; this is a bijection by Riemann-Roch (straightforward exercise).

We can then compose this with a map $\mathrm{Pic}^1 \longrightarrow \mathrm{Pic}^0 C$ given by $D \mapsto D - [O]$, which decreases the degree by 1. This gives a map $\Phi : C(k) \longrightarrow \mathrm{Pic}^0 C$, 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 $E^0 = E \setminus \{0\}$ 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 $\mathrm{Pic}k[E^0]$, and one can show that

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

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 $\mathrm{Pic}k[E^0]$, 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 $G \cong \mathrm{Pic}R$.
- 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 $T(1) \coloneqq (\mathbb{Q}/\mathbb{Z})^2 = \bigoplus_\ell (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^2$.

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. $E(k)[\mathrm{tors}] \hookrightarrow T(1)$.

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

Theorem (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.

Proof (Sketch): Let E/k be an elliptic curve over a field.

Step 1: Note that $\mathrm{End}_k(E) \cong_{\mathbb{Z}=} \mathbb{Z}^{a(E)}$ 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 $0 \longrightarrow E(k) \longrightarrow E(k(E)) \longrightarrow \mathrm{End}_K(E) \longrightarrow 0$. 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 $E(k(E)(E/k(E)))$. Then $k^2(E) \coloneqq k(E)(E/k(E))$, 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.

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 $E(k) \cong \oplus_S \mathbb{Z}$. We now want to introduce a process that allows passing to quotients. And $R \coloneqq k[E^0]$ is the affine coordinate ring of ?, remove the point at infinity (?).

Step 3: Let R be a Dedekind domain. Note it has a fraction field with a certain ideal class group. Let $W \subset \mathrm{maxSpec}\ (R)$, then $R^W \coloneqq \bigcap_{\mathfrak{p} \in \mathrm{maxSpec}\ R \setminus W} R_{\mathfrak{p}}$. Then R^W is Dedekind (and every overring of a Dedekind domain is of this form) and $\mathrm{maxSpec}\ (R^W) = \mathrm{maxSpec}\ (R \setminus W)$.

Then $\mathrm{Pic}\ R^W = \mathrm{Pic}\ R / \left\langle [\mathfrak{p}] \;\middle|\; \mathfrak{p} \in W \right\rangle$. 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 $\mathrm{Pic}\ R = \bigoplus_S \mathbb{Z}$.

Note: Pic R is the class group.

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

> 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.

Easy exercise: $K[E^0]$ 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 $W \subset \text{maxSpec } k[E^0]$ such that $\left\langle [p] \;\middle|\; p \in W \right\rangle = H$.

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 $1 \in \mathbb{Z}$

Claborn's proof: 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 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 $\mathbb{Q}_p/\mathbb{Z}_p = \lim_{\to n} \mathbb{Z}/(p^n)$ iff E is ordinary.

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

Theorem (Mordell-Weil): Let k be a global field (extension of $\mathbb{Q}$ or function field over $\mathbb{F}_p$) and E/k and 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 $m \;\middle|\; n$. So T is generated by at most two elements.

Proof (3 steps)

Step 1: Weak Mordell-Weil theorem.

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

Step 2: Define a height function $h : E(k) \longrightarrow \mathbb{R}$ 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 $h : A \longrightarrow \mathbb{R}$. 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 char k not dividing n, $E(k)/nE(k)$ is finite.

Step 2: Construction of a height function $h : E(K) \longrightarrow \mathbb{R}$ 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 heigh function $h : A \longrightarrow \mathbb{R}$, then A is finitely generated.

Question: What does the weak Mordell-Weil group $E(K)/nE(K)$ tell use 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 $x \longrightarrow nx$ 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 structure.

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 $E(K_{v_i})[\text{tors}] \longrightarrow E(\mathbb{F}_{v_i})$
- 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 $h : A \longrightarrow \mathbb{R}$ 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 $P \in A$, $h(nP) \geq n^2 h(P) - C_3$

> 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 $h : (A, +) \longrightarrow \mathbb{R}$. If A/nA is finite, then A is finitely generated.

Proof: Let r be the size of A/nA. Choose coset representatives $Q_1, \cdots, Q_r$ 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 $\{Q_1, \cdots, Q_r\} \bigcup h^{-1}((-\infty, C])$, 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 $Q_1, \cdots, Q_r$. 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 $\{Q_i\} \bigcup h^{-1}((-\infty, C])$.

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

Then

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

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 $h : A \longrightarrow \mathbb{R}$ from a commutative group is *quadratic* if the associated function $h(x + y) - h(x) - h(y) \coloneqq B_h : A^2 \longrightarrow \mathbb{R}$ 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.

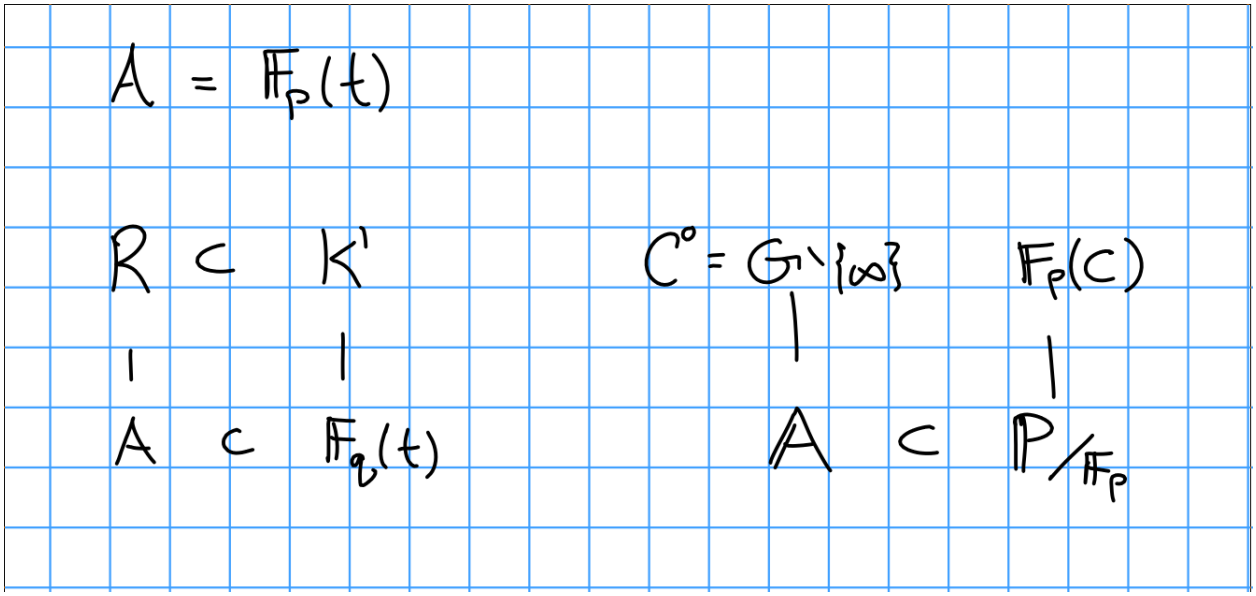


Figure 1: Image

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

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

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

5.2 Step 4

Theorem (Abstract Weak Mordell-Weil):

Let k be a field, E/k an elliptic curve, choose n such that char k doesn't divide n, and let $k' \coloneqq k(E[n])$ 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 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, 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 $L \coloneqq k([n]^{-1}E(k))$ be the compositum $k[\{P\}]$ over the $P \in E/\overline{k}$ such that $[n]P \in E(k)$ is k-rational. It's straightforward to show that L is separable and Galois (it is an etale 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, char (K) not dividing n, E/k an elliptic curve $K \coloneqq K(E[n])$.

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

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

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

Exercise: Take $k = \overline{k}$, C/k a "nice" affine curve, $R = k[C]$, $K = k(C)$, 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 $\iota : E(K)/nE(K) \longrightarrow E(L)/nE(L)$. This is not injective in general, and in fact $\ker(\iota) = (E(K) \bigcap nE(L))/nE(K)$.

Proposition:

a. There exists a map $\ker \iota \longrightarrow \text{Maps}(g_{L/K}, E[n])$, 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 $p \in E(K) \bigcap nE(K)$. 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 $p, p' \in E(K) \bigcap nE(L)$, 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 $\ker \iota = \dfrac{E(K) \bigcap nE(L)}{nE(K)}$.

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 $L \coloneqq K([n]^{-1}E(K)) = K(Q_p/P \in E(K))$. So κ induces group homomorphisms

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

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 $[n] : A \longrightarrow A$ is etale and $A[n]$ is finite. The proof goes through without modification if 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 nth roots of unity, then regular Kummer theory gives a map $K^\times/K^{\times n} \cong \hom(g_K, \mu_n)$ where μ_n are nth 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 $\chi(\,\cdot\,) = \hom(\,\cdot\,, \mathbb{Z}/n\mathbb{Z})$, 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 char k not dividing n, and A/K a commutative algebraic group (includes abelian varieties, additive/multiplicative groups, etc). Assume that K contains all nth roots of unity (we showed that this can be assumed).

Let $L \coloneqq K([n]^{-1}A(K)) = K(\left\{Q \in A(K^{\text{sep}}) \;\middle|\; [n]Q \in A(K)\right\})$. 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 Pic (R) and $R^\times$, then L/K is finite.

7.0.1 Step 3

Let $\mathfrak{p} \in \text{maxSpec } (R)$ 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

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

is unramified over K.

Take integral closures:

Take the inertia group

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

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 $E(L_p) \longrightarrow E(\widehat{L}_p) \longrightarrow \tilde{E}(S/p)$, 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 char (S/p)-primary torsion. Since 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?

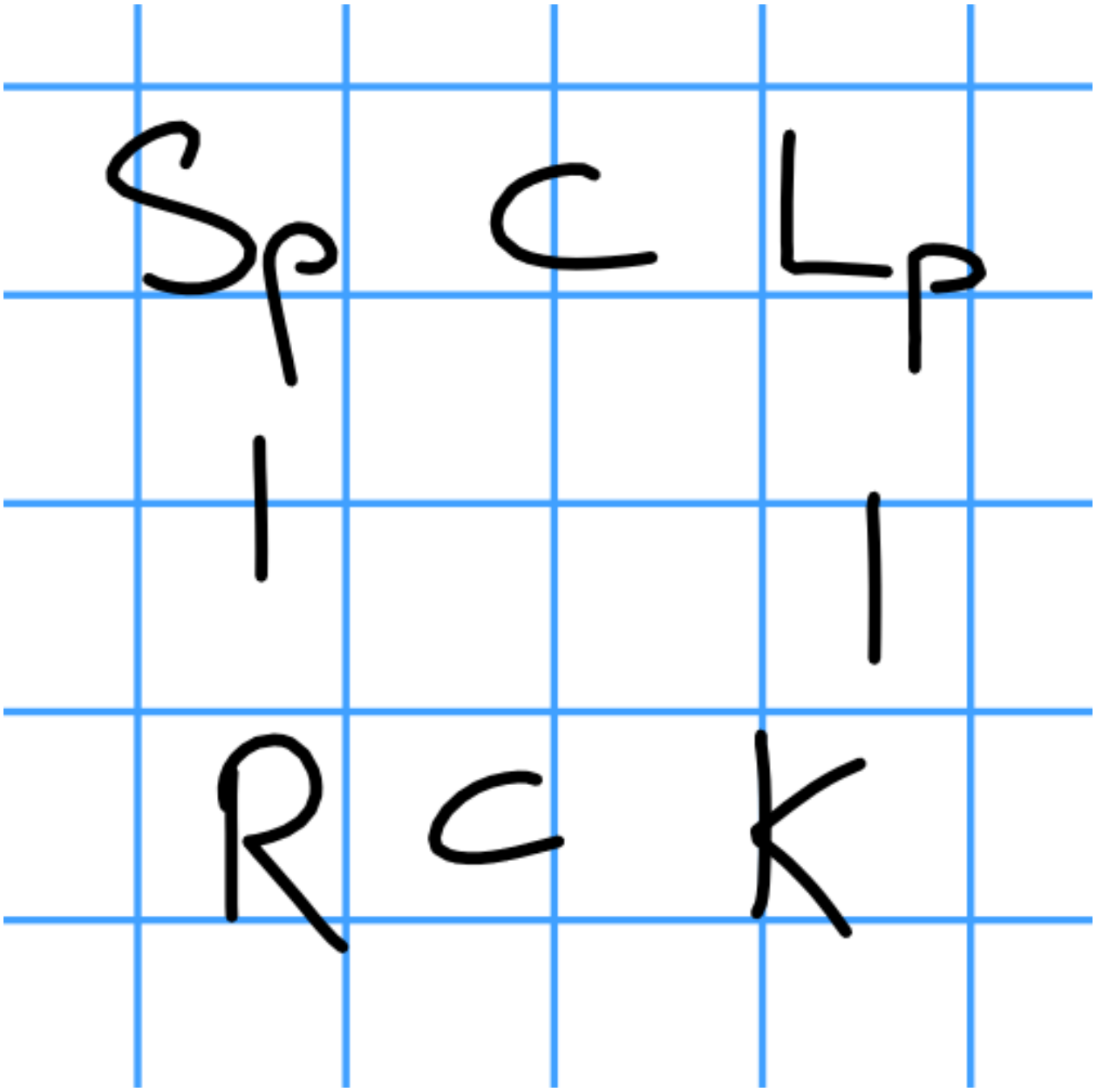


Figure 2: Image

7.0.2 Step 4: Number Theory

Let $S \subset \text{maxSpec } (R)$ 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 (Hermike - Minkowski): Let $d \in \mathbb{Z}^+$, K a number field, $s \subset \text{maxSpec } \mathbb{Z}_l$ 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 $R_s \coloneqq \bigcap_{\mathfrak{p} \in \text{maxSpec } (R \setminus S)} R_{\mathfrak{p}}$. Then R_s is a Dedekind domain, maxSpec R_s = maxSpec $(R \setminus S)$. Also Pic (R_s) is a quotient Pic $(R)/\left\langle [\mathfrak{p}] \ \middle| \ \mathfrak{p} \in S \right\rangle$.

Assume Pic R is finitely generated, then so is 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 $\mathfrak{p} \in \text{maxSpec } ?$ and define $T \coloneqq \bigcap_{q \neq \mathfrak{p}} R_q$. 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 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 nth 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 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 nth roots of unity $\mu_n \in K$.
- R a PID with fraction field K,
- $E(K)/nE(K)$ is finite iff $L \coloneqq K([n]^{-1}E(K))$ 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 $p \Big| n$ 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 $v : K \twoheadrightarrow \mathbb{Z} \bigcup \{\infty\}$ such that $v(n) = 0$. When are Kummer extensions unramified? Every Kummer extension L is a compositum $L \coloneqq K(a^{1/n})$. 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 $v(a^{1/n}) = \dfrac{1}{n}v(a)$, 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

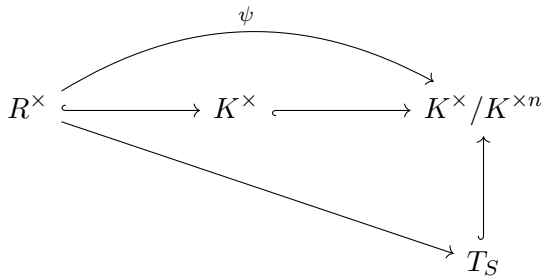
$$S = \left\{ \mathfrak{p} \in \text{Spec}R \;\middle|\; \mathfrak{p} \;\middle|\; n \text{ or } E \text{ has bad reduction at } \mathfrak{p} \right\},$$

and

$$T_S = \left\{ a \in K^\times / K^{\times n} \;\middle|\; \forall \mathfrak{p} \in \mathrm{Spec}(R \setminus S),\ n \;\middle|\; \mathrm{Ord}_p(a) \right\}.$$

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.



Take $\overline{a} \in T_s$ and lift it to $a \in K^\times$, and consider (a) as a fractional R_S ideal; it is an nth 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 $\overline{a} = \psi(a) = \psi(u)\psi(b^n) = \psi(u)$, 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 $(\mathrm{Pic}\ R)[n]$ is finite and $R^\times / R^{\times n}$ is finite.

Application: Let $k = \overline{k}$ 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 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) $\Sigma_K^{\mathrm{Arch}} \subset \Sigma_K$.

(PF2) For all $x \in K^\times$, the set $\left\{ v \in \Sigma_K \;\middle|\; |x|_v \neq 1 \right\}$ 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_vs 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 $g = g_K = \mathrm{Aut}(K\mathrm{sep}/K)$, 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 nth 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. $\left\{ p \in \mathbb{P}^n(K) \;\middle|\; H(P) \leq R \right\}$ is finite for ever 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 $f : \mathbb{P}^n \longrightarrow \mathbb{P}^m$.
2. For E/K with $y^2 = P_S(x)$, then $H : E(K) \longrightarrow \mathbb{R}$ given by $p \mapsto H([X(p) : 1])$.

View $X : E \longrightarrow \mathbb{P}^1$ 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 $(x_0, \cdots, x_n) \in \mathbb{P}^n(\mathbb{Q})$, where $\mathbb{Q}$ is the fraction field of $\mathbb{Z}$, a UFD, so this is a UFD. Appropriately clearing denominators, we can get $\gcd(x_0, \cdots, x_n)$. So $H(x_0, \cdots, x_n) = \max\limits_{0 \le i \le n} |x_i|$, 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 $v : K \longrightarrow \mathbb{R} \bigcup \infty$ 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 $x \in k^\times$, $\prod\limits_{v \in \Sigma_K} |x|_v = 1$.

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

- $|x|_p = p^{-\text{Ord}_p(x)}$
- $|x|_\infty = |x|$ the standard real absolute value
- $|x|_\infty = \left(\prod\limits_p |x|_p \right)^{-1}$ 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 $\Sigma_K = \{v_p,\ p \text{ monic irreducible polyno}$
Question: what is C_{v_p}.

For $c > 1$, we can write $|\cdot|_p \coloneqq c^{-v_p}$. Write $x = \varepsilon p_1^{a_1} \cdots p_r^{a_r}$ with the p_i monic irreducibles and $\varepsilon \in k^\times$. Then $\prod\limits_p |x|_p = \prod\limits_p c^{-v_p(x)} = c^{-\sum^r a_i}$. 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

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

In general, $\deg(\prod\limits_{i=1}^r p_1^{a_1} \cdots p_r^{a_r}) = \sum\limits_{i=1}^r a_i \deg(p_i)$.

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

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 $v \in L/K$ 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 $K \xrightarrow{\text{finite, separable}} k(f_1, \cdots, f_d) \longrightarrow k$.

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 $L_v \coloneqq L \otimes_k K_v$, 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, $L_v \cong \prod_{i=1}^{r} K_v[t]/(f_i) \cong \prod_{w \mid v} L_w$.

> 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 $|x|_w \coloneqq |N_{L_w}/K_v(x)|_v^{\frac{1}{d}}$ 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 $x \in C$, $\prod_{w \mid v} |x|_w = \left|N_{L/K}(x)\right|_v^{\frac{1}{d}}$.

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 $\prod_{w \in \Sigma_L} |x|_w = \prod_{v \in \Sigma_K} \prod_{w \mid v} |x|_w$. This equals $\prod_{v \in \Sigma_K} \left|N_{L/K}(x)\right|_v^{\frac{1}{d}} = 1$ by the product formula on K.

■

10.1 Height Functions

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

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

Thus for any $p \in \mathbb{P}^n(K)$, can write $p = [x_0, \cdots, x_n]$ 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 $\prod_{p \le \infty} \max(|a|_p, |b|_p)$, 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 $H([x_0 : \cdots : x_n]) = \max(|x_0|, \cdots, |x_n|)$.

We in fact have a finite bound

$$\#\left\{P \in \mathbb{P}^n(\mathbb{Q}) \;\middle|\; H(P) \le R \in \mathbb{Z}\right\} \le (2R+1)^{n+1}.$$

> 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 $H([a : b]) = \prod_{p \le \infty} \max(|a|_p, |b|_p) = (\max(|a|_\infty, |b|_\infty)) \prod_p \max(|a|_p, |b|_p) = \max(C^{\deg a}, C^{\deg b})$, 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. $\#\left\{P \in \mathbb{P}^n \;\middle|\; H(P) \leq R\right\} < \infty$ iff K is finite. This holds iff $\#\left\{P \in \mathbb{P}^n \;\middle|\; \log_C H(P) \leq R\right\}$ is finite. Note that if $K = \mathbb{F}_q$, then for $R \in \mathbb{Z}^+$, $\#\left\{P \in \mathbb{P}^n(\mathbb{F}_q) \;\middle|\; \log_C H(P) \leq R\right\} = (q^{r+1})^{n+1}$ 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 $d \in \mathbb{Z}^+$, $\#\left\{P \in \mathbb{P}^n(K\text{sep}) \;\middle|\; [K(P) : K] \leq d,\ H(P) \leq R\right\}$ 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 $H : \mathbb{P}^n(K) \longrightarrow [1, \infty)$ where $[x_0, \cdots, x_n] \mapsto \prod_{v \in \Sigma_K} \max(|x_0|_v, \cdots)$.

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 heigh functions to the separable closure, $H : \mathbb{P}^n(K\text{sep}) \longrightarrow \mathbb{R}$.

Lemma: If $p \in \mathbb{P}^n(K\text{sep})$ and $\sigma \in g_K = \text{Aut}(K\text{sep}/K)$, then $\sigma(p) \coloneqq [\sigma(x_0), \cdots, \sigma(x_n)]$ 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 $f(T) = T^d + a_{d-1}T^{d-1} + \cdots a_1 T + a_0 \in K[T]$, i.e. $f(T) = \prod_{i=1}^{\alpha}(T - \alpha_i)$ with $\alpha_i \in K\text{sep}$, then

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

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 $f(T) = (T - \alpha_k)(T^{d-1} + b_{d-1}T^{d-2} + \cdots + b_1 T + b_0)$ 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 $\alpha, \cdots, \alpha_d \in K\text{sep}$. Then replace K with $K(\alpha_1, \cdots, \alpha_d) \coloneqq L$. This is an extension of K of degree at most $d!$.

Note that if we define $\varepsilon = \max \varepsilon_v$, and $\left|\Sigma_K^{Arch}\right| = A$, then $\prod_{v \in \Sigma_K} \varepsilon_v^{d-1} \leq (\varepsilon^A)^{d-1} = \varepsilon^{A(d-1)}$. We also have $\left|\Sigma_L^{Arch}\right| \leq d!A$ 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 $\left\{P \in \mathbb{P}^n(K\text{sep}) \;\middle|\; [K(P) : K] \leq d,\ H(P) \leq R\right\}$ 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 $P = [x_0, \cdots, x_n]$ where some $x_i = 1$ be rescaling. Then $K(P) = K(x_0, \cdots, x_n)$ is a finite separable extension.

Proof: Let $P \in \mathbb{P}^n(K\text{sep})$ with $\deg P \leq d$, where $P = [x_0, \cdots, x_n]$ 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 $X(K,C,d) = \left\{x \in K\text{sep} \;\middle|\; H(x) \leq C,\ [K(x):K] \leq d\right\}$, we'll show this is a finite set. Let $x \in X(K,C,d)$ and $d' \coloneqq [K(x):K] \leq d$, and $f(T) \coloneqq \text{minpoly}x = \prod_{i=1}^{d'}(T - x_i) = T^{d'} + \sum_{i=0}^{d'-1} a_i T^i$. Take $M \coloneqq \max_{1\leq i\leq d} M(K,i)$ from the previous lemma.

By the lemma, we have $H(a_0, \cdots, a_{d'-1}, 1) \leq M \prod i = 1^{d'} H(x_i)$. 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 $(a_0, \cdots, a_{d'-1}, 1)$, and thus only finitely many possibilities for x.

■

Key Theorem: Let K be a PFF, and $f : \mathbb{P}^n \longrightarrow \mathbb{P}^m$ 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 $\phi : V \longrightarrow \mathbb{P}^n$, then define

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

Key property: Take hyperplanes $\psi : V \longrightarrow \mathbb{P}^m \supset H'$ and $\phi : V \longrightarrow \mathbb{P}^n \supset H$, 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 $h_{V,\cdot} : \text{Div}V \longrightarrow \mathbb{R}^{V(K\text{sep})}$ from divisors on V to ? which is unique modulo bounded functions such that

a. For $H \subset \mathbb{P}^n$ a hyperplane, the divisor $h_{\mathbb{P}^n_1 H} = h + O(1)$ (for the previously defined h).

b. Pullbacks: For $\phi : V \longrightarrow W$ 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 $D \subset \mathrm{Div}V$ be effective and B the base locus (common intersection of linearly equivalent effective divisors), then$h_{V,D}(p) \geq O(1)$ for all $P \in (V \setminus B)(K\mathrm{sep})$.

f. Let $D, E \in \mathrm{Div}V$ with D ample and E algebraically equivalent to 0. Then $\lim_{P \in V(K\mathrm{sep}), h_{V,D}(p) \longrightarrow \infty} h_{V,E}(p)/h_{V,}$ 0.

Ample: Chern class of line bundle is zero.

g. Finiteness: $D \in \mathrm{Div}V$ is ample. For all map into L/K and $r \in \mathbb{R}$, the set $\left\{ p \in V(L) \;\middle|\; h_{V,0}(p) \leq R \right\}$ 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 $D \in \mathrm{Div}A$ 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. $[-1]D \sim D$, $[n]^*D \sim n^2 D$ 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.
- $\psi_\ell : A \longrightarrow A^\vee$ where $x \mapsto \tau_x^* D - D$ (where τ_x is translation by x) has finite kernel.
- $A \longrightarrow \mathbb{P}(L(2D))$ is finite.

3. **(A.7.33)** Define 4 maps, $\sigma, \delta, \pi_1, \pi_2 : A \times A \longrightarrow A$,

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

Then

a. For $D \in \mathrm{Div}A$, $[D]$ 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 $[D] \in \mathrm{Pic}\,^0 A$.

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

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

a. $p \in A(K\mathrm{sep})$ 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 $h_{A,D}([n]p) = n^2 h_{A,D}(p) + O(1)$. If D is antisymmetric, then $h_{A,D}([n]p) = n h_{A,D}(p) + O(1)$.

This follows from properties of the Weil height machine.

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

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 $\phi : V \longrightarrow W$ and $D \in \mathrm{Div}W$, 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 $D \in \mathrm{Div}A$, by definition A carries an ample divisor D_0; then $D \coloneqq D_0 + [-1]^* D_0$ 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.