

Full Notes

D. Zack Garza

January 27, 2020

Contents

1	Wednesday January 8	1
2	Mordell-Weil Groups	2
3	Monday January 13th	3
4	Wednesday January 15th	5
5	Friday January 17th	7
5.1	Continuing Step 3	7
5.2	Step 4	8
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	12
7.0.2	Step 4: Number Theory	14
8	Monday January 27th	15
8.1	Weak Mordell-Weil: Finishing the Proof	15
8.2	Height Functions	17

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

$$\text{Pic}^0 E \rightarrow \text{Pic}[E^0]$$

$$\sum_p n_p \deg(p)[p] \mapsto \sum_{p \neq 0} n_p [p] = \prod_p p^{n_p}$$

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 $\text{Pic}[E^0]$, 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 $G \cong \text{Pic} R$.
- 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: Leatham-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

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 $\text{End}_k(E) \cong_{\mathbb{Z}} \mathbb{Z}^{a(E)}$ 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 $0 \rightarrow E(k) \rightarrow E(k(E)) \rightarrow \text{End}_K(E) \rightarrow 0$. 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 $k^2(E) := k(E)(E/k(E))$, 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 $E(k) \cong \bigoplus_S \mathbb{Z}$. 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 (∞) .

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

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

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 $W \subset \max\text{Spec } k[E^0]$ 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 $1 \in \mathbb{Z}$

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 $\text{char } k = p$, 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 $\mathbb{Q}_p/\mathbb{Z}_p = \varinjlim \mathbb{Z}/(p^n)$ 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 $m \mid n$. 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 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 $E(K_{v_i})[\text{tors}] \rightarrow E(\mathbb{F}_{v_i})$
 - 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

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

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.

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 .

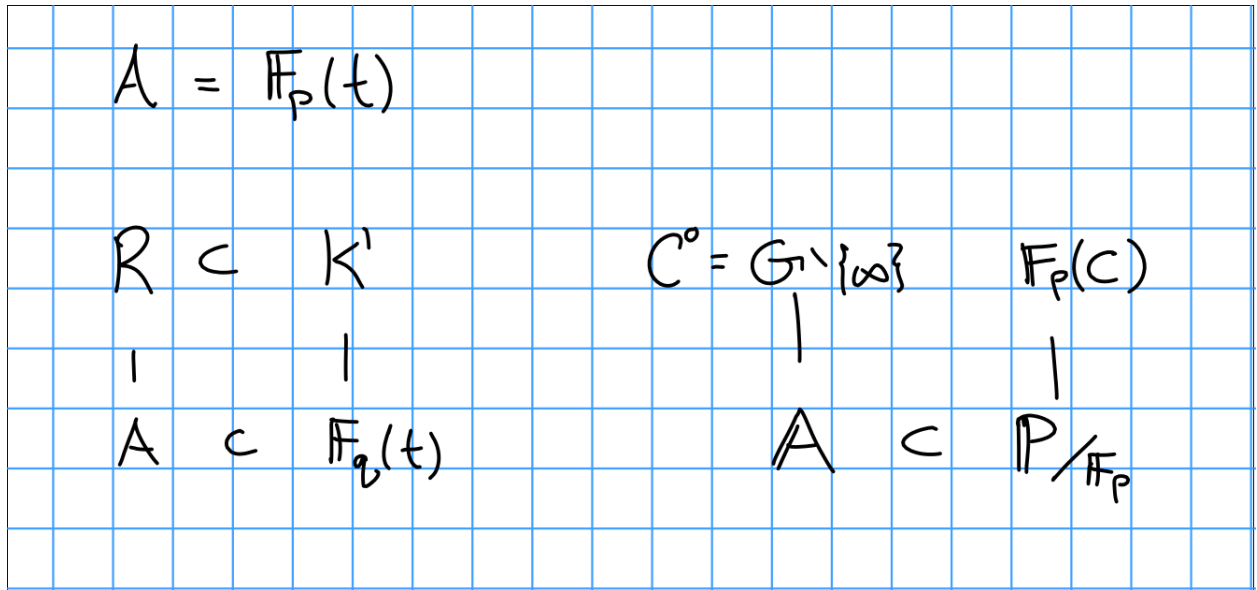


Figure 1: Image

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 $p \in E(K) \cap nE(L)$. 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

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

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

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

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

Define a Kummer pairing

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

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

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

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

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

is unramified over K .

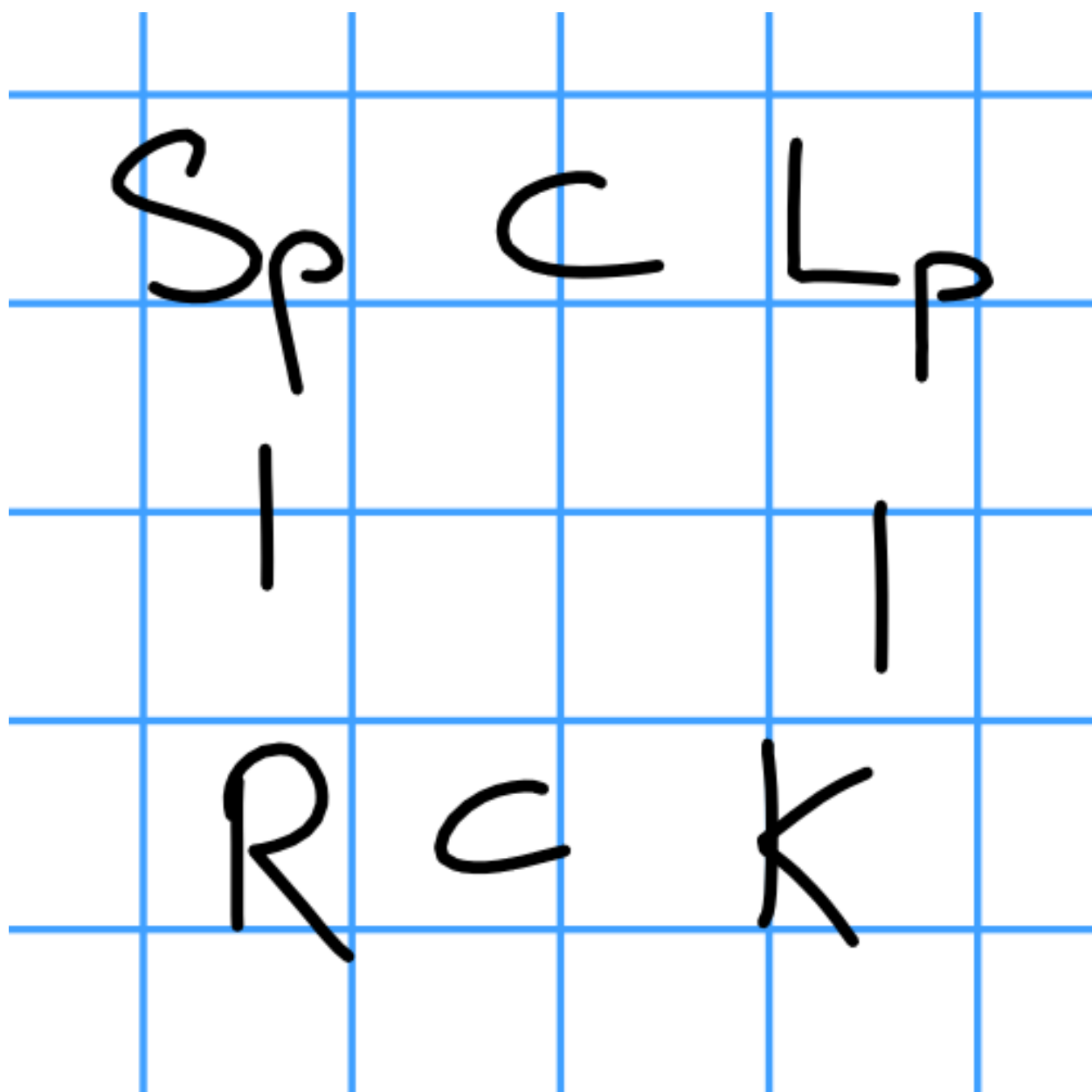


Figure 2: Image

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

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

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

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 (Hermike - 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:

\Rightarrow : 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.

\Leftarrow :

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 $\psi : R^\times \rightarrow T_S$. 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.

$$\begin{array}{ccccc}
 & & \psi & & \\
 & & \curvearrowright & & \\
 R^\times & \hookrightarrow & K^\times & \hookrightarrow & K^\times / K^{\times n} \\
 & \searrow & & & \updownarrow \\
 & & & & T_S
 \end{array}$$

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 $|\cdot| : K \rightarrow [-, \infty) \subset \mathbb{R}$, 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 $v : K \rightarrow \mathbb{R} \cup \infty$ 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.