Diophantine Approximation.

Conjecture (Mordell): Let K be a # field, and C a curve over K of genus ≥ 2.
Then $\#\, C(K) < \infty$ (proved).

Example: $\{ [x:y:z] \in \mathbb{P}^2 \mid x^p + y^p = z^p \}$, $p \geq 5$.

Goal of the course: prove this conjecture.
We won't follow Faltings's (83) proof, as it's too difficult.
We will instead follow the proof due to Vojta / Faltings / Bombieri.

Step 1: Embed $C \hookrightarrow J$, its Jacobian variety, assuming $C(K) \neq \emptyset$.

Step 2: For any smooth projective variety X/K and any divisor class $[D]$ on X, there is a height function $h : X(\bar{K}) \longrightarrow \mathbb{R}$, that has many nice properties ("height machine").

In particular, if $X = J$ and $[D] = [\Theta]$, then we obtain the "Canonical Neron-Tate Height" $\hat{h}_{J,\Theta} : J(\bar{K}) \longrightarrow \mathbb{R}$ with the properties:

a) $\hat{h}$ extends to a positive definite quadratic form on
$$J(\bar{K}) \otimes_{\mathbb{Z}} \mathbb{R}$$

b) $\{ x \in J(K) \mid \hat{h}(x) < C \}$ is finite $\forall C > 0$.

We will write $\|x\| = \sqrt{\hat{h}(x)}$, and $\langle x, y \rangle$ for the euclidean metric associated to $\hat{h}$.

Step 3: Prove that $\dfrac{J(K)}{2J(K)}$ is finite

Together w/ Step 2, get the Mordell-Weil theorem: $J(K)$ is a fgen ab. group.

Step 4: Using techniques from Diophantine Approximation (on $C \times C$) we prove Vojta's inequality: $\exists\, K_1, K_2 > 0$ (K_1 depends on C, K_2 only on $g(C)$) s.t. if $x, y \in C(\bar{K})$ w/ $\|x\| > K_1$, $\|y\| > K_2 \cdot \|x\|$, then $\langle x, y \rangle \leq \frac{3}{4} \|x\| \|y\|$.

To prove Vojta's inequality is a hard step.

Step 5: Suppose that $\#C(K) = \infty$.

By Step 2 (b), for each $N \in \mathbb{N}$ we can find $x_1, \dots, x_N \in C(K)$ such that $\|x_1\| > \kappa_1$, $\|x_{i+1}\| > \kappa_2 \|x_i\|$.

By Vojta's inequality, in $J(K) \otimes \mathbb{R}$, the angle $\sphericalangle(x_i, x_j) \geq \frac{\pi}{6}$ $\forall i \neq j$

For $N >> 0$, this is a contradiction.

Therefore $\#C(K) < \infty$.

To Do:

A) Abelian Varieties, Jacobians, Theta divisor.

B) Heights and height machine, heights on Abelian varieties. Mordell-Weil thm.

C) Diophantine approximation, Roth's theorem. Siegel's subspace thm.

D) Diophantine approximation on $C \times C$. Vojta's inequality.

Abelian Varieties

Let K be a field.

Def: A variety (scheme) G over K is called a group variety (group scheme) if

1) The functor $K\text{-alg} \longrightarrow \underline{\text{Sets}}$, $R \longmapsto G(R)$ takes values in groups.

$\Leftrightarrow$

2) There are algebraic morphisms $G \times_K G \xrightarrow{\mu} G$ s.t. some diagrams commute

$G \xrightarrow{i} G$

$\operatorname{Spec}(K) \xrightarrow{e} G$

(e.g. $\begin{array}{ccc} G \times G \times G & \xrightarrow{(\mu, id)} & G \times G \\ \downarrow{\scriptstyle (id, \mu)} & & \downarrow{\scriptstyle \mu} \\ G \times G & \xrightarrow[\mu]{} & G \end{array}$)

Def: A group variety A/k is called **abelian** if A is complete ($\Rightarrow$ projective) (↑ proper)

Fact: The group operation on an abelian variety is commutative.

Example: If $k = \mathbb{C}$, then (as a complex manifold) $A = \mathbb{C}^g/\Lambda$ for $\Lambda \subseteq \mathbb{C}^g$ a complete lattice. (i.e. $\Lambda \simeq \mathbb{Z}^{2g}$ and $\Lambda \otimes \mathbb{R} \simeq \mathbb{C}^g$).

Warning: if $g > 1$, then $\mathbb{C}^g/\Lambda$ is **not necessarily** an algebraic variety!

Example (Jacobian): Let C be a complex algebraic curve (i.e. a compact Riemann surface).

Then $J_C := \dfrac{H^0(C, \Omega^1_{hol})^\vee}{H_1(C, \mathbb{Z})}$ ($\simeq H^1(C, \mathcal{O}_{hol})$) is an abelian variety, called the Jacobian of C.

Ref: Milne, "Abelian Varieties" in Arithmetic Geometry (Cornell & Silverman ed).
Mumford, "Abelian Varieties".

Over $\mathbb{C}$: it's a connected, compact, cpx Lie group A.

So:
- it's commutative
- V = tgt space of A at the identity $\exp: V \to A$ is surjective with kernel Λ, discrete.

$\Rightarrow A \simeq V/\Lambda$.

But: not all complex tori are abelian varieties.

Need an embedding into Projective space.

For this, one needs a positive definite Hermitian form on V, taking integral values on Λ. (Riemann form).

The conditions on the matrix for this form are called the Riemann relations.

Let the N-torsion be the kernel of multiplication by N.

For $\mathbb{C}^g/\Lambda$, $\Lambda \simeq \mathbb{Z}^{2g}$, so the N-torsion is $\frac{\frac{1}{N}\mathbb{Z}^{2g}}{\mathbb{Z}^{2g}} \simeq \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^{2g}$.

Over $K \neq \mathbb{C}$, it's not a "torus" (check for a good definition of torus).

A/K is complete if $A \to \mathrm{Spec}(K)$ is proper.

It's a group variety: $\exists\, m : A \times A \to A$, $i : A \to A$, $e : \mathrm{Spec}\, K \to A$ s.t. ...

Properties

- It's commutative
- If $K = \bar{K}$ (or at least $K = K_s$ (sep. closure)), then N-torsion on A for $\mathrm{char}\, K \nmid N$ is $\simeq \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^{2g}$ where $\dim A = g$.

Let $\mathrm{Pic}(A) :=$ set of algebraic (generalization of lin. equiv.) equivalence classes of invertible sheaves on A.

$\mathrm{Pic}^0(A) :=$ sheaves in $\mathrm{Pic}(A)$ alg. equiv to the trivial bundle.

They both are functors on AbVar.

Fact: $\mathrm{Pic}^0(-)$ is representable: $\exists$ an abelian variety whose points over $\bar{K}$ are in bijection w/ $\mathrm{Pic}^0(A)$.

Def: The dual abelian variety of A is $A^\vee$ not defined, so $\mathrm{Pic}^0(A) =: A^\vee$.

We have a canonical invertible sheaf $\mathcal{P}$ on $A \times A^\vee$ s.t.

if $a \in A^\vee$, then the pullback of $\mathcal{P}$ to $A \times \{a\} \simeq A$ is a representative of a on $A^\vee$. $\mathcal{P}$ is called the Poincare sheaf.

Def: An isogeny is a surjective morphism of abelian varieties w/ finite kernel.

Example: multiplication by N is an isogeny.

Def The degree of an isogeny is the order of its kernel.

Def: An isogeny $\lambda : A \to A^\vee$ is called a polarization.

If $\deg \lambda = 1$, λ is called a principal polarization.

(Note: ppal polarization is an isomorphism $A \xrightarrow{\sim} A^\vee$).

Polarization "rigidify" ab. vars (e.g. there are finitely many automorphisms fixing ~~the~~ given polarization).

Theorem: Any abelian variety is isogenous to a principally polarized ab. var.

(i.e. $(A, \lambda) \mapsto (A', \lambda')$ with $\deg \lambda' = 1$).

Another def of a polarization: λ is an embedding into projective space.

For jacobians, the polarization associated to the theta divisor is principal

So $J \cong J^\vee$

For a curve C, we have $C \hookrightarrow J(C)$ by $P \mapsto [P - D]$

where D is a fixed degree-~~1~~ divisor.

For an elliptic curve (E, ∞), the map $P \mapsto [P - \infty]$ is an iso:

Proof

- injectivity: if $[P - \infty] \overset{\text{in curves, linear eq.} = \text{alg. equiv}}{\sim} [Q - \infty]$ then $[P - Q] \sim \operatorname{div}(f)$, $f \in K(E)$.
  But $f : E \to \mathbb{P}^1$ has degree 1, or $E \cong \mathbb{P}^1$, contradicting $\operatorname{genus}(E) = 1$.

- surjectivity: Riemann-Roch says that, for any D with $\deg D = 0$, $\ell(D + \infty) = 1$.
  Let $f \in \mathcal{L}(D + \infty)$ generate $\mathcal{L}(D + \infty)$. Then $\operatorname{div}(f) \geq -D - \infty$
  $\deg(\operatorname{div}(f)) = 0$. So $\operatorname{div}(f) = -D - \infty + P$ for some P.
  Hence $D \sim [P - \infty]$ //.

Divisors

Let X be a scheme $/k$.

Def: A <u>divisor</u> (Weil divisor) on X is a formal sum $\sum a_i [Z_i]$, where $Z_i \subset X$ are irreducible subvarieties of pure codimension 1, $a_i \in \mathbb{Z}$.

The group of Weil divisors is $\mathrm{Div}(X)$.

Assume X is integral (reduced + irreducible), and smooth (at least regular in codim 1). And $\kappa(X)$ the field of rat'l functions on X.

(i.e. $\kappa(X) = \mathcal{O}_{X,\eta}$).

If $f \in \kappa(X)$, we can define a divisor (f) as

$$(f) = \sum_{Z \in X^{(1)}} v_Z(f)\,[Z] \qquad \left(X^{(1)} = \text{set of irreducible varieties of pure codim } 1\right)$$

and where v_Z is the valuation corresponding to the DVR $\mathcal{O}_{X,\eta_Z}$ (as X is reg. in codim 1).

Ex: X/k a smooth curve, then a divisor is a formal sum of closed points.

e.g. if $X = \mathbb{P}^1$, and x is a coordinate function, $(x) = (0) - (\infty)$.

Def: We say that a Weil divisor of the form (f) is <u>rational</u>, or "linearly equiv." to 0.

Def: $Cl(X) := \dfrac{\mathrm{Div}(X)}{\text{rational divisors}}$.

Example: $Cl(\mathbb{P}^1) \cong \mathbb{Z}$ (if $k = \bar{k}$, we have an easy proof by degree)

Def: A <u>Cartier divisor</u> on X is a global section of the quotient sheaf

$$\mathcal{K}^\times / \mathcal{O}^\times \qquad (\text{if } X \text{ is integral, } \mathcal{K}^\times = \kappa(X)^\times).$$

(equivalently, a Cartier divisor is given by a cover $X = \bigcup U_i$, for each U_i a function $f_i \in \kappa(X)^\times(U_i)$ ← rat'l function s.t. $\dfrac{f_i}{f_j} \in \mathcal{O}^\times(U_i \cap U_j)$ ← invertible morphisms.

If X is regular in codimension 1, then we get a homomorphism:

$$\begin{aligned} CaDiv(X) &\longrightarrow Div(X) \\ ((U_i)_i, f_i) &\longmapsto \sum_{Z \in X^{(1)}} v_Z(f_i)\,[Z] \end{aligned}$$

(well-defined!)

↑ this is well-defined!

Def $CaCl(X) := \dfrac{CaDiv(X)}{\text{im } K^\times(X)}$.

We get a diagram:

$$\begin{array}{ccccc} K^\times(X) & \longrightarrow & CaDiv(X) & \longrightarrow & CaCl(X) \\ \downarrow & & \downarrow & & \downarrow \\ (\text{rational divisors}) & \longrightarrow & Div(X) & \longrightarrow & Cl(X) \end{array}$$

Thm: If X is "nice" (locally factorial...) (e.g. X smooth) then

$$CaCl(X) \xrightarrow{\sim} Cl(X).$$

Line Bundles

Let X be any scheme.

Def A <u>line bundle</u> $\mathcal{L}$ on X is a locally-free coherent sheaf of rank 1 on X.

Line bundles can be described by "transition functions", so they are connected with Cartier divisors:

Fact (1) If $\mathcal{L}, \mathcal{L}'$ are line bundles, so is $\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{L}'$.

(2) If $\mathcal{L}^{-1} := \mathcal{H}om_{\mathcal{O}_X}(\mathcal{L}, \mathcal{O}_X)$, then $\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{L}^{-1} \xrightarrow{\sim} \mathcal{O}_X$

Def: $Pic(X) :=$ group of isomorphism classes of line bundles on X.

Example: If $X = \operatorname{Spec} R$, R a Dedekind domain, then

$$\{\text{line bundles on } X\}/\cong \;\longleftrightarrow\; \{\text{fractional ideals of } R\}/\{\text{principal fractional ideals}\}.$$

(in the example, we've seen that $\mathrm{Pic}(X) \cong \mathcal{Cl}(R)$).

Thm: $\mathrm{Pic}(X) \cong H^1(X, \mathcal{O}_X^*)$

Pf Describe line bundles using transition functions. //

Corollary: $\mathrm{Pic}(X) \cong \mathrm{CaCl}(X)$.

Pf Exact sequence of sheaves:

$$0 \to \mathcal{O}_X^* \to \mathcal{K}_X^* \to \mathcal{K}_X^*/\mathcal{O}_X^* \to 0.$$

Taking cohomology, get a long exact seq.

$$0 \to H^0(X, \mathcal{K}_X^*/\mathcal{O}_X^*) \to \underbrace{H^0(X, \mathcal{K}_X^*)}_{\text{rational divisors}} \to \underbrace{H^0(X, \mathcal{O}_X^*)}_{\mathrm{CaDiv}(X)} \to$$

$$\to \underbrace{H^1(X, \mathcal{O}_X^*)}_{\cong \mathrm{Pic}(X)} \to H^1(X, \mathcal{K}_X^*)$$

$\searrow 0$ because $\mathcal{K}_X^*$ is flasque. //

Curves: A curve X/k will mean a projective, smooth, connected scheme of dimension 1 over k.

Def: Let $D = \sum_{x \in X^{(1)}} n_x [x]$

Then the degree of D is $\sum n_x \cdot [k(x):k] \in \mathbb{Z}$

(note that $[k(x):k]$ is finite by Hilbert's Nullstellensatz).

We get a gp. hom. $\deg: \mathrm{Div}(X) \to \mathbb{Z}$, and $\deg((f)) = 0$ for $f \in k(X)^*$.

Therefore, get a homomorphism $\mathcal{Cl}(X) \to \mathbb{Z}$.

The kernel of it is $\mathcal{Cl}^0(X)$.

Using $\mathrm{Pic}(X) \cong \mathcal{Cl}(X)$, get a group $\mathrm{Pic}^0(X)$.

Assume: $X/\mathbb{C}$ a compact Riemann surface. We have the exponential sequence:

$$0 \to \mathbb{Z} \to \mathcal{O}_X \xrightarrow{\exp} \mathcal{O}_X^* \to 0 \qquad \text{(of sheaves on } X^{an}\text{)}$$

(sheaf of holomorphic functions)

which induces:

$$H^0(X,\mathcal{O}_X^*) \to H^1(X^{an},\mathbb{Z}) \hookrightarrow H^1(X,\mathcal{O}_X) \to H^1(X,\mathcal{O}_X^*) \xrightarrow{\delta} H^2(X^{an},\mathbb{Z})$$

$$H^1(X,\mathcal{O}_X^*) \xrightarrow{c_1} H^2(X^{an},\mathbb{Z})$$

- $H^0(X,\mathcal{O}_X^*) \to H^1(X^{an},\mathbb{Z})$: because (for H^0) exp is surjective
- $H^1(X^{an},\mathbb{Z}) \hookrightarrow H^1(X,\mathcal{O}_X)$: because (for H^0) exp is surjective
- $H^1(X,\mathcal{O}_X) \to H^1(X,\mathcal{O}_X^*)$: $\cong$ GAGA $\cong \mathrm{Pic}(X)$
- δ: first chern class, deg.
- $H^2(X^{an},\mathbb{Z}) \cong \mathbb{Z}$

$$\text{So } \mathrm{Pic}^0(X) \cong \frac{H^1(X^{an},\mathcal{O}_X^{hol})}{H^1(X^{an},\mathbb{Z})}.$$

Let $D \in \mathrm{Div}(X)$. We can define a line bundle $\mathcal{L}(D)$ as:

$$\mathcal{L}(D)(U) := \{ f \in \kappa(U) = \kappa(X) : (f|_U) \geq -D \} \quad \leftarrow \text{This is a line bundle.}$$

Fact: if $D \sim D'$ (i.e. $D - D' = (g)$ for some g), then $\mathcal{L}(D) \cong \mathcal{L}(D')$.

Def: Let $L(D) := H^0(X,\mathcal{L}(D))$.

Def: The projective space $\mathbb{P}(L(D))$ is called the complete linear system of D.

$$\mathbb{P}(L(D)) \overset{1:1}{\longleftrightarrow} \{ D' \sim D : D' \geq 0 \}.$$

(Let $f \in L(D)$. Then $D' := D + (f)$ is effective, $D' \sim D$).

Jacobians

Let C/κ be a curve. Then J (Jacobian) is a variety s.t.

$J(F)$ $(\kappa \leq F)$ is isomorphic to $\mathrm{Pic}^0(C \times_\kappa F) = Cl^0(C \times_\kappa F)$

Assume there exists $x \in C(\kappa)$, and let $n \geq 1$. Then we get the map

$$\mathrm{Sym}^n C \to J \quad \text{by} \quad x_1 + \cdots + x_n \mapsto (x_1) + \cdots + (x_n) - n(x)$$

Why is this map algebraic? Because it's a transformation of functors.
We go now more formal.

Jacobian of a Curve

Def Let C/k be a (smooth, proj.) curve. The Jacobian variety J of C is a variety representing the following functor:

$$T \longmapsto \mathrm{Pic}^0_C(T) = \{ [\mathcal{L}] \in \mathrm{Pic}(C \times T) \text{ s.t. } \deg \mathcal{L}_t = 0 \ \forall \text{ fibers} \}$$

$\Leftrightarrow \mathcal{L}_t \in \mathrm{Pic}^0_C(C \times \{t\})$

$\{ \mathcal{L} : \mathcal{L} \cong g^* \overline{\mathcal{L}}$ for some $\overline{\mathcal{L}} \in \mathrm{Pic}(T)\}$ ← line bundles that come from T

$= p_2^* (\mathrm{Pic}(T))$

In particular, if $T = \mathrm{Spec}\, F$, then $\mathrm{Pic}^0_C(F) = \mathrm{Pic}^0(C \times_k F)$.

Construction

Assume $C(k) \neq \emptyset$ and that J exists. Choose $x_0 \in C(k)$
Then we can evaluate the functor at J itself.

So $\mathrm{Pic}^0_C(J) = \mathrm{Mor}(J, J) \ni id_J$.

Hence $id_J \leftrightarrow [M] \in \mathrm{Pic}(C \times J)$ s.t. (a) $M|_{\{x_0\} \times J}$ is trivial

(b) $M|_{C \times \{0\}} \Big]^{=0} \in \mathrm{Pic}^0_C(C)$

(i.e. $M|_{C \times \{0\}}$ is trivial).

Let T be a pointed k-scheme w/base point $t_0 \in T(k)$

Thm: Suppose J exists. There is a 1-1 correspondence

$$\mathrm{Pic}^0_C(T) \xleftrightarrow{1:1} \{ [\mathcal{M}] \in \mathrm{Pic}(C \times T) \text{ s.t. } \mathcal{M}|_{\{x_0\} \times T}, \ \mathcal{M}|_{C \times \{t_0\}} \text{ are trivial} \}.$$

by sending $[(id_C \times f)^* \mathcal{M}]$ to $f : T \to J$.

Construction:

Step 1: $\mathrm{Sym}^r C$ is a smooth variety (take r copies of C, and mod out by the action of the group Sym_r on the components).

Then $T \longmapsto \mathrm{Div}_C^r(T)$ ~ relative effective Cartier divisor on $C \times T / T$.

Def: A relative effective Cartier divisor on $C \times T$ of constant degree r over T is a Cartier divisor $D = (U_i, f_i)$ on $C \times T$ s.t.:

a) $f_i \in \mathcal{O}(U_i)$ $\forall i$ (i.e. D is effective).

b) $|D| = \bigcup V(f_i)$ $\left(V(f_i) = \mathrm{Spec}\left(\mathcal{O}_{U_i}/(f_i)\right) \right)$ is flat over T.

c) $\forall t \in T$, $D_t := D \times_T \{t\}$ on $C \times \{t\}$ has degree r.

Write $\mathrm{Div}_C^r(T) = \{ D \in \mathrm{CaDiv}(C \times T) : D \text{ is relat. effective of degree } r \}$.

Fact: Div_C^r is a contravariant functor on k-schemes.

Now, let D_{can} be (the canonical) the relative effective Cartier divisor on $\mathrm{Sym}^r C \times C / \mathrm{Sym}^r C$, obtained as follows: $D_{can} = \left(\sum s_i(C^r) \right) / \sum_r$

where $s_i : C^r \to C \times C^r$

$(P_1, \dots, P_r) \mapsto (P_i, P_1, \dots, P_r)$

Note that the fiber $D_{can, P_1 + \cdots + P_r} = (P_1) + \cdots + (P_r)$.

Theorem: Let T be a scheme. Then there is a (natural) 1-1 correspondence between morphisms $\varphi : T \to \mathrm{Sym}^r C$ and ~~relative effective Cartier~~ $\mathrm{Div}_C^r(T)$, given by $\varphi \longmapsto (1 \times \varphi)^* (D_{can})$

(note $1 \times \varphi : C \times T \to C \times \mathrm{Sym}^r C$).

Pf (of Thm)

This obviously defines a transformation $\pi : \mathrm{Sym}^r C \to \mathrm{Div}^r_C$.

and π is injective (exercise). We need to prove surjectivity.

Assume D is split, i.e. $D = \sum n_i s_i(T)$, for some $s_i : T \to C \times T$

sections of pr_2.

In this case, define $\tilde{\varphi} : T \to C^r$ by $\tilde{\varphi} = (\overbrace{\bar{s}_1, \bar{s}_1, \dots}^{n_1}, \overbrace{\bar{s}_2, \bar{s}_2, \dots}^{n_2}, \dots \overbrace{\bar{s}_r, \bar{s}_r \dots}^{n_r})$

($\sum n_i = r$, and let $\bar{s}_i := pr_1 \circ s_i$ $(\bar{s}_i : T \to C)$.

Then let $\varphi : (T \xrightarrow{\tilde{\varphi}} C^r \to \mathrm{Sym}^r C)$

Exercise: $(1 \times \varphi)^*(D_{\mathrm{can}}) = D$.

Fact: There is a flat cover $T' \xrightarrow{q} T$ (flat surjective morphism) s.t. $(1 \times q)^*(D)$ is split.

So if we believe this, let $\varphi' : T' \to \mathrm{Sym}^r C$ correspond to $(1 \times q)^*(D)$, constructed as above.

$$\begin{array}{ccc} T' \times_T T' & \xrightarrow{pr_2} & T' \\ \downarrow{\scriptstyle pr_1} & \swarrow & \downarrow \\ T' & \longrightarrow & \mathrm{Sym}^r C \end{array}$$

why?

$$\left(1 \times (\varphi' \circ pr_1)\right)^* (D_{\mathrm{can}}) = \left(1 \times (q \circ pr_1)\right)^* (D)$$

(by the univ. property of the fiber product)

$$\left(1 \times (\varphi' \circ pr_2)\right)^* (D_{\mathrm{can}}) = \left(1 \times (q \circ pr_2)\right)^* (D)$$

But as π is injective, this gives $\varphi' \circ pr_1 = \varphi' \circ pr_2$. by flat descent.

By flat descent (look it up!), $\exists\, \varphi : T \to \mathrm{Sym}^r C$ s.t. $(1 \times \varphi)^*(D_{\mathrm{can}}) = D$.

Let $P_C^r(T) := \{ \mathcal{L} \in Pic(C \times T) : \deg \mathcal{L}_t = r \} / \sim$.

(where $\mathcal{L} \sim \mathcal{L}' \iff \exists M$ s.t. $\mathcal{L} \otimes pr_2^* M \cong \mathcal{L}'$ $(pr_2 : C \times T \to T)$.

We can identify P_C^0 with P_C^r via:

$P_C^0 \ni \mathcal{L} \longmapsto \mathcal{L} \otimes pr_1^* \mathcal{L}(r \cdot x_0)$. ← the chosen point $\in C$.

Fact. There is a natural transformation $f : Div_C^r \to P_C^r$

$D \mapsto \mathcal{L}(D)$

Note: $f^{-1}(\mathcal{L}) = \mathbb{P}(H^0(C, \mathcal{L}))$ ← complete linear system of $\mathcal{L}$

Lemma: Assume f has a section $g : P_C^r \to Div_C^r$. Then P_C^r is representable.

Pf: Let $\varphi = g \circ f$, $\varphi : Div_C^r \to Div_C^r \leftrightarrow \varphi : Sym^r C \to Sym^r C$ (Yoneda)

Set J' to be the pull-back:

$$\begin{array}{ccc} Sym^r C & \longleftarrow & J' \\ \downarrow (1,\varphi) & & \downarrow \\ Sym^r C \times Sym^r C & \xleftarrow{\Delta} & Sym^r C \end{array}$$

Exercise: $J' \cong P_C^r$.

Let now $r > 2g$, and let γ be an $(r-g)$-tuple in $C(\kappa)$.

Set $D_\gamma := \sum_{P \in \gamma} P$, $\mathcal{L}_\gamma := \mathcal{L}(D_\gamma)$.

Theorem: a) $Div_C^\gamma(T) = \{ D \in Div_C^r(T) : \ell(D_t - D_\gamma) = 1 \ \forall t \}$.

b) is represented by an open (nonempty) subvariety $C^\gamma \subseteq Sym^r C$.

Moreover, if $\kappa = \kappa^{sep}$, then $Sym^r C = \bigcup_\gamma C^\gamma$.

b) Let $P^\gamma(T) = \{ \mathcal{L} \in P_C^r(T) : \ell(\mathcal{L}_t \otimes \mathcal{L}_\gamma^{-1}) = 1 \}$.

Then $P^\gamma \subseteq P_C^r$ is a subfunctor, and $f : C^\gamma \to P^\gamma$ has a section.

Pf of Thm: Use Semicontinuity. (see it in Cornell-Silverman)

Now we need to show that the constructed scheme is complete.

Choose $P \in C(L)$.

Observe: $\Delta = \{P\} \times C - C \times \{P\} \in \mathrm{Div}(C \times C)$ defines a divisorial correspondence from (C, P) to itself.

This corresponds to $f^P : C \to \mathcal{J}$, which on points is $f^P(Q) = \mathcal{L}(Q - P)$.

For any $r \geq 1$, set $f^r : C^r \to \mathcal{L}$, $f^r = f + f + \cdots + f$ (r times)

So on points, $f^r(Q_1, \ldots, Q_r) = \mathcal{L}(\sum Q_i - rP)$.

As this map is symmetric, it factors through

$$f^{(r)} : \mathrm{Sym}^{(r)} C \to \mathcal{J}.$$

Write $W^{(r)} := f^{(r)}(\mathrm{Sym}^{(r)} C) = f^r(C^r)$.

Thm:

(a) If $r \leq g$, then $f^{(r)} : \mathrm{Sym}^r C \to W^r$ is birational.

(b) Suppose $D \in \mathrm{Sym}^r C(k)$; let $F := \mathrm{Sym}^r C \times_{\mathcal{J}} \{f^{(r)}(D)\}$

Then $0 \to T_D(F) \to T_D(\mathrm{Sym}^r C) \xrightarrow{df^{(r)}_D} T_{f^{(r)}(D)} \mathcal{J}$ is exact

(as vector spaces).

Pf ((a)):

It's not hard to see (using semicontinuity) that there's a nonempty open

$U \subseteq \mathrm{Sym}^r C$ such that $|D| =$ point $\forall\, D \in U(k^{sep})$ (if $r \leq g$).

So $f^{(r)}$, on U, is purely inseparable. This proves (a) if $\mathrm{char}\, k = 0$.

If $\mathrm{char}\, k = p$, then need to prove (b).

Corollary: $f^{(g)} : \mathrm{Sym}^g C \to J$ is birational and surjective.

Pf: want to see $W^g = J$.

As $\dim W^g = g$ (birational to $\mathrm{Sym}^g C$), it's enough to show that $\dim J = g$.

Thm: $T_0 J \cong H^1(C, \mathcal{O}_C)$ has dimension g. $\Rightarrow \checkmark$ (as $\dim J = \dim T_0 J$)

Pf: For any algebraic group G,

$$T_e G = \ker\left(G(k[\varepsilon]) \to G(k)\right) \quad \text{where } k[\varepsilon] = k[t]/(t^2)$$

So we need to compute $\ker\left(P_C^\circ(k[\varepsilon]) \to P_C^\circ(k)\right)$

Now $\mathbb{Z} \times P_C^\circ(k[\varepsilon]) \simeq H^1\left(C_{k[\varepsilon]}, \mathcal{O}_{C_{k[\varepsilon]}}^\times\right)$ ($C_{k[\varepsilon]}$ = pullback of C to $\mathrm{Spec}\, k[\varepsilon]$)

Note that $\mathcal{O}_{C_{k[\varepsilon]}}^\times = \mathcal{O}_C^\times \oplus \varepsilon \mathcal{O}_C$ (indeed, $R[\varepsilon]^\times = R^\times \oplus \varepsilon R$).

and therefore we are computing $\ker\left(H^1(C, \mathcal{O}_C^\times \oplus \varepsilon \mathcal{O}_C) \to H^1(C, \mathcal{O}_C^\times)\right)$

$\cong H^1(C, \varepsilon \mathcal{O}_C)$ //

We want to fix an embedding of J into projective space (we know that there's one, we need just to fix it!)

Let (H) be the divisor $[W^{g-1}]$

Theorem: (H) is an ample, irreducible divisor on J.

Pf: Irreducible is ok. We need to see that it's ample.

Step 1: For an abelian variety A, let $\mathrm{Pic}^0(A) = \{\mathcal{L} : t_a^*\mathcal{L} \cong \mathcal{L},\ a \in A(\bar{k})\}/\cong$

where $t_a : A_{\bar{k}} \to A_{\bar{k}}$
$b \mapsto a+b$

There is an abelian variety $A^\vee$ representing $\mathrm{Pic}^0 A$ (the dual abelian variety).

Suppose $\mathcal{L} \in \mathrm{Pic}\, A$. Then $\mathcal{L}$ defines a homomorphism

$$\varphi_{\mathcal{L}} : A \longrightarrow A^\vee$$
$$a \longmapsto t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$$

(homomorphism by the theorem of the square of abelian varieties.)

Moreover, $\mathcal{L}$ is ample $\iff \ker \varphi_{\mathcal{L}} = \{a \in A(\bar{k}) : t_a^*\mathcal{L} \cong \mathcal{L}\}$ is finite.

($\varphi_{\mathcal{L}}$ is an isogeny).

Note: If $\mathcal{L}$ is ample, $\varphi_{\mathcal{L}}$ is called a polarization.

(There are always polarizations, because A is projective!)

If $\varphi_{\mathcal{L}}$ is an isomorphism, then it is called a principal polarization.

Step 2: Want to show that $\varphi_{\mathcal{L}(\mathcal{H})}$ is an isomorphism.

On $A \times A^\vee$, there is a universal line bundle $\mathcal{P}$ (Poincaré bundle)

(i.e. it corresponds to $\mathrm{id}_{A^\vee}$ under the representing property of $A^\vee$).

It's easy to see that $(f^p \times 1)^* \mathcal{P}$ (on $C \times J^\vee$)

is a divisorial correspondence $(C, p) \to (J^\vee, 0)$, which

in turn corresponds to a morphism $f^\vee : (J^\vee, 0) \to (J, 0)$.

Step 3: One proves that $-f^\vee$ is inverse to $\varphi_{\mathcal{L}(\mathcal{H})}$ (long).

Hence $\mathcal{H}$ is ample.

Heights: Let K be a number field, $([K:\mathbb{Q}] < \infty)$.

We want a function $h : \mathbb{P}^n(K) \to \mathbb{R}_{\geq 0}$

such that $\#\{\underline{x} : h(\underline{x}) \leq C\} < \infty \quad \forall C$ constant.

Then, if we have a projective variety, by choosing an embedding $X \subseteq \mathbb{P}^n$, we will get a height on $X(K)$.

$h(\underline{x})$ depends on embedding $\longleftrightarrow$ very ample divisor on X

In fact, it will only depend additively on to the rat. equiv class of X, up to $O(1)$.

If $X = A$ an abelian variety, choose a very ample divisor D s.t.

h_D is a quadratic form on $A(K)$, (up to $O(1)$)

This can be used to prove:

- $A(K)$ is finitely-generated.
- $A(K) \otimes \mathbb{R}$ into euclidean vectorspace.

Then can study the lattice $A(K)/\text{torsion} \subseteq A(K) \otimes \mathbb{R}$

• Absolute values on fields

Let K be a field.

An absolute value is $|\cdot| : K \to \mathbb{R}_{\geq 0}$ such that:

i) $|x| = 0 \iff x = 0$

ii) $|x+y| \leq |x| + |y|$

iii) $|xy| = |x||y|$

If (ii) can be replaced by

ii)' $|x+y| \leq \max\{|x|, |y|\}$

then it is called non-Archimedean (otherwise it is called archimedean).

Recall: If K is a #field with ring of integers $\mathcal{O}_K$, then we have the following absolute values:

- For each maximal prime $\mathfrak{p} \subseteq \mathcal{O}_K$, have $|x|_{\mathfrak{p}} = N(\mathfrak{p})^{-v_{\mathfrak{p}}(x)}$

  (where $N(\mathfrak{p}) := \#\left(\mathcal{O}_K/\mathfrak{p}\right)$, and $(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)}$)

  Note: H-S calls $|\cdot|_{\mathfrak{p}} = \|\cdot\|_{\mathfrak{p}}$.

- One archimedean for each conjugate pair $\overline{\sigma} : K \hookrightarrow \mathbb{C}$

  $|x|_\sigma := \|\sigma(x)\|$.

Write $M_K = \underbrace{M_K^\infty}_{\text{archimedean}} \sqcup \underbrace{M_K^\circ}_{\text{finite (non-archimedean)}}$

Proposition: Let $x \in K^*$, then:

$$\prod_{v \in M_K} |x|_v = 1$$

Pf $|N_{K/\mathbb{Q}}(x)|_v = \prod_{w|v} |x|_w$ for $v \in M_{\mathbb{Q}}$ Hence we can assume $K = \mathbb{Q}$, and then this is easy, using unique factorization. ∎

- **Heights on Projective Space.**

Def: Let K be a #field, $\underline{x} = [x_0 : \cdots : x_n] \in \mathbb{P}^n(K)$.

Define • $H_K(\underline{x}) := \prod_{v \in M_K} \max\{|x_0|_v, |x_1|_v, \ldots, |x_n|_v\}$

• $h_K(\underline{x}) := \log H_K(\underline{x})$.

Lemma: H_K, h_K are well-defined

Pf Use product formula. ∎

Lemma:

1) $H_k(\underline{x}) \geq 1$

2) Let $[k':k] = n < \infty$. Then $H_{k'}(\underline{x}) = H_k(\underline{x})^n$.

Pf: Easy. //

Def: Let $\underline{x} \in \mathbb{P}^n(\bar{\mathbb{Q}})$. Define then $H(\underline{x}) := H_k(\underline{x})^{\frac{1}{[k:\mathbb{Q}]}}$

(if $\underline{x} \in \mathbb{P}^n(k)$). This is the absolute multiplicative height.

The absolute logarithmic height is $\frac{1}{[k:\mathbb{Q}]} h_k(\underline{x})$.

Corollary of Lemma: H, h are well-defined, independently of choice of coordinates and k.

Exercise: Find all points $\underline{x} \in \mathbb{P}^n(\mathbb{Q})$ such that $H(\underline{x}) = 1$.

Proposition: Let $\sigma \in G_{\mathbb{Q}} = Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, $\underline{x} \in \mathbb{P}^n(\bar{\mathbb{Q}})$.

Then $H(\underline{x}) = H(\sigma(\underline{x}))$.

Pf: Choose a Galois field $k/\mathbb{Q}$ s.t. $\underline{x} \in \mathbb{P}^n(k)$. Then σ permutes the absolute values of k, and $|\sigma(x_i)|_{\sigma v} = |x_i|_v$ if $\underline{x} = (x_0, \dots, x_n)$.

Theorem: Let $B, D \geq 0$. Then the set

$$\{\underline{x} \in \mathbb{P}^n(\bar{\mathbb{Q}}) : H(\underline{x}) \leq B \text{ and } [\mathbb{Q}(\underline{x}):\mathbb{Q}] \leq D\}$$ is finite.

Pf: Choose coordinates $[x_0 : \dots : x_n]$ s.t. $x_0 = 1$, say. Then:

(a) $H([1:x_i]) \leq H(\underline{x})$ $\forall i$

(b) $[\mathbb{Q}(x_i):\mathbb{Q}] \leq [\mathbb{Q}(\underline{x}):\mathbb{Q}]$

$\Rightarrow$ may assume $n = 1$.

So we will show that: $\{x \in \bar{\mathbb{Q}} : H([1:x]) \leq B,\ [\mathbb{Q}(x):\mathbb{Q}] = d\} < \infty$

[

Let $x_1, \dots, x_d$ be the conjugates of $x = x_i$, and:

$$\prod_{i=1}^{d} (T - x_i) = \sum_{r=0}^{d} (-1)^r s_r(x_1, \dots, x_d)\, T^{d-r}$$

Let $v \in M_K$, where $K = \mathbb{Q}(x)$.

We have:

$$|s_r(x_1, \dots, x_d)|_v = \Big| \sum_{1 \le i_1 < \dots < i_r \le d} x_{i_1} \cdots x_{i_r} \Big|_v \le C(v,r,d) \cdot \max_{1 \le i_1 < \dots < i_r \le d} |x_{i_1} \cdots x_{i_r}|_v \le$$

$$\le C(v,r,d) \max_{1 \le i \le d} |x_i|_v^r \quad \text{with} \quad C(v,r,d)^{\frac{1}{[K(v):\mathbb{Q}_v]}} \le \begin{cases} 1 & \text{if } v \in M_K^0 \\ C(d) & \text{if } v \in M_K^\infty \end{cases}$$

Hence: ($\bar{x} = (x_1, \dots, x_d)$ ← the conjugate of x!)

$$\max\{ |s_0(\bar{x})|_v, \dots, |s_d(\bar{x})|_v \} \le C(v,d) \prod_{i=1}^{d} \max\{ |x_i|_v, 1 \}^d$$

$$\Rightarrow H([s_0 : \dots : s_d]) \le \underbrace{\prod_v C(v,d)}_{=C} \prod_{i=1}^{d} H([x_i : 1])^d \le C \cdot H([x:1])^{d^2}$$

So we are reduced to the case $K = \mathbb{Q}$, which is an easy exercise. //

Corollary: If K is a #field, and $P = [x_0 : \dots : x_n] \in \mathbb{P}^n(K)$.

Fix $x_i \neq 0$. Then $H(P) = 1 \Leftrightarrow \dfrac{x_j}{x_i} = \begin{cases} 0 \\ \text{root of unity} \end{cases} \quad \forall j$.

Pf: $\Leftarrow$ is obvious

$\Rightarrow$ Suppose $H(P) = 1$. For $r \in \mathbb{N}$, set $P^r := [x_0^r : \dots : x_n^r]$.

Then $H(P^r) = H(P)^r = 1$.

As there are only finitely many points over K of ht 1 (by Thm), then

$P^r = P^s$ for some $r \neq s$ //

We want, given X projective variety $/\bar{\mathbb{Q}}$, and D a divisor on X, define a height $h_D : X(\bar{\mathbb{Q}}) \to \mathbb{R}$ such that:

- $h_D \approx h_E$ if $D \underset{\text{rat}}{\sim} E$
  (i.e. $h_D = h_E + O(1)$ ← independent of $P \in X(\bar{\mathbb{Q}})$. (so $|h_D(P) - h_E(P)| \leq C$).)
- $h_{D+E} \approx h_D + h_E$
- $h_H \approx h$ on $\mathbb{P}^n$ with H = hyperplane.

+ more properties!

Theorem 1: Let $S_{n,m} : \mathbb{P}^n \times \mathbb{P}^m \hookrightarrow \mathbb{P}^N$ be the Segre embedding

given by $\left([x_0 : \cdots : x_n], [y_0 : \cdots : y_m]\right) \longmapsto \left([x_i y_j]_{i,j}\right)$.

Then (a) $S_{n,m}^* \mathcal{O}_{\mathbb{P}^N}(1) \cong p^* \mathcal{O}_{\mathbb{P}^n}(1) \otimes q^* \mathcal{O}_{\mathbb{P}^m}(1)$ $\quad \begin{cases} p : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^n \\ q : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^m \end{cases}$

(b) $h\left(S_{n,m}(x,y)\right) = h(x) + h(y)$

(c) If $\Phi_d : \mathbb{P}^n \to \mathbb{P}^N$ is the d-uple embedding,

then $h\left(\Phi_d(x)\right) = d\,h(x)$

Pf/ Exercise, or look up in book //

Theorem 2: Let $\Phi : \mathbb{P}^n \to \mathbb{P}^m$ be a rational map, given by homogeneous polynomials $(f_0, \ldots, f_m)$ of degree d.

Let $Z := V(f_0, \ldots, f_m)$ (so Φ is defined on $\mathbb{P}^n \setminus Z$).

Then: (a) $\forall P \in (\mathbb{P}^n \setminus Z)(\bar{\mathbb{Q}})$, $h(\Phi(P)) \leq d\,h(P) + O(1)$ ← indep. of P.

(b) If $X \subseteq \mathbb{P}^n$ is closed and $X \cap Z = \emptyset$, then $\forall P \in X(\bar{\mathbb{Q}})$,

$h(\Phi(P)) = d\,h(P) + O(1)$ (so bounded above & below!).

Pf (a) write $f_i(\underline{X}) = \sum_{|\underline{e}|=d} a_{i,\underline{e}}\, \underline{X}^{\underline{e}}$ where $\underline{e} = (e_0, \dots, e_n) \in \mathbb{N}^{n+1}$, $|\underline{e}| = \sum e_i$

Note that this sum has $\binom{n+d}{n}$ summands. Fix $K/\mathbb{Q}$, $v \in M_K$

Notation: • $|P|_v := \max\{|x_i|_v \mid i=0..n\}$, for $P = [x_0 : \dots : x_n] \in \mathbb{P}^n(K)$

(Rk: depends on the choice of coordinates).

• $|f|_v := \max\{|a_{\underline{e}}|_v \mid \underline{e} \text{ multiindices}\}$ for $f(X) = \sum_{\underline{e}} a_{\underline{e}} X^{\underline{e}}$.

• $e_v(r) := \begin{cases} r & \text{if } r \in M_K^\infty \\ 1 & \text{if } r \in M_K^0 \end{cases}$ (note $\prod_v e_v(r) < \infty$).

Consider $P \in \mathbb{P}^n(K)$, $P = [x_0 : \dots : x_n]$ such that Φ is defined /k.

We have $|f_0(P)|_v = \left| \sum_{\underline{e}} a_{i,\underline{e}}\, \underline{x}^{\underline{e}} \right|_v \le e_v\left(\binom{n+d}{n}\right) \cdot |f_i|_v |P|_v^d$

whence $|\Phi(P)|_v \lesssim C \left(\max_i |f_i|_v\right) \cdot |P|_v^d$

Multiplying over all $v \in M_K$, we get:

$$H_K(\Phi(P)) \le C^{\#M_K^\infty} \cdot H_K(\Phi) \cdot H_K(P)^d \quad \text{where } H_K(\Phi) = H_K\left([a_{i,\underline{e}}]_{i,\underline{e}}\right).$$

Take log and divide by $[K:\mathbb{Q}]$ to get (a). ✓

(b) We need an inequality in the opposite direction.

Choose homogeneous equations defining X, $X = V(P_1, \dots, P_s)$

By assumption, $V(f_0, \dots, f_m, P_1, \dots, P_s) = X \cap Z = \emptyset$.

So by Hilbert's Nullstellensatz, $\sqrt{(f_0, \dots, f_m, P_1, \dots, P_s)} = (X_0, \dots, X_n)$

That is, there $\exists\, t \ge d$, and $\exists$ homogeneous polynomials g_{ij}'s, q_{ij}'s s.t.

$$g_{0j} f_0 + \dots + g_{mj} f_m + q_{1j} P_1 + \dots + q_{sj} P_s = X_j^t \quad \text{for } 0 \le j \le n.$$

We may assume that everything is defined over K (enlarge K, if necessary).

(cont'd)

Now let $P = [x_0 : \cdots : x_n] \in X(k)$, (so that $P_i(\underline{x}) = 0$, $1 \le i \le s$).

Hence $g_{0j}(\underline{x}) f_0(\underline{x}) + \cdots + g_{mj}(\underline{x}) f_m(\underline{x}) = x_j^t \quad 0 \le j \le n$

Then $|P|_v^t = \max_j |g_{0j}(\underline{x}) f_0(\underline{x}) + \cdots + g_{mj}(\underline{x}) f_m(\underline{x})|_v \le$

$\le e_v(m+1) \left(\max |g_{ij}(\underline{x})|_v\right) \left(\max |f_i(\underline{x})|_v\right) \le C \cdot |\underline{g}|_v |P|_v^{t-d} |\underline{F}(P)|_v$ (if v is fin.)

Taking $\prod_v$, we get, after taking logs:

$$dh(P) \le h(\underline{F}(P)) + O(1).$$

§3. Heights on Projective Varieties.

Def: Let $\Phi : X \to \mathbb{P}^n$ be a morphism, where $X/\bar{\mathbb{Q}}$ is a projective variety.
Then $h_\Phi(P) := h(\underline{F}(P))$, for $P \in X(\bar{\mathbb{Q}})$ (height on X).

Thm 3: X proj. smooth var., $\Phi : X \to \mathbb{P}^n$, $\Psi : X \to \mathbb{P}^n$ s.t. $\Phi^* \mathcal{O}_{\mathbb{P}^n}(1) \cong \Psi^* \mathcal{O}_{\mathbb{P}^n}(1)$
Then $h_\Phi = h_\Psi + O(1)$ (assume Φ, Ψ nonconstant).

Pf Choose $D \ge 0$ s.t. $\mathcal{L}(D) \cong \Phi^* \mathcal{O}_{\mathbb{P}^n}(1) \cong \Psi^* \mathcal{O}_{\mathbb{P}^n}(1)$.
Then we can write $\Phi = (\text{linear map}) \circ f_{|D|}$, $\Psi = (\text{linear map}) \circ f_{|D|}$
and apply Thm 2 to get the result.

Thm 4 (Height Machine): To each smooth, projective X/k, and $D \in \mathrm{Div}(X)$, we can assign a function $h_{X,D} : X(\bar{k}) \to \mathbb{R}$ s.t.

a) If $X = \mathbb{P}^n$ and $D = H$ (hyperplane) then $h_{id,H} = h + O(1)$;

b) If $D \overset{\text{rat}}{\sim} E$, then $h_{X,D} = h_{X,E} + O(1)$

c) If $D, E \in \mathrm{Div}(X)$, then $h_{X,D+E} = h_{X,D} + h_{X,E} + O(1)$

d) If $f : X \to Y$, $D \in \mathrm{Div}(Y)$, $E \in f^*([D])$, then $h_{X,E}(P) = h_{Y,D}(f(P)) + O(1)$

Moreover, $h_{X,D}$ is uniquely determined by (a)-(d), up to $O(1)$.

Proof:
Note that any divisor is the difference of two ample divisor, so we get uniqueness of $h_{X,D}$ given (a)-(d).

Construction: Let D be a divisor whose linear system is base point free, and let $\Phi_D : X \to \mathbb{P}^n$ be ~~the~~ any associated morphism (i.e. $\Phi_D^* \mathcal{O}_{\mathbb{P}^n}(1) \simeq \mathcal{L}(D)$).

Set now $h_{X,D} := h_{\Phi_D}$, so $h_{X,D}(P) = h(\Phi_D(P))$.

By Thm 3 the choice of Φ_D does not matter, up to a bounded function.

Part (a) follows, by choosing $\Phi_H = id$.

Moreover, (b) follows from Thm 3 if $|D| = |E|$ is basepoint free.

If D, E are base point free, part (c) follows from Thm 1, and (d) follows as well.

For general D, we write $D = D_1 - D_2$, D_i ample (so in particular, D_i are base point free), and we set

$$h_{X,D} := h_{X,D_1} - h_{X,D_2}.$$

If $D = E_1 - E_2$ is another such decomposition, then $D_1 + E_2 = D_2 + E_2$, and using (a), (c) for base-point free divisors we get

$$h_{X,D_1-D_2} = h_{X,E_1-E_2} + O(1).$$

Similarly, can check (b)-(d) for general divisors.

Theorem 5: The $h_{X,D}$ satisfy:

a) If $D \geq 0$ (=: is effective) and $\mathcal{B}$ is the base locus of $|D|$, then

$$h_{X,D} \geq O(1) \text{ on } (X - \mathcal{B})(\bar{K}) \qquad \left(\mathcal{B} := \bigcap_{E \in |D|} \operatorname{Supp} E\right)$$

b) If D is ample, and $D \underset{\text{alg}}{\geq} 0$, then $\lim_{\substack{P \in X(\bar{K}) \\ h_{X,D}(P) \to \infty}} \dfrac{h_{X,E}(P)}{h_{X,D}(P)} = 0$

c) For any K' w/ $[K':K] < \infty$, D ample,

$$\#\{P \in X(K') \mid h_{X,D}(P) \leq C\} < \infty.$$

Pf

(a) write $D = D_1 - D_2$, w/ D_1, D_2 base-point free.

Choose a basis $\{f_0, \dots, f_n\}$ of $H^0(X, \mathcal{L}(D_2)) \subseteq K(X)$

Now $D_1 - D_2$ is effective, so $\{f_0, \dots, f_n\} \in H^0(X, \mathcal{L}(D_1)) \Rightarrow$

$\Rightarrow$ can complete to get a basis $\{f_0, \dots, f_n, f_{n+1}, \dots, f_m\}$ of $H^0(X, \mathcal{L}(D_1))$.

We obtain morphisms

$$X \xrightarrow{\Phi_{D_1}} \mathbb{P}(H^0(X, \mathcal{L}(D_1))) \cong \mathbb{P}^m$$

$$x \longmapsto [f_0(x) : \cdots : f_m(x)]$$

(these isomorphisms change at each $x \in X$!!)

and

$$X \xrightarrow{\Phi_{D_2}} \mathbb{P}(H^0(X, \mathcal{L}(D_2))) \cong \mathbb{P}^n$$ using only $f_0, \dots, f_n$.

If $P \notin \operatorname{Supp}(D_1)$, we conclude $h_{X,D}(P) = h_{X,D_1}(P) - h_{X,D_2}(P) + O(1) =$ (because $h_{X,D}$ may be only uniquely defined w/ some other decomposition)

$$= h(\Phi_{D_1}(P)) - h(\Phi_{D_2}(P)) + O(1) = h([f_0(P) : \cdots : f_m(P)]) - h([f_0(P) : \cdots : f_n(P)]) + O(1)$$

$$\geq O(1)$$

Choose very ample divisors $H_1, \dots, H_s$ on X s.t.:

i) $D + H_i$ is base point free $\forall i$

ii) $\bigcap_{i=1}^{s} H_s = \emptyset$

$\Leftarrow$ easy to do (See book, or think (uses $\dim X \geq 1$))

Doing the previous calculation w/ $D_1 = D + H_i$, $D_2 = H_i$ we see that

$h_{X,D}(P) \geq O(1) \quad \forall P \notin \mathrm{Supp}(D)$.

Write $B = \bigcap_{i=1}^{r} D_i$, w/ $D_i \sim D$. Use the same argument $\Rightarrow h_{X,D}(P) \geq O(1)$ for $P \notin B$ //

(b) Since D is ample and $E \gtrsim_{alg} 0$, $\exists m \in \mathbb{N}$ s.t. $\forall n \in \mathbb{Z}$, $mD + nE$ is base point free (prove it as exercise).

Therefore, for any $n \in \mathbb{Z}$ $\exists$ c s.t. $m h_{X,D} - n h_{X,E} \geq -c$ (may depend on n!)

So, for $n \geq 1$, we get:

$$\frac{m}{n} + \frac{c}{n h_{X,D}(P)} \geq \frac{h_{X,E}(P)}{h_{X,D}(P)} \geq -\frac{m}{n} - \frac{c}{n h_{X,D}(P)} \qquad \forall P \in X(\bar{k}).$$

Let $h_{X,D}(P) \to \infty$, gives:

$$\frac{m}{n} \geq \frac{h_{X,E}(P)}{h_{X,D}(P)} \geq -\frac{m}{n} \Rightarrow \left| \frac{h_{X,E}(P)}{h_{X,D}(P)} \right| \leq \frac{m}{n} \quad \forall n \in \mathbb{Z} \Rightarrow \checkmark$$ //

• Heights on Abelian Varieties.

Thm: Let A/k be an abelian variety, $D \in \mathrm{Div}(A)$. Then:

a) Suppose $m \in \mathbb{Z}$. Then, $\forall P \in A(\bar{k})$,

$$h_{A,D}([m]P) = \frac{m^2+m}{2} h_{A,D}(P) + \frac{m^2-m}{2} h_{A,D}(-P) + O(1)$$

b) If $D \sim [-1]^* D$ (i.e. D is symmetric), then

$$h_{A,D}([m]P) = m^2 h_{A,D}(P) + O(1)$$

$$h_{A,D}(P+Q) + h_{A,D}(P-Q) = 2h_{A,D}(P) + 2h_{A,D}(Q) + O(1)$$

c) If $-D \sim [-1]^* D$ (i.e. D is antisymmetric), then:

$$h_{A,D}([m]P) = m\, h_{A,D}(P) + O(1)$$
$$h_{A,D}(P+Q) = h_{A,D}(P) + h_{A,D}(Q) + O(1).$$

← the divisors in $\mathrm{Pic}^0(A)$.

Pf (Thm):

(a) The theorem of the cube implies that $[m]^* D \sim \frac{m^2+m}{2} D + \frac{m^2-m}{2} [-1]^* D$

Now use the properties of the height machine, noting:

$$h_{A,[m]^*D}(P) = h_{A,D}([m]P) + O(1).$$

(b) The first statement is clear from (a).

For the second part (parallelogram law), we need to prove: (and use the height machine)

$$s^* D + d^* D \sim 2\,pr_1^* D + 2\,pr_2^* D \qquad (\text{on } A \times A)$$

where $s, d, pr_1, pr_2 : A \times A \to A$ s.t. $s(P,Q) = P+Q$, $pr_1(P,Q) = P$

$d(P,Q) = P-Q$, $pr_2(P,Q) = Q$

So we need to see that

$$\Gamma_D := s^* D + d^* D - pr_1^* D - pr_2^* D \sim 0 \quad \text{i.e.} \quad \mathcal{L}(\Gamma_D) \cong \mathcal{O}_{A\times A}.$$

Thm (Seesaw principle): Let X be a complete variety, and T an integral scheme $/k$. Let $\mathcal{L}$ be a line bundle on $X \times T$.

Write $\mathcal{L}_t$ = pullback of $\mathcal{L}$ to $X \times_T k(t)$, $t \in T$.

Sps $\mathcal{L}_t \cong \mathcal{O}_{X \times_T k(t)}$ $\forall t \in T$, and that $\exists\, x \in X(k)$ s.t. $\mathcal{L}_x \cong \mathcal{O}_T$

Then $\mathcal{L}$ is trivial.

Remark: By semicontinuity, it suffices to check it for t in some dense subset.

In our application, $X = T = A$, $t = a \in A(\bar{k})$, and $x = 0 \in A$.

Let $j : A \to A \times A$, $a \mapsto (a, a)$. Need to check that $j^*(\mathcal{L}(\Gamma_D)) \cong \mathcal{O}_A$

← we should pullback the line bundle but abuse notation

$$j^*\left(s^* D + d^* D - 2pr_1^* D - 2pr_2^* D\right) = (s\circ j)^* D + (d\circ j)^* D - 2(pr_1 \circ j)^* D - 2(pr_2 \circ j)^* D$$

$$\sim D + [-1]^* D - 2[0] - 2D \sim [-1]^* D - D \sim 0 \quad \checkmark$$

Let $i_a : A \to A \times A$, $b \mapsto (b, a)$. Need to check $i_a^* \mathcal{L}(\Gamma_D) \cong \mathcal{O}_{A_{k(a)}}$

We compute:

$$i_a^*(\Gamma_D) = (s\circ i_a)^* D + (d\circ i_a)^* D - 2(pr_1\circ i_a)^* D - 2(pr_2\circ i_a)^* D \sim$$

$$\sim t_a^* D + t_{-a}^* D - 2D - 2\cdot[0] \sim 0 \quad \text{by the theorem of the square.}$$

Hence, applying the seesaw principle, $\Gamma_D \sim 0$.

(c) is similar, and we omit it.

Canonical Heights

Let X/k be a smooth projective var., $\Phi: X \to X$ and $D \in \mathrm{Div}(X)$, such that $\Phi^* D \sim \alpha D$ for some $\alpha > 1$.

Then:

Thm: There exists a unique function $\hat{h}_{X,D,\Phi}: X(\bar{k}) \to \mathbb{R}$ such that:

a) $\hat{h}_{X,D,\Phi} = h_{X,D} + O(1)$

b) $\hat{h}_{X,D,\Phi}(\Phi(P)) = \alpha \cdot \hat{h}_{X,D,\Phi}(P) \quad \forall P \in X.$

c) $\hat{h}_{X,D,\Phi}$ depends only on $[D]$.

Proof: (c) is obvious from the others

We define $\hat{h}_{X,D,\Phi}(P) := \lim_{n\to\infty} \frac{1}{\alpha^n} h_{X,D}(\Phi^n(P))$

Exercise: The limit exists, and (a), (b), (c) hold.

Example:
- $X = A$, D a symmetric divisor, $\Phi = [m]$, $m \geq 2$.
- $X = \mathbb{P}^n$, $[D] = [H]$, $\Phi: \mathbb{P}^n \to \mathbb{P}^n$ a morphism of degree $d \geq 2$, so that $\Phi^*[D] = d\cdot[D]$.

Def: Let $\Phi: X \to X$, $P \in X(\bar{K})$ is <u>pre-periodic</u> if $\{P, \Phi(P), \Phi^2(P), \dots\}$ is finite.

Prop: Suppose that D is ample, and that $\Phi^* [D] = \alpha [D]$, $\alpha > 1$.

Then: (a) $\hat{h}_{X,D,\Phi} \geq 0$ and $\hat{h}_{X,D,\Phi}(P) = 0 \iff P$ is preperiodic.

(b) If K'/K is a finite extension of K, then there are finitely-many preperiodic points in $X(K')$.

pf (b) follows from (a) and our finiteness theorem.

The first part of (a) is immediate, as D is ample.

If P is preperiodic, $\hat{h}_{X,D,\Phi}(P) = 0$ because $\alpha > 1$.

Conversely, if $\hat{h}_{X,D,\Phi}(P) = 0$, then $\Phi^n(P)$ is defined over $K(P)$ $\forall n \geq 0$ (extension of K obtained by adjoining coords of P)

Therefore, $\{P, \Phi(P), \dots\}$ is finite as $\hat{h} \approx h$.

Application: $X = A$, $\Phi = [m]$ $m > 1$, D an ample symmetric divisor.

(start with an ample divisor D' then $[-1]^* D'$ is ample, and also $[-1]^* D' + D'$ is ample and symmetric).

Now $P \in A(K')$ is $[m]$-preperiodic $\iff \exists\, i > j > 0$ s.t. $[m^i] P = [m^j] P \iff$

$\iff [m^i - m^j] P = 0$

Note that for any $r \in \mathbb{Z}$, $\exists\, i > j > 0$ s.t. $r \mid m^i - m^j$ (exercise)

So P is $[m]$-preperiodic $\iff P$ is torsion.

Canonical Heights on abelian varieties

Thm: Let A/K be an abelian variety, and $D \in \mathrm{Div}(A)$ s.t. $[-1]^* [D] = [D]$.

Then $\exists\ \hat{h}_{A,D} : A(\bar{K}) \to \mathbb{R}$ s.t.

a) $\hat{h}_{A,D} = h_{A,D} + O(1)$

b) $\hat{h}_{A,D}([m]P) = m^2 \hat{h}_{A,D}(P) \quad \forall m, \forall P.$

c) $\hat{h}_{A,D}(P+Q) + \hat{h}_{A,D}(P-Q) = 2\hat{h}_{A,D}(P) + 2\hat{h}_{A,D}(Q)$

d) $\hat{h}_{A,D}$ is a quadratic form, with associated pairing $\langle P, Q \rangle_D := \frac{1}{2}\left(\hat{h}_{A,D}(P+Q) - \hat{h}_{A,D}(P) - \hat{h}_{A,D}(Q)\right)$

e) (a)+(b) determine $\hat{h}_{A,D}$ uniquely (even knowing only one $m \geq 2$), and only depends on A and $[D]$.

Pf $\hat{h}_{A,D} := \hat{h}_{A,D,\Phi}$ where $\Phi := [2] : A \to A$.

This proves (a) and uniqueness.

For part (b), note first $h_{A,D}([m]Q) = m^2 h_{A,D}(Q) + O(1)$.

Then $\hat{h}_{A,D}([m]P) = \lim_{n\to\infty} \frac{1}{4^n} h_{A,D}([2^n m]P) = \lim_{n\to\infty} \frac{1}{4^n}\left(m^2 h_{A,D}([2^n]P) + O(1)\right) =$

$= m^2 \hat{h}_{A,D}(P)$.

Part (c) is done similarly, using the $\lim$ with $O(1)$.

Part (d) follows from (c) by linear algebra. ∎

Proposition: Let A/K be an abelian variety, D an ample symmetric divisor.

Then a) $\hat{h}_{A,D} \geq 0$, and $\hat{h}_{A,D}(P) = 0 \iff P \in A(\bar{K})_{\mathrm{tors}}$

b) $\langle \cdot, \cdot \rangle_D$ extends to a positive definite quadratic form on $A(\bar{K}) \otimes \mathbb{R}$

Proof:
(a) follows from general properties of canonical heights & what we saw last time.

For (b) suppose that $\hat{h}_{A,D}(P) = 0$ for some $P \in A(\bar{K}) \otimes \mathbb{R}$. Write $P = \sum_{i=1}^{s} a_i P_i$, $a_i \in \mathbb{R}$, $P_i \in A(\bar{K})$

We may assume, after extending the ground field K, that all $P_i \in A(K)$. ↓

(cont pf)

we will show that $q = \hat{h}_{A,D}\big|_{\mathbb{R}\langle P_1,\dots,P_s\rangle}$ ($\mathbb{R}\langle P_1,\dots,P_s\rangle$ ← span of P_i as $\mathbb{R}$-vectorspace) is positive definite.

Let $V := \mathbb{R}\langle P_1,\dots,P_s\rangle$, $\Lambda := \mathbb{Z}\langle P_1,\dots,P_s\rangle \subseteq V$.

- $q|_\Lambda$ is positive definite

It could happen, though, that $q|_{\Lambda\setminus\{0\}}$ wasn't bounded below, and then after allowing real coefficients we might loose definiteness.

we will show that $q|_{\Lambda\setminus\{0\}}$ is bounded below.

Let $B \geq 0$. Claim: $\{\lambda \in \Lambda \mid q(\lambda) \leq B\}$ is finite.

It follows from standard properties of heights for ample D, using that

$\Lambda \subseteq A(k)/_{\text{torsion}}$.

One then applies Minkowski's theorem on fundamental domains of lattices in symmetric vectorspaces, which implies that q is positive definite. //

Theorem: Let A/k be an abelian variety, D a divisor on A s.t. $[-1]^*[D] = [-D]$.

Then $\exists\ \hat{h}_{A,D} : A(\bar{k}) \to \mathbb{R}$ s.t.

(a) $\hat{h}_{A,D} = \hat{h}_{A,D} + O(1)$

(b) $\hat{h}_{A,D}(P \pm Q) = \hat{h}_{A,D}(P) \pm \hat{h}_{A,D}(Q)$

Moreover, $\hat{h}_{A,D}$ is uniquely determined by (a), (b) and $[D]$.

Pf Like in the symmetric case. //

Recall that $[-1]^*D = [-D] \Leftrightarrow [D] \in \mathrm{Pic}^0(A)$. We obtain, writing $\hat{A} = \mathrm{Pic}^0(A)$,

Theorem: The assignement $[D] \longmapsto \hat{h}_{A,D}$ defines a pairing

$$[\cdot,\cdot] : A(\bar{k}) \times \hat{A}(\bar{k}) \longrightarrow \mathbb{R}$$ such that

a) $[\cdot;\cdot]$ is bilinear, with kernel in either side being the torsion subgroup.

b) $[\cdot,\cdot]_A = \langle \cdot,\cdot \rangle_D$ on $A \times \hat{A}$, where D = Poincaré divisor.

Pf omitted //

• Mordell-Weil Theorem.

Thm: Let k be a number field (or any field finitely generated (as a field) over its prime field) (includes function fields in any finite number of variables).

Let A be an abelian variety / k. Then $A(k)$ is a finitely-generated abelian group.

(**Note**: $A(\bar{k})$ is not finite-generated, because it's divisible!).

How to prove it:

Step 1: $\dfrac{A(k)}{2A(k)}$ is finitely-generated. (Rk: $\left(\dfrac{A}{2A}\right)(k) = 0$ as A is divisible!)

Step 2: Infinite descent using $\hat{h}_{A,D} \geq 0$:

- $\{ x \in A(k) : \hat{h}_{A,D}(x) \leq C \}$ is finite
- $\hat{h}_{A,D}([2]x) = 4\hat{h}_{A,D}(x)$. . . . . (see next page)

~~So choose generators $\{P_1, \dots, P_r\}$ of $\dfrac{A(k)}{2A(k)}$, $P_i \in A(k)$~~

• Infinite descent:

• Assume $A(\kappa)/nA(\kappa)$, for some $n \geq 2$, is finite.

Choose an ample symmetric divisor $D \in Div(A)$, and let

$$\|\cdot\| := \sqrt{\hat{h}_{1,D}} : A(\bar{\kappa}) \to \mathbb{R}.$$

Choose lifts $P_1, \dots, P_s$ of elements in $A(\kappa)/nA(\kappa)$

Set $C := \max\{\|P_1\|, \dots, \|P_s\|\}$.

Claim: $A(\kappa)$ is generated by $\{P_1, \dots, P_s\} \cup \{R \in A(\kappa) : \|R\| \leq C\}$.

Pf: Let $Q_0 \in A(\kappa)$, $Q_0 = nQ_1 + P_{i_1}$

$$\vdots$$

$$Q_r = nQ_{r+1} + P_{i_r}$$

and note $\|Q_{r+1}\| = \frac{1}{n}\|Q_r - P_{i_r}\| \leq \frac{1}{n}\left(\|Q_r\| + C\right)$ (*).

If $\|Q_r\| \leq C$, we are done.

Else, (*) $< \frac{2}{n}\|Q_r\|$ and, since $n \geq 2$, $\|Q_{r+1}\| < \|Q_r\|$.

As there are only finitely many points of bounded norm, $\|Q_i\| \leq C$ for some i. //

Theorem (Weak Mordell-Weil): Let κ be a number field, A/κ an abelian variety, and $n \geq 2$. Then: $A(\kappa)/nA(\kappa)$ is finite.

Proof:

Consider the sequence of G_κ ($= Gal(\bar{\kappa}/\kappa)$) - modules:

$$0 \to A[n] \to A \xrightarrow{[n]} A \to 0 \qquad (A = A(\bar{\kappa})!)$$

Taking Galois cohomology (see Cassels-Frohlich, for example), we get:

$$0 \to A(\kappa)[n] \to A(\kappa) \to A(\kappa) \to H^1(G_\kappa, A[n]) \to H^1(G_\kappa, A) \xrightarrow{[n]} H^1(G_\kappa, A) \to \dots$$

We get a short exact sequence: ↘

$$0 \to \frac{A(K)}{nA(K)} \xrightarrow{\delta} H^1(G_K, A[n]) \to H^1(G_K, A)[n] \to 0$$

$$x \longmapsto [\sigma \mapsto \sigma(y) - y]$$

w/ $[n]y = x$

Unfortunately, $H^1(G_K, A[n])$ is not finite in general.

Write $G = G_K$, and let $v \in M_K$. Write $G_v \subseteq G$ be the decomposition group of v. (i.e $G_v \cong G_{K_v}$). and write $I_v \subseteq G_v$ for an inertia subgroup (well-defined up to conjugation).

Remark: Let K/k be a finite extension. Then the image of I_v in $G(K/k)$ is trivial iff K/k is unramified at v.

The image of G_v is trivial $\iff$ K/k is completely decomposed at v.

By restriction, we get diagrams (one for each v):

$$\begin{array}{ccccccc} 0 & \to & \frac{A(K)}{nA(K)} & \to & H^1(G, A[n]) & \to & H^1(G, A)[n] \to 0 \\ & & \downarrow \text{res} & & \downarrow \text{res} \quad \searrow \varphi & & \downarrow \text{res} \\ 0 & \to & \frac{A(K_v)}{nA(K_v)} & \to & H^1(G_v, A[n]) & \to & H^1(G_v, A)[n] \to 0 \end{array}$$

Def: The n^{th} Selmer group of A/K is $Sel^{(n)}(A/K) = \bigcap_v \overline{\ker\left(H^1(G, A[n]) \to H^1(G_v, A)[n]\right)}^{\varphi}$

Clearly, $\frac{A(K)}{nA(K)} \hookrightarrow Sel^{(n)}(A/K)$.

So we need to show that $Sel^{(n)}(A/K)$ is finite.

Suppose that $A[n](\bar{K}) \subseteq A(K)$ (we will deal with this later).

By the Weil pairing, it implies that $\mu_n(\bar{K}) \subseteq A(K)$.

We have $H^1(G_K, A[n]) \cong \bigoplus_{\text{zg}} H^1(G_K, \mathbb{Z}/n\mathbb{Z}) \cong \bigoplus_{\text{zg}} \frac{K^*}{(K^*)^n}$

(↑ zg: Kummer theory; $\frac{K^*}{(K^*)^n}$: classifying deg-n cyclic extensions of K.)

There are only finitely-many ~~ramified~~ extensions of degree n which are unramified outside a finite number of places.

Def Let M be a continuous G_K-module, $\alpha \in H^r(G_K, M)$. We say that

α is <u>unramified</u> at $v \iff \alpha|_{I_v} = 0 \in H^r(I_v, M)$.

Write $H^1_S(G_K, M)$ = subgroup of classes unramified <u>outside</u> at some $S \subseteq M_K$.

<u>Theorem</u>: Let $S = M_K^\infty \cup \{v : v|n\} \cup \{v : A \text{ has bad reduction at } v\}$ ← finite set!

Then: (a) $H^1_S(G_K, A[n])$ is finite.

(b) $Sel^{(n)}(A/K) \subseteq H^1_S(G_K, A[n])$.

Proof:

(a) There's a finite galois extension L/K s.t. $A[n](\bar{K}) \subseteq A(L)$

We have an exact sequence:

$$0 \to H^1(G(L/K), A[n]^{G_L}) \xrightarrow{\text{inf}} H^1(G_K, A[n]) \xrightarrow{\text{res}} H^1(G_L, A[n]).$$

(finite gp (both $G(L/K)$ and $A[n]^{G_L}$ are finite).

This implies (letting $\tilde{S}$ = set containing all places above those in S).

$$0 \to H^1_{\tilde{S}}(G(L/K), A[n]^{G_L}) \to H^1_S(G_K, A[n]) \to H^1_{\tilde{S}}(G_L, A[n])$$

So we may assume $A[n](\bar{K}) \subseteq A(K)$, and then Kummer theory proves (a).

In fact, if $K' \supseteq A[n]$, then

$$H^1_{\tilde{S}}(G_{K'}, \mathbb{Z}/n) \cong \mathrm{Hom}_{\tilde{S}}\left(G_{K'}, \mathbb{Z}/n\right) \cong \mathrm{Hom}\left(G(L/K'), \mathbb{Z}/n\right)$$

where $L = \max$ unram outside $\tilde{S}$ extension of exponent n.

For part (b), let $\Phi \in Sel^{(n)}(A/K)$, $v \notin S$.

Choose $y \in A(\bar{K}_v)$ s.t. $\Phi(\sigma) = \sigma(y) - y$ for $\sigma \in G_v (\cong G_{K_v})$

(this is possible because $Sel^{(n)}(A/K) \longrightarrow H^1(G_{K_v}, A_{K_v})[n]$ is the 0 map).

Then, if $\sigma \in I_v$, reduction mod $\mathfrak{P}_v \subseteq \mathcal{O}_K$ is:

$$\overline{\sigma(y) - y} = \overline{\sigma(y)} - \bar{y} = \bar{0} \quad \text{because } \sigma \text{ acts trivially on the inertia fields.}$$
$$\uparrow A[n](K(v)) \quad , K(v) = \mathcal{O}_K/\mathfrak{P}_v .$$

However, $\Phi(\sigma) \in A[n](K)$, so $\overline{\Phi(\sigma)} = \bar{0}$.

We now have the theorem:

Thm (*)! Let v be a place of good reduction, $v \nmid n$. Then the reduction map

$$A(K)[n] \hookrightarrow A(K(v))[n] \quad \text{is injective.}$$

And so $\Phi(\sigma) = 0$ for $\sigma \in I_v$ $\forall v \notin S \Rightarrow \Phi \in H^1_S(G_K, A[n])$. ∎

Proof of Thm (*): we do a scheme-theoretic proof (not only formal groups).

Let A be our abelian variety over $K \supseteq \mathcal{O}_K$ (its ring of integers).

A **model** for A over $\mathcal{O}_K[S^{-1}]$ is a scheme $\mathcal{A} \longrightarrow \mathcal{B} = \mathrm{Spec}\left(\mathcal{O}_K[S^{-1}]\right)$

such that the fiber $\mathcal{A}_K \cong A$.

∎

Lemma 1: Suppose that $\mathcal{A}$ is a proper model of A (i.e. $\mathcal{A} \to B$ is proper).
Then $\mathcal{A}(\mathcal{O}_K[S^{-1}]) \cong A(K)$ (as sets)

Pf: Use the valuative criterion of properness. //

Def: Let $\mathfrak{p} \subset \mathcal{O}_K[S^{-1}]$ be a prime, $\kappa = \mathcal{O}_K[S^{-1}]/\mathfrak{p}$ (a finite field), and

$A_\kappa = A \times_{\mathcal{O}_K[S^{-1}]} \kappa$. (Assume $\mathcal{A}$ is a proper model)

Then we get a map $A(K) \longrightarrow A_\kappa(\kappa)$ as follows:

Given $x \in A(K)$, x corresponds to a section $x \in \mathcal{A}(\mathcal{O}_K[S^{-1}])$, i.e

$x : B \to A$ (with σ, $\mathrm{id} \to B$) . Can pullback back to $\operatorname{Spec} \kappa \xrightarrow{\bar{x}} A_\kappa \in A_\kappa(\kappa)$ (with $\to \operatorname{Spec} \kappa$)

Proposition 2: There exists a finite set of places S and a model $\mathcal{A}$ over $\mathcal{O}_K[S^{-1}]$ of A such that:

a) $\mathcal{A}$ is proper

b) $\mathcal{A}$ is flat

c) $\mathcal{A}$ is a group scheme over B (i.e. we have $\mathcal{A} \times_B \mathcal{A} \to \mathcal{A}$, $B \to \mathcal{A}$)

(A proper flat group scheme is called "Abelian scheme over B". They are commutative.)

d) For any geometric point $\operatorname{Spec}(\bar{F}) \to B$, $A_{\bar{F}}$ is an abelian variety.

(In particular, $\mathcal{A} \to B$ is smooth!).

Remark: The primes outside S are those where A "has good reduction".

A has bad reduction at a prime $\mathfrak{p} \subset \mathcal{O}_K$ if there is no model like this in Prop 2 over $\mathcal{O}_{K,\mathfrak{p}}$.

Note: The reduction map $A(K) \to A_{K(\mathfrak{P})}(K(\mathfrak{P}))$ is a homomorphism, for $\mathfrak{P} \notin S$.

Pf of Prop:

Embed $A \hookrightarrow \mathbb{P}^N_K$, given by equations $f_1, \dots, f_s$, such that

$\left(\frac{\partial f_i}{\partial x_j}\right)_{i,j}$ has maximal rank along A, and can assume (by scaling)

that $\frac{\partial f_i}{\partial x_j}$ have coefficients in $\mathcal{O}_K$.

Throw away sufficiently many primes so that the projective scheme defined by $f_1, \dots, f_s$ is smooth over $\mathcal{O}_K[S_1^{-1}]$.

Enlarge S_1 to S such that the group structure is defined over $\mathcal{O}_K[S^{-1}]$. //

Lemma 3: Let $\mathcal{A} \to B$ be an abelian scheme (i.e. proper flat gp scheme).

Then $[n]_{\mathcal{A}} : \mathcal{A} \to \mathcal{A}$ (over B) is a flat morphism, and $\mathcal{A}[n]$ is a finite and flat B-group scheme, of order n^{2g}.

(i.e. $\mathcal{A}[n] = \underline{\mathrm{Spec}}(\mathcal{R})$, $\mathcal{R}$ a sheaf of $\mathcal{O}_B$-algebras, locally free of rank n^{2g}).

Warning: There are flat finite group schemes over $\bar{\mathbb{F}}_p$ that are not reduced.

(e.g. μ_p has order p, but $\mu_p = \mathrm{Spec}\, \bar{\mathbb{F}}_p[X]/(X^q-1)_{i(X-1)^p}$.).

Pf

(1) Do it over fields
(2) Use that $\mathcal{A}$ itself is flat. $\Big\} \Rightarrow$ flatness

(3) $\mathcal{A}[n] \to B$ is proper + quasifinite $\Rightarrow$ finite.

Corollary 4: If, with the same set-up, we assume in addition that $\frac{1}{n} \in \mathcal{O}_B$, then $A[n] \to B$ is étale, and therefore the reduction map $A[n](\bar{K}) \to A_{\bar{k}}[n](\bar{k})$ is an isomorphism for any residue field k of B.

(Assume for this that $B = \mathrm{Spec}$ (Dedekind Domain).)

Diophantine Approximation

Q: Given $\alpha \in \mathbb{R}$, how easy is it to approximate α with $\frac{p}{q} \in \mathbb{Q}$, i.e. are there lots of numbers $\frac{p}{q}$ s.t. $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^N}$, $N \gg 0$?

Example: Let $\alpha = \sum_{n \geq 0} 2^{-n!}$. Then, $\forall \varepsilon > 0$, $\exists$ ∞-ly many $\frac{p}{q} \in \mathbb{Q}$ s.t. $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^\varepsilon}$

Thm 1 (Dirichlet): For $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, there are ∞-ly many $\frac{p}{q} \in \mathbb{Q}$ s.t.

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}$$

Thm 2 (Roth's Thm): For $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, α algebraic and $\varepsilon > 0$, there are only finitely many $\frac{p}{q} \in \mathbb{Q}$ s.t. $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{2+\varepsilon}}$

Thm 3 (Liouville): Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, α algebraic of degree $d \geq 2$ and $\varepsilon > 0$, there are only finitely many $\frac{p}{q} \in \mathbb{Q}$ s.t. $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{d+\varepsilon}}$

Pf (Thm 3):

Step 1: Construct an auxiliary polynomial, vanishing at α. We'll use the minimal polynomial $p(x)$ of α.

Step 2: Show that $p\left(\frac{p}{q}\right) \neq 0$ if $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{d+\varepsilon}}$ and $q \gg 0$. (Later)

Step 3: $p\left(\frac{p}{q}\right) \neq 0$ because $p(x)$ is irreducible in $\mathbb{Q}[x]$!

Step 4: Contradiction because, if ∞-ly many approximations, we can find one with $q \gg 0$.

So we need to prove step 3:

$$P\left(\frac{p}{q}\right) = \frac{N}{q^d} \quad (\text{as } P(X) \text{ has degree } d), \quad N \in \mathbb{Z}$$

Now, $P(X) = \sum_{i=1}^{d} \frac{1}{i!} P^{(i)}(\alpha)(X-\alpha)^i$ (no constant term as $P(\alpha)=0$)

$$\Rightarrow \left|\frac{N}{q^d}\right| = \left|P\left(\frac{p}{q}\right)\right| \leq \left|\frac{p}{q}-\alpha\right| \cdot \sum_{i=1}^{d} \frac{1}{i!} \left|P^{(i)}(\alpha)\right| \underbrace{\left|\frac{p}{q}-\alpha\right|^{i-1}}_{\leq 1} \leq \left|\frac{p}{q}-\alpha\right| \cdot d \cdot \underbrace{C(\alpha)}_{\text{some constant}} \leq$$

$$\leq \frac{B(\alpha)}{q^{d+\varepsilon}}.$$

$$\Rightarrow |N| \leq \frac{B(\alpha)}{q^{\varepsilon}}. \quad \text{If } q \gg 0, \ |N| < 1, \text{ so } N = 0 \Rightarrow \checkmark$$

We now state (and prove) a more general result than Roth's:

Theorem 4: Let K be a number field, $S \subseteq M_K$ a finite set, and extend each $v \in M_K$ to $\bar{K}$ (choose one such extension for each v). Let $\alpha \in \bar{K}$, $\varepsilon > 0$. Then there are only finitely many $\beta \in K$ s.t.

$$\prod_{v \in S} \min\left\{ \|\beta-\alpha\|_v, 1 \right\} \leq \frac{1}{H_K(\beta)^{[K:\mathbb{Q}](2+\varepsilon)}} \qquad (*)$$

pf (sketch):

Step 1: Construct $P(X_1, \dots, X_m)$ s.t. P vanishes to high degree at $(\alpha, \alpha, \dots, \alpha)$.

Choose $\beta_1, \dots, \beta_m$ s.t. $(*)$ holds and $H_K(\beta_1) \gg 0$, $H_K(\beta_{i+1}) \gg H_K(\beta_i)$

Step 2: Show that P vanishes to fairly high order at $(\beta_1, \dots, \beta_m)$.

Step 3: Roth's lemma: P cannot vanish to a high order at $(\beta_1, \dots, \beta_m)$

Step 4: Contradiction.

Proof of Thm 1 (Dirichlet)

Let $Q \geq 1$. Consider $\{ q\alpha - \lfloor q\alpha \rfloor : q = 0, 1, \dots, Q \} \subseteq [0,1]$.

Δ, $\alpha \notin \mathbb{Q}$, # set $= Q+1$.

By pigeonhole pple, $\exists\, q_1, q_2, 0 \leq q_1 < q_2 \leq Q$ s.t. $\left| (q_1\alpha - \lfloor q_1\alpha \rfloor) - (q_2\alpha - \lfloor q_2\alpha \rfloor) \right| \leq \frac{1}{Q}$

s.o. $\left| \frac{\lfloor q_2\alpha \rfloor - \lfloor q_1\alpha \rfloor}{q_2 - q_1} - \alpha \right| \leq \frac{1}{(q_2-q_1)Q} \leq \frac{1}{(q_2-q_1)^2}$

Making Q increase to ∞, this yields ∞ly many approximations. //

Proposition 5: (for the proof of Thm 4 (Roth's)): It suffices to look at algebraic integers $\alpha \in \bar{k}$.

Prop 6: Thm 4 $\Leftrightarrow$ Thm 7, where:

Thm 7: Let k be a # field, $S \subseteq M_k$ finite set of places, $\varepsilon > 0$, $\alpha \in \bar{k}$.

Suppose $\xi : S \to [0,1]$ s.t. $\sum_{v \in S} \xi_v = 1$.

Then there are only finitely-many $\beta \in k$ s.t.:

$$(**) \qquad \|\beta - \alpha\|_v \leq \frac{1}{H_k(\beta)^{(2+\varepsilon)\xi_v}} \quad \forall v \in S.$$

Pf of Prop 6 (Thm 4 $\Leftrightarrow$ Thm 7):

a) Thm 4 $\Rightarrow$ Thm 7:

If $\|\beta - \alpha\|_v \leq \frac{1}{H_k(\beta)^{(2+\varepsilon)\xi_v}} \quad \forall v \in S \Rightarrow \prod_{v \in S} \min\{ \|\beta-\alpha\|_v, 1 \} \leq \frac{1}{H_k(\beta)^{2+\varepsilon}}$ //

b) Thm 7 $\Rightarrow$ Thm 4:

First, as there are only finitely-many β w/ $H_k(\beta) = 1$ (roots of unity), we can WLOG assume $H_k(\beta) > 1$.

Now (**) with $\min\{1, \|\beta-\alpha\|_v\}$ (and possibly different S) is equivalent to (**)

(because $1 \leq \frac{1}{H_k(\beta)^{(2+\varepsilon)\xi_v}} \Leftrightarrow \xi_v = 0$).

V

Now, suppose $\beta \in K$ satisfies $(*)$, i.e $\prod_v \min\{1, \|\beta-\alpha\|_v\} \le \frac{1}{H_K(\beta)^{(2+\varepsilon)}}$. (for ε)

Fix $\varepsilon' < \varepsilon$, and for $v \in S$, let $\lambda_v(\beta) \ge 0$ be defined by:

$$\min\{\|\beta-\alpha\|_v, 1\} = \frac{1}{H_K(\beta)^{(2+\varepsilon')\lambda_v(\beta)}}$$

~~Note that $\prod(\text{RHS}) \le \frac{1}{H_K(\beta)^{(2+\varepsilon)}} < \frac{1}{H_K(\beta)^{(2+\varepsilon')}}$~~

Note: Since $\varepsilon' < \varepsilon$, there exist $N \in \mathbb{N}$, not depending on β, s.t
(and $H_K(\beta) \ge 1+\delta$ for some $\delta > 0$)

$$\sum_{v \in S} \lambda_v(\beta) \ge 1 + \frac{1}{N}$$

Then $\exists\ \xi : S \to [0,1] \cap \mathbb{Z}\left[\frac{1}{N \cdot |S|}\right]$ s.t.

a) $\xi_v \le \lambda_v(\beta)\ \forall v \in S$

b) $\sum_{v \in S} \xi_v = 1$

That is, β satisfies $(*)$ for $(\alpha, \varepsilon) \Rightarrow \beta$ satisfies $(**)$ for $(\alpha, \varepsilon', \xi)$

Note: there are only finitely many possible functions ξ, as they have bounded denominator.

The proof of Roth's theorem.

(0) Preliminaries:

Def: $\partial_{i_1 \dots i_r} := \frac{1}{i_1! i_2! \cdots i_r!} \frac{\partial^{i_1+\dots+i_r}}{\partial^{i_1} X_1 \cdots \partial^{i_r} X_r}$

Lemma 1: Let $P(X_1, \dots, X_m) \in \mathbb{Z}[\underline{X}]$, $\underline{i} := (i_1, \dots, i_m)$. Assume $\deg_{X_j} P \le r_j$

Then: a) $\partial_{\underline{i}} P \in \mathbb{Z}[\underline{X}]$

b) $|\partial_{\underline{i}} P| \le 2^{r_1+\dots+r_m} |P|$ where $|P| = \max\{|\text{coeff}|\}$.

(cont pf)

Remark: The Taylor series of P around $(a_1,\dots,a_m)$ is:

$$\sum_{0\le \underline{i}\le \underline{r}} \partial_{\underline{i}} P(a_1,\dots,a_m)\,(X-a_1)^{i_1}\cdots(X-a_m)^{i_m}$$

Def: Let K be a field, $P\in K[X_1,\dots,X_m]$, $(\alpha_1,\dots,\alpha_m)\in K^m$, and $r_1,\dots,r_m>0$ be integers. Then the "index of P at $\underline{\alpha}$ relative to $\underline{r}$" is:

$$\mathrm{Ind}_{\underline{\alpha},\underline{r}}(P) := \min\left\{ \frac{i_1}{r_1}+\cdots+\frac{i_m}{r_m} : \partial_{\underline{i}} P(\underline{\alpha})\neq 0 \right\}$$

Lemma 2: Let $P,P'\in K[\underline{X}]$, $\underline{r}$, $\underline{\alpha}$ fixed.

a) $\mathrm{Ind}(\partial_{\underline{i}} P) \ge \mathrm{Ind}(P) - \left(\frac{i_1}{r_1}+\cdots+\frac{i_m}{r_m}\right)$

b) $\mathrm{Ind}(P+P') \ge \min\{\mathrm{Ind}(P), \mathrm{Ind}(P')\}$

c) $\mathrm{Ind}(P\cdot P') = \mathrm{Ind}\,P + \mathrm{Ind}\,P'$

Note: $\mathrm{Ind}\,P \le m$ if $P\neq 0$ and $\underline{r}\ge \deg P$.

$\mathrm{Ind}\,P = 0 \iff P(\underline{\alpha})\neq 0$.

Lemma 3: Let $K/\mathbb{Q}$ be a # field, $\alpha\in K^\times$, $S\subseteq M_K$.

Then $\prod_{v\notin S} \min\{\|\alpha\|_v, 1\} \ge \frac{1}{H_K(\alpha)}$

Lemma 4: Let α be an algebraic integer, $Q(X)=X^d+a_1X^{d-1}+\cdots+a_d$ its minimal polynomial (so $Q(X)\in\mathbb{Z}[X]$). Then, for $\ell\ge 0$, write

$$\alpha^\ell = a_1^{(\ell)}\alpha^{d-1}+\cdots+a_d^{(\ell)}, \quad \text{and} \quad |a_i^{(\ell)}| \le (|Q|+1)^\ell.$$

Lemma 5: Let $m\ge 1$, $r\ge 0$. Then there are exactly $\binom{r+m-1}{r}$ m-partitions of r (i.e. $(i_1,\dots,i_m)\in\mathbb{N}_0^m : \sum_{j=1}^m i_j = r$).

Lemma 6: Let $r_1, \dots, r_m \geq 0$, $0 < \varepsilon < 1$.
Then there are at most $(r_1+1)\cdots(r_m+1)\cdot e^{-\varepsilon^2 m/4}$ m-tuples of integers $(i_1, \dots, i_m)$, with $0 \leq i_k \leq r_k$, s.t.:

$$\frac{i_1}{r_1} + \cdots + \frac{i_m}{r_m} \leq \frac{m}{2} - \varepsilon \cdot m$$

Lemma (Siegel): Let $N > M \in \mathbb{N}$, and $A\vec{T} = 0$ be a system of M linear equations in N variables ($A \in M_{M\times N}(\mathbb{Z})$).
Let $|A|_\infty = |A| = \max\{|a_{ij}|\}_{i,j}$
Then there is a $\vec{t} \in \mathbb{Z}^N$, $A\cdot\vec{t} = 0$ and $|\vec{t}| \leq (N|A|_\infty)^{\frac{M}{N-M}}$

Pf $\#\{\vec{t} : |\vec{t}| \leq B\} = (2B+1)^N$

$|A\vec{t}| \leq N|A|\cdot|\vec{t}|$

$\#\{\vec{s} : |\vec{s}| \leq NAB\} = (2N|A|B+1)^M$

For $a \in \mathbb{R}$, let $a^+ = \max\{a, 0\}$, $a^- = \max\{-a, 0\}$ (so $a = a^+ - a^-$, $|a| = a^+ + a^-$).
Set $L_j = (a_{j1}, \dots, a_{jN})$, a linear form, $L_j^+ = \sum_i a_{ji}^+$, $L_j^- = \sum_i a_{ji}^-$
Then $\|L_j\| = L_j^+ + L_j^-$ (where $\|\cdot\|$ is the 1-norm).
Let $B \geq 0$. If $0 \leq t_i \leq B$ $\forall i$, then

$$-L_j^- B \leq L_j(\vec{t}) \leq L_j^+ B$$

We have $\#\{\vec{t} : 0 \leq t_i \leq B \ \forall i\} = (B+1)^N$, while
the image $A\cdot\{\vec{t} : 0 \leq t_i \leq B\} \subseteq \prod_{j=1}^{M} [-L_j^- B, L_j^+ B]$, hence has at most $\prod_{j=1}^{M} (\|L_j\|B + 1)$

If $(B+1)^N \geq \prod (\|L_j\| B + 1)$, then $\exists t_1, t_2$ s.t. $A(\vec{t_1} - \vec{t_2}) = 0$, $|\vec{t_1} - t_2| \leq B$.

(cont. pf of Siegel's lemma).

So just need to check that $(B+1)^N \geq \prod (\|L_j\| B+1)$, for

$B = \lfloor (N|A|)^{\frac{M}{N-M}} \rfloor$

Indeed, $(B+1)^{N-M} > (N|A|^{\frac{M}{N-M}})^{N-M} \Rightarrow (B+1)^{N-M} > (N|A|)^M \Rightarrow (B+1)^N \geq (N|A|B+1)$

$\geq \prod_{j=1}^{M} (\|L_j\| B+1)$ //

Prop 8:

Let α be an algebraic integer of degree d, $0 < \varepsilon < 1$,

and $m \geq 1$ s.t. $e^{\frac{\varepsilon^2 m}{16}} > 2d$.

Let $r_1, \dots, r_m \in \mathbb{N}$. Then $\exists\ P(x_1, \dots, x_m) \in \mathbb{Z}[\underline{x}]$ s.t.

a) $\deg_{x_i} P \leq r_i$ (write $\deg_{\underline{x}} P \leq \underline{r}$)

b) $\mathrm{Ind}_{\alpha, \underline{r}} \geq \frac{m}{2}(1-\varepsilon)$

c) $|P| \leq B(\alpha)^{r_1 + \dots + r_m}$ ($B(\alpha)$ only depends on α)

pf

Write $P(\underline{x}) = \sum_{0 \leq \underline{j} \leq \underline{r}} p_{\underline{j}} \underline{x}^{\underline{j}}$ $(\underline{x}^{\underline{j}} = x_1^{j_1} \cdots x_m^{j_m})$ $p_{\underline{j}} \in \mathbb{Z}$.

(there are $N = (r_1+1)\cdots(r_m+1)$ coefficients $p_{\underline{j}}$).

Let $\underline{i} = (i_1, \dots, i_m)$.

Then $\partial_{\underline{i}} P = \sum_{\underline{i} \leq \underline{j} \leq \underline{r}} p_{\underline{j}} \binom{\underline{j}}{\underline{i}} \underline{x}^{\underline{j}-\underline{i}}$ where $\binom{\underline{j}}{\underline{i}} = \binom{j_1}{i_1} \cdots \binom{j_m}{i_m}$.

(cont'd)

As in lemma 4, write $\alpha^\ell = a_1^{(\ell)}\alpha^{d-1} + \cdots + a_d^{(\ell)}$, and

evaluate $\partial_{\underline{i}} P(\underline{\alpha}) = \sum_{\underline{i} \le \underline{j} \le \underline{r}} p_{\underline{j}} \binom{\underline{j}}{\underline{i}} \alpha^{\|\underline{j}-\underline{i}\|} = \sum_{\underline{i} \le \underline{j} \le \underline{r}} p_{\underline{j}} \binom{\underline{j}}{\underline{i}} \left(\sum_{k=1}^{d} a_k^{(\|\underline{j}-\underline{i}\|)} \alpha^{d-k} \right) =$

$$= \sum_{k=1}^{d} \underbrace{\left[\sum_{\underline{i} \le \underline{j} \le \underline{r}} \binom{\underline{j}}{\underline{i}} a_k^{(\|\underline{j}-\underline{i}\|)} p_{\underline{j}} \right]}_{\text{inner terms}} \alpha^{d-k}.$$

This is 0 iff all the inner terms are 0 $\Rightarrow$ d linear-equations in the a_k's.

So, for each $\underline{i} \le \underline{r}$ we can set up d equations ensuring $\partial_{\underline{i}} P(\alpha) = 0$.

For (b) to hold, we need $\partial_{\underline{i}} P(\alpha) = 0 \quad \forall \underline{i}$ s.t. $\frac{i_1}{r_1} + \cdots + \frac{i_m}{r_m} < \frac{m}{2}(1-\varepsilon)$

$$= \frac{m}{2} - \frac{\varepsilon}{2} m$$

By Lemma 6, there are at most $(r_1+1)\cdots(r_{m+1}) e^{-\varepsilon^2 m/16}$ such $\underline{i}$.

By our choice of N, this means that we get at most $d \cdot \frac{N}{2d} = \frac{N}{2}$ such equations.

Note that the coeffs of the equations are bounded using Lemma 4:

$$\left| \binom{\underline{j}}{\underline{i}} a_k^{\|\underline{j}-\underline{i}\|} \right| \le 2^{\|\underline{j}\|} \left(|Q|+1\right)^{\|\underline{j}\|} = \left(2|Q|+2\right)^{\|\underline{j}\|} \le \left(2|Q|+2\right)^{\|\underline{r}\|},$$

where Q = min poly of α.

By Siegel's Lemma, $\exists$ $P(\underline{X})$ satisfying (a), (b), such that

$$|P| \le N \left(2|Q|+2\right)^{\|\underline{r}\| \frac{M}{N-M}} \le N \left(2|Q|+2\right)^{\|\underline{r}\|} = \quad \left(\text{because } M \le \tfrac{N}{2} \Rightarrow \tfrac{M}{N-M} \le 1\right)$$

$$= (r_1+1)\cdots(r_m+1)\left(2|Q|+2\right)^{\|\underline{r}\|} \le 2^{r_1} \cdots 2^{r_m} \left(2|Q|+2\right)^{\|\underline{r}\|}$$

$$= 2^{\|\underline{r}\|} \left(2|Q|+2\right)^{\|\underline{r}\|} = B(\alpha)^{\|\underline{r}\|} \quad \text{with } B(\alpha) = 4|Q|+4, \text{ giving (c)}$$

Lemma 11: Let $\underline{r} > \underline{0}$, $P \in \mathcal{O}_K[\underline{X}]$, $\deg P \leq \underline{r}$. Let $\theta = \mathrm{Ind}_{\underline{\alpha},\underline{r}}(P)$.

Let $0 < \delta \leq 1$, $0 < \theta_0 < \theta$. Let $S \subset M_K$ be a finite set of places.

Let $\xi : S \to [0,1]$ s.t. $\sum_{v} \xi_v = 1$, $\beta_1, \dots, \beta_m \in K$: $\|\beta_i - \alpha\|_v \leq \dfrac{r}{H_K(\beta_i)^{(2+\delta)\xi_v}}$ $(*)$

Set $D := \min \{ H_K(\beta_i)^{r_i} \}$, $\underline{j} = (j_1, \dots, j_m)$ such that

$$\sum_{i=1}^{m} \frac{j_i}{r_i} \leq \theta_0 \qquad \left(\text{write } \|\underline{j}/\underline{r}\| := \sum_{i=1}^{m} \frac{j_i}{r_i} \right).$$

Then: $$\prod_{v \in S} \|\partial_{\underline{j}} P(\underline{\beta})\|_v \leq \left(\delta H(\alpha)\right)^{[K:\mathbb{Q}]\|\underline{r}\|} \cdot H_K(P) \cdot D^{-(2+\delta)(\theta-\theta_0)}$$

Pf

Let $\underline{j}$ be as in the statement, and write $Q := \partial_{\underline{j}} P$.

We need to estimate $Q(\underline{\beta})$. Let $v \in M_K$, extended to $K(\alpha)$.

Then $$|\partial_{\underline{k}} Q(\underline{\alpha}^{(v,\alpha,\dots,\alpha)})| \leq 4 \max\{|\alpha|_v, 1\}^{\|\underline{r}\|} |P|_v \qquad (****)$$
(↑ if $v \in M_K^{\infty}$)

From Lemma 2, $\mathrm{Ind}_{\underline{\alpha},\underline{r}}(Q) = \mathrm{Ind}(\partial_{\underline{j}} P) \geq \mathrm{Ind}(P) - \|\underline{j}/\underline{r}\| \geq \theta - \theta_0$

So the Taylor expansion of Q at $\underline{\alpha}$ is

$$Q(\underline{X}) = \sum_{\substack{\underline{0} \leq \underline{i} \leq \underline{r} \\ \|\underline{i}/\underline{r}\| \geq \theta - \theta_0}} \partial_{\underline{i}} Q(\underline{\alpha}) (\underline{X} - \underline{\alpha})^{\underline{i}}$$

Setting $\underline{X} := \underline{\beta}$, using $(**)$ & $(****)$ we estimate: only at ∞-primes.

$$|Q(\beta)|_v \leq \sum_{\substack{\underline{0} \leq \underline{i} \leq \underline{r} \\ \|\underline{i}/\underline{r}\| \geq \theta - \theta_0}} |\partial_{\underline{i}} Q(\underline{\alpha})|_v \, |\underline{\beta} - \underline{\alpha}|_v^{\underline{i}} \leq \underbrace{(r_1+1)\cdots(r_m+1)}_{\text{only at } \infty \text{ primes}} \cdot \max_{\substack{\underline{0} \leq \underline{i} \leq \underline{r} \\ \|\underline{i}/\underline{r}\| \geq \theta - \theta_0}} \{ |\partial_{\underline{i}} Q(\underline{\alpha})| \} \cdot \max_{\|\underline{i}/\underline{r}\| \geq \theta - \theta_0} \{ |\underline{\beta} - \underline{\alpha}|_v^{\underline{i}} \}$$

$$\leq \delta^{\|\underline{r}\|} |P|_v \max\{|\alpha|_v, 1\}^{\|\underline{r}\|} \cdot \max_{\|\underline{i}/\underline{r}\| \geq \theta - \theta_0} \left\{ \frac{1}{\left(H_K(\underline{\beta})^{\underline{i}}\right)^{(2+\delta)\xi_v}} \right\}$$

Step 2: Bounding the index below.

Proposition 9: Let $0 < \delta < 1$, $0 < \varepsilon << \delta$ (*).

Suppose α is an alg. integer of degree d, and $m \in \mathbb{N}$ s.t. $e^{\varepsilon^2 m/16} > 2d$

Let $\underline{r} \geq \underline{1}$. Using Prop 8, choose a polynomial satisfying (a), (b), (c), say $P(X)$. Let $S \subseteq M_K$ be a finite set of valuations.

Let $\xi : S \to [0,1]$ s.t. $\sum_{v} \xi_v = 1$, $\beta_1, \dots, \beta_m \in K$

Such that $\|\beta_i - \alpha\|_v \leq \dfrac{1}{H_K(\beta_i)^{(2+\delta)\gamma_v}} \quad \forall v \in S$ (**).

In addition, suppose that $\max_i \{ H_K(\beta_i)^{r_i} \} \leq \min_i \{ H_K(\beta_i)^{r_i} \}^{1+\varepsilon}$ (***)

Then: $\exists\, C = C(\alpha, \delta)$ s.t. $\left[C \leq H_K(\beta_i) \ \forall i \right] \Rightarrow \left[\operatorname{ind}_{\underline{\beta}, \underline{r}}(P) \geq \varepsilon \cdot m \right]$

Lemma 10: Let $P \in \mathbb{Z}[\underline{X}]$ w/ $\deg P \leq \underline{r}$, and let $\underline{\beta} \in K^m$.

$\forall\, \underline{j} = (j_1, \dots, j_m) \geq \underline{0}$ we have: (we may write it as $\in$ on $H_K(\underline{\beta})^{\underline{r}}$)

$$H_K\left(\partial_{\underline{j}} P(\underline{\beta}) \right) \leq 4^{\|\underline{r}\|[K:\mathbb{Q}]} H_K(P) \cdot \prod_i H_K(\beta_i)^{r_i}.$$

Pf: $|\partial_{\underline{j}} P|_v \leq 2^{\|\underline{r}\|} |P|_v$ by Lemma 1, $\forall v \in M_K$.

Let $v \in M_K^{\infty}$. Then $|\partial_{\underline{j}} P(\underline{\beta})|_v \underset{\text{triangle ineq.}}{\leq} (r_1+1)\cdots(r_m+1) \cdot |\partial_{\underline{j}} P| \cdot \max\{|\beta_1|_v, 1\}^{r_1} \cdots \max\{|\beta_m|_v, 1\}^{r_m}$

$$\leq \underbrace{2^{\|\underline{r}\|} \cdot 2^{\|\underline{r}\|}}_{4^{\|\underline{r}\|}} \cdot |P| \cdot \max\{|\beta_1|_v, 1\}^{r_1} \cdots \max\{|\beta_m|_v, 1\}^{r_m}.$$

If $v \in M_K^{0}$, we get a similar bound, but without the factor of $4^{\|\underline{r}\|}$.

Taking the product over all v, we get the result,

(cont'd pf of Lemma 11)
To finish the proof, we need to estimate

$$\max_{\substack{\underline{i}\in\Gamma \\ \|\underline{i}/\Gamma\|\geq\theta-\theta_0}} \left\{ \frac{1}{\left(H_K(\underline{\beta})^{\underline{i}}\right)^{(2+\delta)\xi_v}} \right\} \leq \left(\frac{1}{D^{\theta-\theta_0}} \right)^{(2+\delta)\xi_v}.$$

Multiplying over all $v\in S$ and using $\sum \xi_v = 1$ we get the result.

Proof of Prop 9.

Let $\underline{i}$ be such that $\|\underline{i}/\Gamma\| \leq \varepsilon\cdot m$. We want to show that then $\partial_{\underline{i}} P(\underline{\beta}) = 0$

From Lemma 11, $\prod_{v\in S} \|\partial_{\underline{i}} P(\underline{\beta})\|_v \leq \left(\delta H(\alpha)\right)^{[K:\mathbb{Q}]\|\Gamma\|} \dfrac{M_K(P)}{D^{(2+\delta)(\theta-\theta_0)}}$

(with $\theta \geq \frac{m}{2}(1+\varepsilon)$, $\theta_0 \leq \varepsilon m$) $\Rightarrow \prod_{v\in S} \|\partial_{\underline{i}} P(\underline{\beta})\|_v \overset{(\S)}{\leq} \dfrac{\left(\delta \tilde{B}(\alpha)\right)^{\|\Gamma\|[K:\mathbb{Q}]}}{D^{\left(\left(\frac{m}{2}(1-\varepsilon)\right)-\varepsilon m\right)(2+\delta)}}$

($\tilde{B}(\alpha) = (\text{Const from Prop } 8)\cdot M(\alpha)$).

On the other hand, by Lemma 10,

$$(\S\S)\quad H_K\left(\partial_{\underline{i}} P(\underline{\beta})\right) \leq 4^{[K:\mathbb{Q}]\cdot\|\Gamma\|} M_K(P) \prod_i H_K(\beta_i)^{r_i} \overset{\text{assumption}}{\leq} \left(4B(\alpha)\right)^{\|\Gamma\|[K:\mathbb{Q}]} \cdot D^{m(1+\varepsilon)}$$

Now use Liouville's inequality (Lemma 3), so either $\partial_{\underline{i}} P(\underline{\beta}) = 0$ or

$$\prod_{v\in S} \|\partial_{\underline{i}} P(\underline{\beta})\|_v \geq \frac{1}{H_K(\partial_{\underline{i}} P(\underline{\beta}))} \qquad (\S\S\S)$$

Comparing $(\S)$ and $(\S\S)$, we get $\dfrac{\left(\delta B(\alpha)\right)^{\|\Gamma\|[K:\mathbb{Q}]}}{D^{\left[\frac{m}{2}(1-\varepsilon)-\varepsilon m\right](2+\delta)}} \geq \dfrac{1}{\left(4B(\alpha)\right)^{\|\Gamma\|[K:\mathbb{Q}]} D^{m(1+\varepsilon)}}$

or equivalently, $2^{\|\Gamma\|[K:\mathbb{Q}]} \left(4B(\alpha)\right)^{2\|\Gamma\|[K:\mathbb{Q}]} \geq D^{m\left[\left(1+\frac{\delta}{2}\right)(1-3\varepsilon)-(1+\varepsilon)\right]}$

If $\varepsilon << \delta$, the exponent on the RHS > 0. Making then $C >> 0$ leads to a contradiction. So $\partial_{\underline{i}} P(\underline{\beta}) = 0$ as desired.

Step 3: The index is small.

Def Let $f(\underline{X}) \in K[\underline{X}]$, $K/\mathbb{Q}$ a number field. The *affine height* of f over K is $H_K(f) := H_K([\text{1: coeffs of } f])$, $h_K(f) := \log H_K(f)$.

The *projective height* is $H_K^{pr}(f) = H_K([\text{coeffs of } f])$ if $f \neq 0$.

Lemma 12: Let $\mathcal{F} = \{f_1, \dots, f_n\} \subseteq K[\underbrace{\underline{X}}_{m \text{ variables}}]$. Let $H_K(\mathcal{F}) := \max\{H_K(f_i)\}$.

Let $\deg f_i :=$ total degree of f_i.

a) $h(f_1 \cdots f_n) \leq \sum_{i=1}^{n} [h(f_i) + (\deg f_i + m)\log 2]$

b) $h(f_1 + \cdots + f_n) \leq \sum_{i=1}^{n} h(f_i) + \log n$.

c) Suppose that $f_i \in \mathcal{O}_K(\underline{X})$ $\forall i$. Then

$h(f_1 + \cdots + f_n) \leq [K:\mathbb{Q}] \cdot h(\mathcal{F}) + \log n$.

Lemma 13 (Gelfand's Inequality): Let $d_1, \dots, d_m \in \mathbb{Z}$, $f_1, \dots, f_n \in \bar{\mathbb{Q}}[\underline{X}]$ s.t.

$\deg_{X_i}(f_1 \cdots f_n) \leq d_i$ $\forall i$.

Then, $\sum_{i=1}^{n} h^{pr}(f_i) \leq h^{pr}(f_1 \cdots f_n) + \sum_{i=1}^{n} d_i$

Prop 14 (Roth's Lemma): Let $m \geq 1$, $P \in \bar{\mathbb{Q}}[X_1, \dots, X_m]$, s.t. $\deg P \leq r$

Let $\underline{\beta} = (\beta_1, \dots, \beta_m) \in \bar{\mathbb{Q}}^m$. Fix $\eta > 0$ s.t

i) $\frac{r_{i+1}}{r_i} \leq \eta^{2^{m-1}}$ $\forall i = 1 \dots m-1$ ← degrees get smaller fast

ii) $\eta^{2^{m-1}} \cdot \min_{1 \leq i \leq m} \{r_i \log H(\beta_i)\} \geq \log H(P) + 2mr_i$ ← $H(\beta_i)$ gets longer fast.

Then $\mathrm{Ind}_{\underline{\beta}, \underline{r}}(P) \leq 2m\eta$

Proof: We work by induction on m. Suppose that all β_i and P are defined over k, with $[k:\mathbb{Q}]=d$.

(A) Case $m=1$: Write $\beta=\beta_1$, $r=r_1$.

Let ℓ be the exact degree of vanishing at $P(X)$ at β, so that

$\mathrm{Ind}_\beta(P)=\frac{\ell}{r}$. So $\quad P(X)=(X-\beta)^\ell\cdot Q(X), \quad Q(\beta)\neq 0$.

Using Lemma 13, we estimate:

$$H(\beta)^{r\cdot \mathrm{Ind}\,P}=H(\beta)^\ell=H^{pr}\big((X-\beta)\big)^\ell \le H^{pr}\big((X-\beta)\big)^\ell H^{pr}(Q(x)) \le$$

(Gelfond: Dneg)

$$\le H^{pr}\Big((X-\beta)^\ell Q(X)\Big)\,e^r \le H(P)\,e^r$$

(the proj. height is $\le$ than the affine height)

So that $\quad \mathrm{Ind}\,P \le \dfrac{\log H(P)+r}{r\log H(\beta)} \le 2^{\le 2n}$ by (ii)

Note: The bound we've found is 2^n (instead of 2^k), and instead of (ii) we used $2r\log H(\beta)\ge \log H(P)+r$ ← instead of $2r$.

(B) Induction Step: We need to factor $P(\underline{X})$

Def: Let $f_1,\dots,f_n\in K(X_1,\dots,X_m)$. A generalized Wronski determinant of $(f_1,\dots,f_n)$ is a function $F:=\det\big[\Delta_i f_j\big]_{1\le i,j\le n}$

where Δ_i is a linear differential of order $\le i-1$

(take it to be monomial)

Lemma 15: $(f_1,\dots,f_n)$ are l.i over K $\Leftrightarrow$ there exists a generalized Wronski determinant s.t. $\det(\Delta_i f_j)\neq 0$.

$\Rightarrow$ If $f_1,\dots,f_n$ are linearly dependent, then the columns of the Wronski det are l.dep. $\Rightarrow 0$.

↓

(cont'd of Lemma 15)

$\Rightarrow$] Suppose $\lambda \neq 0$ in $K(\underline{X})$. Then $\{f_1, \dots, f_n\}$ l.i. $\Leftrightarrow$ $\{\lambda f_1, \dots, \lambda f_n\}$ l.i.

Also, $W(f_1, \dots, f_n) \neq 0 \Leftrightarrow \exists W'$ s.t. $W'(\lambda f_1, \dots, \lambda f_n) \neq 0$.

In particular, we may assume $f_1 = 1$.

We use induction on n, and note $n=1$ is trivial.

Suppose the assertion true for all sets of functions w/ $1 \leq k < n$ elements.

Let $V = K\langle f_1, \dots, f_n \rangle$, an n-dim vectorspace $\subseteq K(\underline{X})$.

Claim: If V has any basis $\psi_1, \dots, \psi_n$ having a nonzero wronskian, then $W(f_1, \dots, f_n) \neq 0$ (as $\{f_1, \dots, f_n\}$ is another basis). $\leftarrow$ easy!

We may assume wlog that $\frac{\partial f_2}{\partial x_1} \neq 0$. Let $U = \{f \in V : \frac{\partial f}{\partial x_1} = 0\} \subseteq V$.

Then $(0) \subsetneq U \subsetneq V$.

Choose a basis $\{\psi_1, \dots, \psi_k\}$ of U, and extend it w/ $\psi_{k+1}, \dots, \psi_n$ to a basis of V.

Note that $\{\frac{\partial \psi_{k+1}}{\partial x_1}, \dots, \frac{\partial \psi_n}{\partial x_1}\}$ is l.i. over K.

By induction, $\exists$

(a) $\Delta_1^*, \dots, \Delta_k^*$ w/ $\operatorname{ord}(\Delta_i^*) \leq i-1$

s.t. $W_1(\psi_1, \dots, \psi_k) = \det(\overbrace{\Delta_i^* \psi_j}^{W_1}) \neq 0$

(b) $\Delta_{k+1}^*, \dots, \Delta_n^*$ w/ $\operatorname{ord}(\Delta_i^*) \leq i-k-1$ s.t.

$$\det\left(\overbrace{\Delta_i^* \frac{\partial}{\partial x_1} \psi_j}^{W_2}\right)_{k+1 \leq i,j \leq n} \neq 0$$

Let now $\Delta_i = \begin{cases} \Delta_i^* & 1 \leq i \leq k \\ \Delta_i^* \frac{\partial}{\partial x_1} & k+1 \leq i \leq n \end{cases}$ $\leftarrow$ note that $\operatorname{ord}(\Delta_i) \leq i-1$

So $\Delta_i \psi_j = 0$ if $i \geq k+1, j \leq k$. Hence $\left|(\Delta_i \psi_j)_{1 \leq i,j \leq n}\right| = \left|\begin{bmatrix} W_1 & * \\ 0 & W_2 \end{bmatrix}\right| \neq 0$

Back to the proof of Roth's lemma,

Let $m>1$ and assume it true for $<m$ variables.

Write $P(X_1,\dots,X_m)=\sum_{j=1}^{k}\Phi_j(X_1,\dots,X_{m-1})\Psi_j(X_m)$ (so viewed in $K[X_1,\dots,X_{m-1}][X_m]$)

Do it in such a way such that k is minimal. Note $k\le r_m+1$

Claim: $\{\Phi_1,\dots,\Phi_k\}$ is K-linearly independent, as is $\{\Psi_1,\dots,\Psi_k\}$.

Pf Suppose $\Phi_k=\sum_{i=1}^{k-1}a_i\Phi_i$, $a_i\in K$. Then $P=\sum_{j=1}^{k-1}\Phi_j\Psi_j+\sum_{i=1}^{k-1}a_i\Phi_i=\sum_{j=1}^{k-1}\Phi_j\underbrace{(\Psi_j+a_j\Psi_k)}_{\widetilde{\Psi}_j}\Rightarrow!!$ minimal k!

Similarly for $\{\Psi_j\}_j$

Let now $U(X_m)=\det\left(\partial_{(0,0,\dots,i-1)}\Psi_j(X_m)\right)_{1\le i,j\le k}$ ← the classical Wronskian $\neq 0$ because $\{\Psi_j\}$ is l.i.

Also, by Lemma 15 $\exists\ \Delta_i'=\partial_{\underline{s}_i}$ w/ $\|\underline{s}_i\|\le i-1$ such that

$$V(X_1,\dots,X_{m-1})=\det\left(\Delta_i'\Phi_j\right)_{1\le i,j\le k}$$

Now define $W(X_1,\dots,X_m):=\det\left(\Delta_i'\partial_{(0,\dots,j-1)}P\right)_{1\le i,j\le k}$

Note that $W(X_1,\dots,X_m)=\det\left(\left[\Delta_i'\partial_{(a_0,\dots,j-1)}\right]\sum_{t=1}^{k}\phi_t\Psi_t\right)_{1\le i\le k}=$

$$=\det\left(\sum_{t=1}^{k}\Delta_i'\Phi_t\cdot\partial_{(0,\dots,0,j-1)}\Psi_t\right)_{1\le i,j\le k}=\det\left(\Delta_i'\Phi_t\right)_{1\le i,t\le k}\cdot\det\left(\partial_{(0,\dots,j-1)}\Psi_t\right)_{j,t}$$

$$=V\cdot U.\ \left(=V(X_1,\dots,X_{m-1})\cdot U(X_m)\right).$$

To perform the induction we will:

(C) → Use induction hypothesis to bound $\mathrm{Ind}(U)$, $\mathrm{Ind}(V)$, $\mathrm{Ind}(W)$ (above)

(D) → Bound the order of W below in terms of $\mathrm{Ind}(P)$.

To do ©, we may assume $\eta \le \frac{1}{2}$, otherwise the conclusion is trivial.

Note that $h(W) = h(U \cdot V) \le h(U) + h(V)$
(↑ disjoint sets of variables.)

Claim: (a) $\deg_{X_m} U \le k r_m$, $\deg_{X_j} V \le k r_j$, $j \le m-1$.

(b) $h(W) = h(U) + h(V) \le k\left(h(P) + 2r_1\right)$

Pf (a) is clear.

(b) W being a determinant is a sum of $k!$ terms, each being a product of k polynomials of deg $\le \underline{r}$, satisfying:

$$H\left(\Delta_i' \circ_{(0,\dots,\delta)} P\right) \le 2^{\|\underline{r}\|} H(P)$$

By Lemma 12 (B7.2 in book) we conclude

$$h(W) \le k\cdot\left(h(P) + \|\underline{r}\| \log 2\right) + \log(k!)$$

Now $\|\underline{r}\| \le r_1\left(1 + \eta' + \eta'^{(2)} + \eta'^{(m-1)}\right)$ where $\eta' := \eta^{2^{m-1}}$ (by (i))

Since $\eta \le \frac{1}{2}$, then $\eta' \le \frac{1}{4}$ $(m \ge 2)$. $\Rightarrow \|\underline{r}\| \le \frac{4}{3} r_1$.

Also, $\frac{\log(k!)}{k} \le \log k \le k-1 \le r_m \le \frac{1}{2} r_1$. So

$$h(W) \le k\left(h(P) + \underbrace{\left(\frac{4}{3}\log 2 + \frac{1}{2}\right)}_{c_1 \approx 1.424 < 2} r_1\right) \le k\left(h(P) + 2r_1\right)$$

Now, for (D): Claim: that $\mathrm{Ind}_{\beta_m, r_m}(U) \le k\eta^{2^{m-1}}$, $\mathrm{Ind}_{(\beta_1,\dots,\beta_{m-1}),(r_1,\dots,r_{m-1})}(V) \le 2k(m-1)\eta^2$.

So $\overline{\mathrm{Ind}}_{\underline{\beta},\underline{r}}(W) \le 2k(m-1)\eta^2 + k\eta^{2^{m-1}}$)

Proof (of claim): Let $\underline{r}' := k\cdot(r_1,\dots,r_{m-1})$, $\eta' := \eta^2$, $m' := m-1$. We need to check:

a) $\deg V \le \underline{r}'$ (by Claim (a)).

i) $\frac{r_{i+1}'}{r_i'} \le \eta'^{2^{m'-1}}$ but LHS $= \frac{r_{i+1}}{r_i}$, and RHS $= \eta^{2^{m-1}}$, so it's hypothesis (i).

ii) $\eta'^{2^{m'-1}} \cdot \min_{1 \le i \le m-1}\left\{r_i' \log H(\beta_i)\right\} \ge \log H(V) + 2m' r_1'$. ↘

To check (ii), we do:

$$\eta'^{2^{m-1}} \cdot \min_{1\le i\le m-1}\{r_i' \log H(\beta_i)\} \gtrsim \eta^{2^{m-1}} \cdot k \cdot \min_{1\le i\le m}\{r_i \log H(\beta_i)\} \overset{(ii)}{\gtrsim} k\left(\log H(P) + 2m r_1\right) \gtrsim$$

$$\gtrsim k\cdot \log H(P) + 2kr_1 + 2m' \underbrace{k r_1}_{r_1'} \gtrsim \log H(V) + 2m' r_1'.$$

This gives the ~~first~~ second inequality (i.e. for V).

For U, we use the stronger version of Roth's thm ($m=1$), with

$\eta'' := \eta^{2^{m-1}}$, $r_m'' = k r_m$, $m'' = 1$.

Again, (i) $\deg_{x_m} U \le r_m''$

(ii) empty condition.

(iii) $\eta''^{r_m''} \log H(\beta_m) \overset{?}{\gtrsim} \log H(U) + r_m''$

To check (iii), note:

$$k\cdot \eta^{2^{m-1} r_m} \log H(\beta_m) \overset{(ii)}{\gtrsim} k\left(\log H(P) + 2m r_1\right) \gtrsim k\cdot\left(\log H(P) + 2r_1\right) + 2(m-1)k r_1 \gtrsim$$

$$\gtrsim \log H(V) + 2k r_m \gtrsim \log H(U) + r_m''$$

(claim(s) $m>1$) // (ends ⓒ)

Part Ⓓ: (need to bound below the index of W in terms of that of P)

Claim D.1: $\mathrm{Ind}_{\underline{\beta},\underline{r}} W \gtrsim \frac{\kappa}{2} \min\{\mathrm{Ind}(P), \mathrm{Ind}(P)^2\} - k\frac{r_m}{r_{m-1}}$.

Once we prove the claim we can finish the proof of Roth's Lemma, by:

$$\left(\mathrm{Ind}_{\underline{\beta},\underline{r}}(P)\right)^2 \underset{\mathrm{Ind}(P)\le m}{\le} m \cdot \min\{\mathrm{Ind}(P), \mathrm{Ind}(P)^2\} \underset{\text{D.1.}}{\lesssim} \frac{2m}{\kappa}\mathrm{Ind}(W) + 2m\frac{r_m}{r_{m-1}} \underset{\text{C.Z.}}{\lesssim}$$

$$\lesssim 4m(m-1)\eta^2 + 2m\eta^{2^{m-1}} + 2m\frac{r_m}{r_{m-1}} \overset{(i)}{\lesssim} 4m^2\eta^2 + 4m\eta^{2^{m-1}} - 4m\eta^2 \le 4m^2\eta^2 \Rightarrow //$$

Proof of Claim D.1:

Recall that $W = \det\left(\partial_{(i_1^{(s)},\dots,i_{m-1}^{(s)},j-1)} P\right)_{1\le s,j\le k}$ for $\|\underline{i}^{(s)}\| \le s-1$.

↓

Now, estimate:

1) $\mathrm{Ind}\left(\mathcal{O}_{(i^{(s)},j-1)}P\right) \geq \mathrm{Ind}(P) - \frac{(i^{(s)},j-1)}{r} \geq \mathrm{Ind}(P) - \frac{\|i^{(s)}\|}{r_{m-1}} - \frac{j-1}{r_m} \geq$ ($r_{i-1} \geq r_m$; $\|i^{(s)}\| \leq s-1 \leq k-1 \leq r_m$)

$\geq \mathrm{Ind}(P) - \frac{r_m}{r_{m-1}} - \frac{j-1}{r_m}$

2) W = sum of $k!$ summands, each of which is a product of k terms with one factor as in (1), for each $1 \leq j \leq k$.

Therefore, $\mathrm{Ind}(W) \geq \mathrm{Ind}(\Sigma)$ $\min\left\{\mathrm{Ind}\left(\text{product of } k\text{-terms as in (1) for each } 1\leq j\leq k\right)\right\} \geq$

$\geq \mathrm{Ind}(\Pi) \sum_{j=1}^{k} \max\left\{\mathrm{Ind}P - \frac{r_m}{r_{m-1}} - \frac{j-1}{r_m}, 0\right\} \geq \sum_{j=1}^{k} \max\left\{\mathrm{Ind}P - \frac{j-1}{r_m}, 0\right\} - \frac{k r_m}{r_{m-1}}$

Let $LHS := \sum_{j=1}^{k} \max\left\{\mathrm{Ind}P - \frac{j-1}{r_m}, 0\right\} \geq \frac{k}{2}\min\left\{\mathrm{Ind}P, (\mathrm{Ind}P)^2\right\}$

Case 1: $\mathrm{Ind}P \geq \frac{k-1}{r_m}$.

Then $LHS = \sum_{j=1}^{k} \mathrm{Ind}P - \frac{j-1}{r_m} = k\,\mathrm{Ind}P - \frac{k(k-1)}{2r_m} \geq \frac{k}{2}\mathrm{Ind}P$ ✓ (because $\mathrm{Ind}P \geq \frac{k-1}{r_m}$)

Case 2: $\mathrm{Ind}P < \frac{k-1}{r_m} \leq 1$, and $k \leq r_m$

Let $N := \lfloor r_m \mathrm{Ind}P \rfloor$; then $N+1 < k$, and $LHS = \sum_{j=1}^{N+1}\left(\mathrm{Ind}P - \frac{j-1}{r_m}\right) =$

$= (N+1)\mathrm{Ind}P - \frac{N(N+1)}{2r_m} = (N+1)\left(\mathrm{Ind}P - \frac{\lfloor r_m \mathrm{Ind}P\rfloor}{2r_m}\right) \geq (N+1)\mathrm{Ind}P \cdot \frac{1}{2}\mathrm{Ind}P$

$\geq \frac{1}{2} r_m (\mathrm{Ind}P)^2 \geq \frac{k}{2}\mathrm{Ind}(P)^2$. ✓

Case 3: $k = r_m + 1$.

$LHS \overset{\text{case 2}}{\geq} (N+1)\mathrm{Ind}P - \frac{N(N+1)}{2(k-1)} =: q(N)$

Since $(k-1)\mathrm{Ind}P - 1 \leq N \leq (k-1)\mathrm{Ind}P$, then $q(N) \geq \min\left\{q\left((k-1)\mathrm{Ind}P\right), q\left((k-1)\mathrm{Ind}P - 1\right)\right\}$ (both more equal)

$= (k-1)(\mathrm{Ind}P)^2 - \frac{1}{2}(k-1)(\mathrm{Ind}P)^2 + \frac{1}{2}\mathrm{Ind}P = \frac{(k-1)(\mathrm{Ind}P)^2 + \mathrm{Ind}P}{2} \geq \frac{k}{2}(\mathrm{Ind}P)^2$. ✓ ($\mathrm{Ind}P \leq 1$)

(BOTH).

Now, with Roth's lemma we can go on with the proof of Roth's Theorem.

Thm: Let K be a # field, $\alpha \in \bar{K}$, $S \subseteq M_K$, $\delta > 0$, $\xi : S \to [0,1]$ s.t. $\sum_v \xi_v = 1$

Then there are only finitely-many $\beta \in K$ s.t.

$$\|\beta - \alpha\|_v \leq \frac{1}{H_K(\beta)^{(2+\delta)\xi_v}} \quad \forall v \in S \qquad (**)$$

Pf

Step 1
- (1) $e^{\varepsilon^2 m/16} > 2d$ (where $d = \deg(\alpha)$).
- (2) $\mathrm{Ind}_{\underline{\alpha}, \underline{\xi}}(\underline{P}) \geq \frac{m}{2}(1-\varepsilon)$ $\deg P \leq \underline{r}$
- (3) $|P| = H(P) \leq B(\alpha)^{\|r\|}$

Step 2
- (4) $0 < \varepsilon << \delta$ (how small ε depends only on δ).
- (5) $\|\beta_i - \alpha\|_v \leq \frac{1}{H_k(\beta_i)^{(2+\delta)\xi_v}} \quad \forall v, \ \forall i \in \{1 \dots m\}$
- (6) $D := \min\{H(\beta_i)^{r_i}\} \leq \max\{H(\beta_i)^{r_i}\} \leq D^{1+\varepsilon}$
- (7) $H(\beta_i) \geq C(\alpha, \delta) \ \forall i$

Step 3
- (8) $r_{i+1} \leq \eta^{2^{m-1}} r_i$
- (9) $\log H(P) + 2m r_1 \leq \eta^{2^{m-1}} \log D$

We are going to choose, in that order, $\varepsilon, m, \eta, \underline{\beta}, \underline{r}, P(\underline{X})$, assuming the existence of only many approximations β.

a) Choose $\varepsilon << \delta$ s.t. (4) is satisfied.

b) Choose m s.t. (1) holds.

c) Set $\eta := \frac{\varepsilon}{16}$, note that $2\eta < \varepsilon$

d) Choose β_1 s.t. $H(\beta_1) > C(\alpha, \delta)$ and $\log H(\beta_1) \geq \frac{m(\log B(\alpha) + 2)}{\eta^{2^{m-1}}}$ and $(**)$ is satisfied.

So (7) is now satisfied for β_1

e) Choose $\beta_2, \dots \beta_m$ so that $\eta^{2^{m-1}} \log H(\beta_{i+1}) \geq 2 \log H(\beta_i)$ and $(**)$.

Note how that (7) is completely satisfied.

f) Choose r_1 s.t. $r_1 \eta^{2^{m-1}} \log H(\beta_1) \geq 2 \log H(\beta_m)$ (or $r_1 >> 0$).

(Choose r_1 large enough so that (6) is satisfied).

g) We can now choose $r_2, \dots, r_m$ s.t (6) and (8) hold, and s.t $D = H(\beta_1)^{r_1}$

h) Props 8 & 9 (step 1 & Step 2) allow us to choose $P(X_1, \dots, X_n)$ s.t (2) & (3) hold, and $\mathrm{Ind}_{\underline{\beta}, \underline{r}} P \geq \varepsilon^{[m]}$.

We want to apply Roth's lemma. So we need to make sure that (9) is satisfied.

In that case, $\mathrm{Ind}_{\underline{\beta}, \underline{r}}(P) \leq 2\eta^m \overset{(c)}{<} \varepsilon^m \Rightarrow !!$

Because of (8), we need to check that

$$\eta^{2^{m-1}} r_1 \log H(\beta_1) \geq \log H(P) + 2mr_1$$

Note that $P \in \mathbb{Z}[\underline{X}]$, so $H(P) = |P|$. We estimate:

$$\log H(P) + 2mr_1 \underset{(3)}{\leq} \|\Sigma\| \log B(\alpha) + 2mr_1 \leq mr_1 \log B(\alpha) + 2mr_1 = mr_1 (\log B(\alpha) + 2)$$

Looking at how we choose (d), this is $\leq \eta^{2^{m-1}} r_1 \log H(\beta_1)$

Roth's Thm.

Applications:

Theorem 1: Let K be a number field, $S \subseteq M_K$ finite set of places containing M_K^∞.

Let $R_S := \mathcal{O}_K[S^{-1}]$ $\left(R_S = \{x \in K : |x|_v \leq 1 \ \forall v \notin S\}\right)$.

Then the equation $U + V = 1$ has only finitely-many solutions $U, V \in R_S^\times$

Pf Let $s := |S|$, $m >> s$ (i.e. $m > 2^s$). The group $R_S^\times / (R_S^\times)^m$ is finite.

(because $R_S^\times$ is finitely-generated abelian).

Fix a set A of coset representatives in $R_S^\times$.

Let $T := \{(U,V) : U+V=1\} \longrightarrow A \times A$

$$(U,V) \longmapsto (a,b)$$

where $U = aX^m$, $V = bY^m$, $a,b \in A$, $X,Y \in R_S^\times$.

If we had only many solutions, then $\exists\, a,b \in A$ s.t.

$aX^m + bY^m = 1$ has only many solutions in $X,Y \in R_S^\times$.

Since S is finite, $\exists\, w \in S$ s.t.

$\{(x,y) : ax^m + by^m = 1$ and $\|Y\|_w \geq \|Y\|_v \ \forall v \in S\}$ is infinite.

Fix $\alpha \in \bar{K}$ s.t. $\alpha^m = -\frac{b}{a}$. Then $\frac{1}{aY^m} = \frac{X^m}{Y^m} + \frac{b}{a} = \frac{X^m}{Y^m} - \alpha^m =$

$$= \prod_{\zeta \in \mu_m} \left(\frac{X}{Y} - \zeta\alpha\right)$$

There is a constant $C = C(K,S,m) > 0$ s.t.

$$\frac{1}{\|Y\|_w^m} \geq C \min_{\zeta} \left\| \frac{X}{Y} - \zeta\alpha \right\|_w \qquad (*)$$

A priori, C depends on a,b, but we can take $C = \min_{(a,b) \in A \times A_*\text{ finite}} C_{a,b}$.

As there are finitely many $\zeta \in \mu_n$, $\exists\, \zeta$ s.t. $\min \left\| \frac{X}{Y} - \zeta\alpha \right\|_w = \left\| \frac{X}{Y} - \zeta\alpha \right\|_w$ for only many (X,Y).

So for only many X,Y,

$$\frac{1}{\|Y\|_w^m} \geq C \left\| \frac{X}{Y} - \zeta\alpha \right\|_w .$$

Now $\|Y\|_w = \max_{v \in S} \|Y\|_v \geq \left[\prod_{v \in S} \|Y\|_v\right]^{\frac{1}{s}} \overset{Y \in R_S^\times}{=} \left[\prod_{v \in M_K} \|Y\|_v\right]^{1/s} = H_K(Y)^{\frac{1}{s}}$

Hence we can estimate

$$H_K\left(\frac{X^m}{Y^m}\right) = H_K\left(\frac{1}{aY^m} - \frac{b}{a}\right) \leq 2^{[K:\mathbb{Q}]} H_K\left(\frac{1}{aY^m}\right) H_K\left(\frac{1}{a}\right) \leq \tilde{C}\, H_K\left(\frac{1}{Y^m}\right)$$

($H(x+y) \leq 2H(x)H(y)$ for canonical height, otw we have this other bound)

($\tilde{C}$ depends on K,S,m)

That is, $\exists C'>0$ s.t $M_k\left(\frac{x}{y}\right) \le C' H_k(y)$

↑ taking m^{th} roots.

Setting $C'' := (C')^{-\frac{1}{s}}$, we get $C'' H_k\left(\frac{x}{y}\right)^{\frac{1}{s}} \le \|y\|_w$.

Combined with (*), we get that there are only many x, y s.t.

$$\left\| \frac{x}{y} - \zeta\alpha \right\|_w \le \frac{C'''}{H_k\left(\frac{x}{y}\right)^{n/s}}$$. Since $n > 2s$ this contradicts Roth's Theorem.

Theorem 2: $K/\mathbb{Q}$ a number field, C/K a smooth projective curve of genus $g \ge 1$.

Let $S \subseteq M_K$ finite, $f \in K(C)$

Then $\{x \in C(K) : f(x) \in R_S$ is finite$\}$.

Proof: Let $s := \#S$.

Prop 2.1: Let $e = e(f)$ be the maximal order of any zero of f., $\varepsilon > 0$,

and let $t \in C(K)$ regular and non-zero at all zeros and poles of f. (and unramified)

(i.e. if Q is a zero or pole of f, then $(t - t(Q))$ is a local parameter at Q)

Then: $\exists c = c(f, t, C, \varepsilon, S)$ s.t

$$\prod_{v \in S} \min\{\|f(P)\|_v, 1\} \ge \frac{c}{H_k(t(P))^{(2+\varepsilon)se}} \qquad \forall P \in C(K) \text{ s.t } f(P) \in R_S \setminus \{0\}$$

(wouldn't matter for the statement)

Proof: write $\mathrm{div}(f)_\infty (f) = e_1 Q_1 + \cdots + e_r Q_r - E$, $e_i > 0$, $E \ge 0$.

The proof is by contradiction.

So suppose we have a sequence $(P_n)_{n \in \mathbb{N}}$ s.t $f(P_n) \in R_S$

and $\lim_{n \to \infty} \left[H_K(t(P))^{(2+\varepsilon)se} \prod_{v \in S} \min\{\|f(P)\|_v, 1\} \right] = 0$

Prop 2.2 (Strengthening): As above, but now assume $g \geq 1$, and let $\delta > 0$.

Then $\exists\, C = C(f, t, C, \delta, S) > 0$ s.t.

$$\prod_{v \notin S} \min\{\|f(P)\|_v, 1\} \geq \frac{C}{H_K(t(P))^{\delta}} \quad \forall P \in C(K) : f(P) \in R_S \setminus \{0\}.$$

Proof: By contradiction.

We'll reduce to 2.1 by:

- Find $\Phi : C' \to C$ unramified, such that $e(f \circ \Phi) = e(f)$. For this, we use that $g \geq 1$.
- Find a corresponding $f' \in K(C')$, and bound $H_K(t'(P'))$ in terms of $H_K(t(P))^{\frac{1}{\deg \Phi}}$ (for $\Phi(P') = P$, and $P' \in C'(K)$).

Making $\deg \Phi >> 0$, we will get the result.

So fix $C > 0$. Suppose there is $(P_n)_{n \in \mathbb{N}} \subseteq C(K)$, $f(P_n) \in R_S$ s.t.

$$H_K(t(P_n))^{\delta} \prod_{v} \min\{\|f(P_n)\|_v, 1\} \leq C \quad \forall n.$$

Embed $C \hookrightarrow J = J(C)$. Since $J(K)/mJ(K)$ is finite (weak M-W), by replacing (P_n) by a subsequence we may assume that

$$P_n \equiv P_k \bmod mJ(K) \quad \forall n, \forall k. \quad \text{i.e. } \exists\, (P_n') \in J(K),\ R \in J(K)$$

s.t. $P_n = mP_n' + R$ $(\forall n)$.

Let $\Phi : J \to J$, $a \mapsto ma + R$.

$$\begin{array}{ccc} C' & \xrightarrow{i'} & J \\ \downarrow \Phi & \circlearrowleft & \downarrow \Phi \\ C & \xrightarrow{i} & J \end{array}.$$

The obtained map $\Phi : C' \to C$ is unramified (because $J \to J$ is étale).

The term in the limit is $\geq H_K(f(P))^{(2+\varepsilon)se} \cdot \min_{v\in S}\{\|f(P_n)\|_v, 1\}^s$.

So this converges also to 0, and so it does its sth root. Hence

$$\lim_{n\to\infty} H_K(f(P))^{(2+\varepsilon)e} \min_{v\in S}\{\|f(P)\|_v, 1\} = 0.$$

Replacing $(P_n)_n$ by a subsequence (we call it $(P_n)_n$ anyway), and noting that $H_K(f(P)) \to \infty$ (because finite points of $\mathbb{P}^1$ of bounded height), we have that $\exists w \in S$ s.t. $H_K(f(P_n))^{(2+\varepsilon)e} \|f(P_n)\|_w \to 0$.

$\left(\Rightarrow \|f(P_n)\|_w \to 0\right)$.

$C(K_w)$ can be endowed with an analytic topology (like $C(\mathbb{C})$).

As f is rational, it defines a continuous function $f_w : C(K_w) \to K_w$.

As f has finitely-many zeros, $\exists Q_j$ (one of them) s.t. a subsequence of the P_n is s.t. ~~$f(P_n) \to 0$~~ $P_n \to Q_j$.

Recall that $t - t(Q_j)$ is a uniformizer at Q_j, and

$(t - t(Q_j))^{-e_j} f$ has no zero/pole at Q_j.

Hence $\exists\ 0 < C_1 < C_2$ s.t. $C_1 \leq \|(t(P_n) - t(Q_j))^{-e_j} f(P_n)\|_w \leq C_2$ $(n \gg 0)$.

As $e \geq e_j$, $\lim_{n\to\infty} H_K(t(P_n))^{(2+\varepsilon)e} \|(t(P_n) - t(Q_j))^e\|_w = 0$

Taking e^{th} roots, get $\lim_{n\to\infty} H_K(t(P_n))^{(2+\varepsilon)} \|t(P_n) - t(Q_j)\|_w = 0$

That is, $t(P_n) \in K$ approximate $t(Q_j) \in \overline{K}$ well in the sense of Roth's thm.

which is a contradiction. //

(cont pf 2.2)

Choose a very ample symmetric D on $\mathcal{J}$, and let $t: C \to \mathbb{P}^1$ s.t. $t': C \to \mathbb{P}^1$

(i) $t^{-1}(\infty) \sim j^*(D)$, $t'^{-1}(\infty) \sim j'^*(D)$.

(ii) $|(t)| \cap |(f)| = \phi$, t is unramified at (f)

$|(t')| \cap |(f \circ \Phi)| = \phi$, t' is unramified at $(f \circ \Phi)$.

So for $P \in C(\bar{K})$, $P' \in C'(\bar{K})$ we have:

$$h(t(P)) = \hat{h}_{\mathcal{J},D}(j(P)) + O(1)$$

$$h(t'(P')) = \hat{h}_{\mathcal{J},D}(j'(P')) + O(1)$$

$$\Rightarrow h(t \circ \Phi(P')) = \frac{m^2}{2} h(t'(P')) + O(m^2)$$

$$\Rightarrow H_K(t(P_n)) \geq \kappa_m H_K(t'(P_{n'}))^{\frac{m^2}{2}}$$ (κ_m some constant depending on m)

(κ_m dep on m, not on n).

$$\text{So } c \geq H_K(t(P_n))^{\rho} \prod_v \min\{\|f(P_n)\|_v, 1\} \geq \kappa_m H_K(t'(P_{n'}))^{\rho \frac{m^2}{2}} \prod_{v \in S} \min\{\|f(\Phi(P_{n'}))\|_v, 1\}$$

$$\geq \kappa_m H_K(t'(P_{n'}))^{\rho m^2/2} \cdot c' \cdot H_K(t'(P_{n'}))^{-(2+\varepsilon) s e(f \circ \Phi)}$$

for $\varepsilon > 0$ (some $c' \geq 0$) by prop 2.1.

Since $e(f \circ \Phi) = e$, $\exists\, c''$ (indep of n) s.t.

$$c'' \geq H_K(t'(P_{n'}))^{\rho \frac{m^2}{2} - (2+\varepsilon) s e}$$

As the height goes to ∞ and c'' does not depend on n, the exponent is ≤ 0.

So $\frac{\rho m^2}{2} \leq (2+\varepsilon) s e \quad \forall m > 0 \Rightarrow !!$

Proof of Thm 2: Assume $\{P \in C(K) : f(P) \in R_S\}$ is infinite.

Fix t as before, set $\rho := \frac{\deg f}{2 \deg t}$

By 2.2, $\exists C_1 > 0$ s.t:

$$\prod_{v \notin S} \max\{\|v_f(P)\|_v, 1\} \geq \frac{C_1}{H_K(f(P))^\rho} \quad \forall \{P \in C(K) : f(P) \in R_S\}.$$

$$\Rightarrow H_K(t(P))^\rho \geq C \prod_{v \in S} \max\{\|f(P)\|_v, 1\} \quad \forall P \dots$$

If $f(P) \in R_S \Rightarrow \|f(P)\|_w \leq 1 \quad \forall w \notin S$, so that:

$$H_K(f(P)) = \prod_{w \in S} \max\{\|f(P)\|_w, 1\} \quad \text{in that case.}$$

So if $f(P) \in R_S$, then $H_K(t(P))^\rho \geq C_1 H_K(f(P)) \Rightarrow$

$$\Rightarrow \rho h(t(P)) \geq h(f(P)) - C_2 \quad (f(P) \in R_S) \Rightarrow$$

$$\Rightarrow \frac{\deg f}{2 \deg t} \geq \frac{h(f(P))}{h(t(P))} - \frac{C_2}{h(t(P))} \quad f(P) \in R_S.$$

By assumption we can let $h(t(P)) \to \infty$, and so:

$$\frac{\deg f}{2 \deg t} \geq \frac{\deg f}{\deg t} \Rightarrow \text{Contradiction.}$$

Faltings' Theorem.

Thm: Let K be a number field, and C/K a curve of genus $g \geq 2$.

Then $C(K)$ is finite.

Recall: To prove it, we embed $C \hookrightarrow J$, then $C(K) \subseteq J(K) \otimes \mathbb{R}$ (really, torsion doesn't matter, as it is finite)

which is a finite-dim euclidean vectorspace wrt the canonical height associated to the Θ-divisor $j(C) + \cdots + j(C)$ ($(g-1)$ copies)

We will prove:

Thm (Vojta's inequality): There are constants $\kappa_1 = \kappa_1(C)$, $\kappa_2 = \kappa_2(g)$ s.t.

if $z, w \in C(\bar{K})$ satisfying $|z| \geq \kappa_1$, $|w| \geq \kappa_2 |z|$ $(*)$.

Then $\langle z, w \rangle \leq \frac{3}{4} |z| \cdot |w|$.

Recall: This implies Faltings', through the discussion done at the beginning of the course.

Idea of Proof of Vojta's:

We are going to produce a height on $C \times C$, associated to a divisor Ω (called a Vojta divisor) and use standard properties of heights to estimate:

$$(\text{const}) \cdot |z|^2 + (\text{const}) \cdot |w|^2 - (\text{const}'') \langle z, w \rangle \geq F(h_\Omega(z, w)).$$

Warning: The choice of Ω will have to depend on (z, w).

Next, choosing Ω to be linearly equivalent to an effective divisor, we can estimate $h_\Omega(z, w) \geq \mathcal{O}(1)$ away from the base locus of $|\Omega|$.

Then, assuming $|z|, |w| >> 0$ and some algebra, we will conclude that

(z, w) satisfy $\langle z, w \rangle \leq \frac{|z||w|}{\sqrt{g}} \Rightarrow (*)$

Problems with the idea:

1) To get our estimates, we have to choose $D \in |\Sigma|$ defined by "small sections" of $\mathcal{O}(\Sigma)$.

2) We'll really be able to work away from D, but can't be sure that $(z,w) \notin \mathrm{supp}(D)$. We'll use Roth's lemma to show that D does not go through (z,w) with a high multiplicity. In this way, we'll still get a lower bound $h_\Sigma(z,w)$.

Step 0: Vojta divisor and associated heights

Fix: A divisor $A \in \mathrm{Div}(C)$ of deg 1, such that $(2g-2)A \in [K_C]$ (canonical divisor of C)

(possibly extending K).

Using A, get an embedding $j_A : C \hookrightarrow \mathcal{J}$

$$P \longmapsto [(P) - A]$$

We also get a Θ-divisor $\Theta_A := \underbrace{j_A(C) + \cdots + j_A(C)}_{(g-1)}$

Lemma 0.1: (a) $\Theta_A^- \sim \Theta_A$ $\quad (\Theta_A^- = [-1]^* \Theta_A)$

(b) $j_A^* \Theta_A \sim g \cdot A$

(c) $(j_A \times j_A)^* \left(s_{12}^* \Theta_A - p_1^* \Theta_A - p_2^* \Theta_A \right) \sim -\Delta_C + A \times C + C \times A$

($s_{12}(a,b) = a+b$; $p_1, p_2 : \mathcal{J} \times \mathcal{J} \to \mathcal{J}$ the projections)

Pf Observe that $\Theta_A = \Theta_P - j_P(\mathcal{O}(-1)A)$

(Θ_P: operation on $\mathcal{J}$, translate; when we choose $P \in C(k)$, $j_P : C \hookrightarrow \mathcal{J}$, corresponding Θ_P)

Use standard properties of Θ-divisors, and that $(2g-2)A \in [K_C]$.

Remark 0.3: If $d >> 0$, then the map $L(B)^{\otimes d} \longrightarrow L(dB)$ is surjective.

$$(y_{i_1} \otimes \cdots \otimes y_{i_d}) \longmapsto y_{i_1} \cdots y_{i_d}$$

Likewise, if $\delta_1, \delta_2 >> 0$, then the map

$$L(NA)^{\otimes \delta_1} \otimes L(NA)^{\otimes \delta_2} \longrightarrow L\left(\delta_1(NA \times C) + \delta_2(C \times NA)\right)$$

sending $(x_{i_1} \otimes \cdots \otimes x_{i_{\delta_1}}) \otimes (x'_{j_1} \otimes \cdots \otimes x'_{j_{\delta_2}}) \longmapsto x_{i_1} \cdots x_{i_{\delta_1}} \boxtimes x'_{j_1} \cdots x'_{j_{\delta_2}}$

is also surjective.

(if $X \times Y$ with projections to X and Y, and $L \to X$, $M \to Y$ are line bundles, then $L \boxtimes M \to X \times Y$ is defined to be $p_1^* L \otimes p_2^* M$)

Ftx: $h_{C\times C,\, \delta_1(NA\times C)+\delta_2(C\times NA)}(z,w) := \delta_1 h\left(\Phi_{NA}(z)\right) + \delta_2 h\left(\Phi_{NA}(w)\right)$.

Now let $d, d_1, d_2 \geq 0$ be integers. Set

$$\Omega := \Omega(d,d_1,d_2) := (d_1 - d)(A \times C) + (d_2 - d)(C \times A) + d\Delta \in \mathrm{Div}(C \times C).$$

Def: A divisor Ω is a Vojta divisor if $g d^2 < d_1 d_2 < g^2 d^2$ (**)

(note: for $g \leq 1$, there are no Vojta divisors!)

We will also assume that $N \mid d_1, d_2, d$ (we can always make them as large as we want)

Set $\delta_1 := \frac{d_1 + Md}{N}$ $\delta_2 := \frac{d_2 + Md}{N}$ and assume $d, d_1, d_2 >> 0$ s.t. (0.3) holds.

We can write

$$(0.4)\quad \Omega(d_1,d_2,d) = \overbrace{\delta_1(NA \times C) + \delta_2(C \times NA)}^{\text{very ample}} - \overbrace{dB}^{\text{very ample}}$$

Hence we can define

$$(0.5)\quad h_{C\times C,\,\Omega}(z,w) := \delta_1 h_{C,NA}(z) + \delta_2 h_{C,NA}(w) - d\, h_{C\times C,\,B}(z,w).$$

Fix: $N>0$ s.t NA is very ample (possible by Riemann-Roch, as any effective divisor is ample).

Fix: $\Phi_{NA}: C \hookrightarrow \mathbb{P}^n$ the corresponding embedding to NA (by choosing coordinates).

Note: $\Phi_{NA}(C)$ is not contained in any hyperplane.

Choose the coordinates $[x_0 : \cdots : x_n]$ s.t

(i) $\Phi_{NA}(C) \cap [x_i = x_j = 0, i \neq j] = \emptyset$, so that the natural map $[x_0 : \cdots : x_n] \mapsto [x_i : x_j]$ gives a morphism

$C \xrightarrow{\sim} \Phi_{NA}(C) \longrightarrow \mathbb{P}^1$ of degree N

(ii) The projection $\mathbb{P}^n \to \mathbb{P}^2$, $[x_0, \ldots, x_n] \mapsto [x_i : x_j : x_k]$ induces a birational map from $\Phi_{NA}(C)$ onto its image.

That is, $K(C) \cong K\left(\frac{x_j}{x_i}, \frac{x_k}{x_i}\right)$ and $\frac{x_k}{x_i}$ is integral of deg N over $K\left[\frac{x_j}{x_i}\right]$

Remark: the choices of coordinates on $\mathbb{P}^n$ are parametrized by $PGL(n+1)$.

One can show that (i), (ii) are dosed conditions;

Since K is infinite, we can choose coordinates as asserted.

Fix: $M>0$ s.t $B := (M+1)(A \times C) + (M-1)(C \times A) - \Delta$ is very ample on $C \times C$.

- An embedding $\Phi_B : C \times C \longrightarrow \mathbb{P}^m$, $[Y_0 : \cdots : Y_m]$ coming from the divisor B.
- $h_{C\times C, B}(z,w) := h(\Phi_B(z,w))$ (so that $h_{C\times C, B} = h \circ [Y_0, \ldots, Y_m]$).
- $h_{C\times C, dB} := d h_{C\times C, B}$

• Constants appearing in the proof:

→ γ, ε, ν : small positive numbers.

→ $c_1, c_2, \ldots$: constants depending on C, A and the choices of the various height functions we have made.

→ M, N (fixed)

d_1, d_2, d (not fixed) large integers s.t • $gd^2 < d_1 d_2 < g^2 d^2$

• $d_1 d_2 - gd^2 \geq \gamma d_1 d_2$

→ δ_1, δ_2 just defined (depending on d_1, d_2, d, M, N).

Step 1: Bounding h_{Ω} above:

Prop 1.1: There is $c_1 > 0$, depending on the choice of height function, s.t $\forall d, d_1, d_2 >> 0$ and $\forall (z,w) \in C(\bar{\kappa})$ we have:

$$h_{C\times C, \Omega(d,d_1,d_2)}(z,w) \leq \frac{d_1}{g}|z|^2 + \frac{d_2}{g}|w|^2 - 2d\langle z,w\rangle + c_1\cdot(d_1+d_2+d)$$

Note: c_1 does not depend on d_1, d_2, d, z, w.

Pf Recall that $h_{C\times C,\Omega}(z,w) = \delta_1 h_{C,NA}(p_1(z,w)) + \delta_2 h_{C,NA}(p_2(z,w)) - d\, h_{C\times C, B}(z,w)$

where $B = Mp_1^*A + Mp_2^*A + (-\Delta + p_1^*A + p_2^*A)$.

Now $h_{C,NA} = N h_{C,A} + O(1)$

$$h_{C\times C, B} = M h_{C,A}\circ p_1 + M h_{C,A}\circ p_2 + h_{C\times C, -\Delta + p_1^*A + p_2^*A} + O(1)$$

Recalling $\delta_i = \frac{d_i + Md}{N}$ and substituting, get:

$$h_{C\times C,\Omega}(z,w) = d_1 h_{C,A}(z) + d_2 h_{C,A}(w) - d\, h_{C\times C, -\Delta + p_1^*A + p_2^*A}(z,w) + O(d_1+d_2+d)$$

↓

By lemma 0.1, $j_A^* \mathcal{O}_A \sim gA$ and $(j \times j_A)^* (s_{12}^* \mathcal{O}_A - p_1^* \mathcal{O}_A - p_2^* \mathcal{O}_A) \sim -\Delta + p_1^* A + p_2^* A$ on $C \times C$

Using functoriality for j_A, s_{12}, p_1, p_2 we get:

$$h_{C,A}(u) = \frac{1}{g}|u|^2 + O(1) \quad \forall u \in C(\bar{k}).$$

$$h_{C\times C, -\Delta + p_1^*A + p_2^*A}(z,w) = |z+w|^2 - |z|^2 - |w|^2 + O(1) = 2\langle z,w\rangle + O(1).$$

Plug this in to get:

$$h_{C\times C, \Omega}(z,w) = \frac{d_1}{g}|z|^2 + \frac{d_2}{g}|w|^2 - 2d\langle z,w\rangle + O(d_1+d_2+d)$$

Step 2: Estimating heights below (away from zeroes of sections).

To estimate $h_{C\times C,\Omega}(z,w)$ below, we need to find an effective divisor $D \in |\Omega|$.

Now $D \hookrightarrow s \in L(\Omega)$ (up to constant multiples, this is 1:1).

$$L(\Omega) = L\left(\delta_1 (NA \times C) + \delta_2 (C \times NA) - dB\right).$$

So s can be described as $\frac{s'}{s''}$ (i.e. $s' = s \cdot s''$),

where s' is a homogeneous polynomial in $x_0, \dots, x_n$ of degree δ_1.

s' is a homogeneous bidegree (δ_1, δ_2) in $(x_0, \dots, x_n, x_0', \dots, x_n')$

s'' is a homogeneous degree d poly. in $(y_0, \dots, y_m)$

Actually, on this is a local description, taking the open where $y_i \neq 0$, we can assume $s'' = y_i^d$, and so:

$$S \xleftrightarrow{1:1} \text{collection } \mathcal{F} = \left\{ F_i(\underline{x}, \underline{x}') : \deg_{(\underline{x},\underline{x}')} F_i = (\delta_1, \delta_2) \text{ and } \frac{F_i}{y_i^d}\Big|_{C\times C} = \frac{F_j}{y_j^d}\Big|_{C\times C} \text{ where } y_i \neq 0 \text{ and } y_j \neq 0 \right\}$$

Proposition 1.1: Let $S \in L(\Omega)$, $\overline{F} = \{F_i\}$ as above.

Then $\forall (z,w) \in (C \times C)(\bar{K})$ s.t. $S(z,w) \neq 0$,

we have $h_{C\times C, \Omega}(z,w) \geq -h(\overline{F}) - n \log\left((\delta_1+n)(\delta_2+n)\right) \cdot |M_K^\infty|$.

Pf We write $\underline{x} := \Phi_{NA}(z)$, $\underline{x}' := \Phi_{NA}(w)$, $\underline{y} := \Phi_B(z,w)$.

Then $h_{C\times C,\Omega}(z,w) = \delta_1 h(\underline{x}) + \delta_2 h(\underline{x}') - d h(\underline{y}) =$

$$= \delta_1 \sum_v \max_j \log |x_j|_v + \delta_2 \sum_v \max_{j'} \log |x'_{j'}|_v - d \sum_v \max_i \log |y_i|_v =$$

$$= -\left(\delta_1 \sum_v \min_j \log |x_j^{-1}|_v + \delta_2 \sum_v \min_{j'} \log |x_{j'}^{-1}|_v + d \sum_v \max_i \log |y_i|_v \right)$$

$$= -\sum_v \max_i \min_{j,j'} \left| \frac{y_i^d}{x_j^{\delta_1} x_{j'}^{\delta_2}} \right|_v$$

Write $S(z,w) = \dfrac{F_i(\underline{x},\underline{x}')}{y_i^d}$ for some i s.t. $y_i^d \neq 0$ $(\in \bar{K})$

By the product formula, since $S(z,w) \neq 0$,

$$\sum_v \log |S(z,w)|_v = 0$$

Therefore, we can write:

$$h_{C\times C,\Omega}(z,w) = -\sum_v \max_i \min_{j,j'} \log \left| \frac{S(z,w)\, y_i^d}{x_j^{\delta_1} x_{j'}^{\delta_2}} \right|_v \overset{\checkmark}{=} \text{can avoid the term } y_i = 0, \text{ or the max will not be attained there!}$$

$$= -\sum_v \max_i \min_{j,j'} \log \left| \frac{F_i(\underline{x},\underline{x}')}{x_j^{\delta_1} x_{j'}^{\delta_2}} \right|_v = -\sum_v \max_i \min_{j,j'} \log \left| F_i\left(\frac{\underline{x}}{x_j}, \frac{\underline{x}'}{x'_{j'}}\right) \right|_v$$

The $\min_{j,j'}$ will be attained by picking $\max_j |x_j|_v$, $\max_{j'} |x'_{j'}|_v$

So $\min_{j,j'} \log \left| F_i\left(\frac{\underline{x}}{x_j}, \frac{\underline{x}'}{x'_{j'}}\right) \right| \leq \log \sum_{\text{if } v \text{ is archimedean}} (\#\text{monomials})(\max |\text{coeffs}|_v)$

If v is not archimedean, we don't get the (#monomials) term:

$$\max \log \left|F_i\left(\frac{x}{x_j^r}, \frac{x'}{x_{j'}^{r'}}\right)\right|_v \leq \begin{cases} \log(\#\text{monomials})(\max|\text{coeff}|_v) & v \text{ arch} \\ \log(\max|\text{coeff}|_v) & v \text{ non-arch} \end{cases}$$

So summing over all v, we get:

$$h_{C\times C,\mathcal{L}}(z,w) \geq -h(\mathcal{F}) - |M_K^\infty| \cdot n \cdot \log\left((\sigma_1+n)(\sigma_2+n)\right)$$

Next: bound $h(\mathcal{F})$ and make explicit how it depends on (d, d_1, d_2).

i.e. find $s \in \mathcal{L}(\mathcal{Q})$ s.t. $h(\mathcal{F})$ is small.

For this, we want to use a variant of Siegel's lemma for $\mathcal{O}_K$ (the proof is similar to the one for $\mathbb{Z}$).

Write then $\frac{y_i}{y_0}$ in terms of $\underline{x}, \underline{x}'$. Then $\frac{F_i}{y_i^d} = \frac{F_j}{y_j^d}$

$\Rightarrow P_i Q_j F_i = P_j Q_i F_j$, $P_i, Q_j \in K[\underline{x}, \underline{x}']$.

We will need the following version of Riemann-Roch:

Thm (Riemann-Roch for surfaces):
Let S be a smooth surface, K_S the canonical divisor on S, $D \in \mathrm{Div}(S)$.

Then: $\ell(D) - s(D) + \ell(K_S - D) = \frac{1}{2} D\cdot(D - K_S) + 1 + p_a(S)$

- $\ell(D) = \dim H^0$, which by Serre's duality is $\dim H^0$. $\left(h^0(S, \mathcal{O}_S(D))\right)$.
- $s(D) = \dim H^1(S, \mathcal{O}_S(D))$ called superabundancy. $\left(\text{write } s(D) = h^1(S, \mathcal{O}_S(D))\right)$.
- $p_a(S) = \chi(\mathcal{O}_S) - 1 = h^2(S, \mathcal{O}_S) - h^1(S, \mathcal{O}_S)$.

Recall also that Siegel's lemma tells us:

"If we have a system of linear equations $\mathcal{L}$ of height $h(\mathcal{L})$, with $\tilde{M}$ equations in $\tilde{N}$ unknowns, then there is a solution $\mathcal{F}$ s.t

$$h(\mathcal{F}) \leq \frac{\hat{M}}{\tilde{N}-\tilde{M}}\, h(\mathcal{L}) \leq \frac{\tilde{N}}{\tilde{N}-\tilde{M}}\, h(\mathcal{L})$$

Note: $\tilde{N}-\hat{M}$ = dimension of the space of solutions.

In our case, $\tilde{N}-\tilde{M} = \dim L(-\Omega)$ ← need a lower bound for $\ell(-\Omega)$.

$\tilde{N}$ = dim. of space of $\{F_i\}_{0\leq i\leq m} = (m+1)\cdot \dim L\left(\delta_1(NA\times C) + \delta_2(C\times NA)\right)$

For this estimate, we use Riemann-Roch.

Lemma 1.2: For all $d, d_1, d_2 \gg 0$, we have:

a) $\ell(-\Omega(d_1,d_2,d)) \geq d_1 d_2 - g d^2 - (g-1)(d_1+d_2)$.

b) $\ell(\delta_1(NA\times C) + \delta_2(C\times NA)) = (N\delta_1 - g + 1)(N\delta_2 - g + 1)$

Pf/ Write $A_1 := A\times C$, $A_2 := C\times A$.

Then recall (i) $K_C \sim (2g-2)\cdot A$

(ii) $K_{C\times C} \sim p_1^* K_C + p_2^* K_C \sim (2g-2)A_1 + (2g-2)A_2$.

Also, recall that $\Omega = (d_1 - d)A_1 + (d_2 - d)A_2 + d\Delta$.

Have the following table of intersection numbers (which we will use for R-R):

$\cdot$	A_1	A_2	Δ
A_1	0	1	1
A_2	1	0	1
Δ	1	1	$2-2g$

← This can be seen from the rest of the table, (i), (ii), and the fact that, for any $C' \subseteq X$, $(2g_{C'}-2) = C'\cdot(C'+K)$

So $\frac{1}{2}\Omega\cdot(\Omega-K) \overset{\text{exercise}}{=} d_1 d_2 - g d^2 - (g-1)(d_1+d_2)$.

By R-R: $\ell(\Omega) - s(\Omega) + \ell(K-\Omega) = d_1 d_2 - g d^2 - (g-1)(d_1+d_2) + 1 + \overbrace{(g-1)^2}^{P_a(C)}$

From this, that $s(\Omega) \geq 0$ and $1+(g-1)^2 \geq 0$, we need only to prove that $\ell(K-\Omega)=0$.

We'll show that $|K-\Omega| = \emptyset$, by showing that there's some divisor in $K-\Omega$ intersects negatively with some ample divisor.

$$(K-\Omega)\cdot(\overbrace{A_1+A_2}^{\text{ample}}) = (4g-4) - (d_1+d_2) < 0 \quad \text{for } d_1, d_2 \geq 0$$

(a)

For part (b), we get (R-R) $\ell(N(\delta_1 A_1 + \delta_2 A_2)) - s(\dots) + \ell(K-\dots) =$

$$= \frac{1}{2}(\dots)\cdot[(\dots)-K] + 1 + (g-1)^2 = (N\delta_1 - g + 1)(N\delta_2 - g + 1)$$

↑ exercise, computing with intersection numbers.

~~As before, we are reduced to show~~

Now we want to compute $s(N(\delta_1 A_1 + \delta_2 A_2))$.

If $\delta_1, \delta_2 >> 0$ then $N(\delta_1 A_1 + \delta_2 A_2)$ becomes very ample. $\Rightarrow$

$\Rightarrow s(N(\delta_1 A_1 + \delta_2 A_2)) = 0$ for some $\delta_1, \delta_2 >> 0$.

(lemma)

We can write $K(C\times C) = K\left(\frac{x}{x_0}, \frac{x'}{x_0}\right)$ ← restricted, of course, to $C\times C$.

Then $\frac{y_i}{y_0} = \frac{P_i(x,x')}{Q_i(x,x')}$, and the condition $\frac{F_i(x,x')}{y_i^d} = \frac{F_j(x,x')}{y_j^d}$ translates into

(*) $(P_i Q_j)^d F_i\big|_{C\times C} = (P_j Q_i)^d F_j\big|_{C\times C}$ $\quad 0 \leq i,j \leq m$.

Proposition 1.3: Let $\gamma > 0$, $d_1, d_2, d \gg 0$, s.t $d_1 d_2 - g d^2 \geq \gamma d_1 d_2$.

Then $\exists\, s \in \mathcal{L}(\Omega(d_1, d_2, d))$ given by $\mathcal{F}$, with

$$h(\mathcal{F}) \leq C \frac{d_1 + d_2}{\gamma} + \sigma(d_1 + d_2) \qquad \left(\frac{\sigma(d_1+d_2)}{(d_1+d_2)} \to 0 \text{ when } (d_1+d_2) \to \infty\right)$$

(C depending on C, K, Φ_{NA}, Φ_{NB} but not on d_1, d_2, d).

Pf/ we need to choose affine coordinates

(α) $$\begin{array}{ccccc} C & \xrightarrow{\Phi_{NA}} & \mathbb{P}^n & \dashrightarrow & \mathbb{P}^1 \\ & & [x_0 : \dots : x_n] & \longmapsto & [x_0 : x_1] \end{array}$$ (π is a morphism of degree N on C)

(β) The map $\pi_j : C \hookrightarrow \mathbb{P}^n \longrightarrow \mathbb{P}^2$, $[\underline{x}] \longmapsto [x_0 : x_1 : x_j]$ is a morphism, birational onto its image $\pi_j(C) \subseteq \mathbb{P}^2$.

Also, $$\begin{array}{ccc} C & \xrightarrow[\pi_j]{\leftarrow \text{bimer} \rightarrow} & \pi_j(C) \subseteq \mathbb{P}^2 \\ & \searrow^{\pi} \quad \swarrow \deg N & \\ & \mathbb{P}^1 & \\ & [x_0, x_1] & \end{array}$$ $\Rightarrow$ $\pi_j(C)$ is a degree-N curve inside $\mathbb{P}^2$.

We will use only π_2 ($j=2$).

$K(C) = K(\xi_1, \xi_2)$, where $\xi_i = \frac{x_i}{x_0}\Big|_C$, $i \geq 1$.

We can get $C \setminus \operatorname{supp} A$ as the Spec of $K[\xi_1, \dots, \xi_n]$.

WLOG may assume that $\pi_2(C)$ is given by an equation

$$\xi_2^N = \sum a_{i2}(\xi_1)\, \xi_2^i \quad \text{w/ } a_{i2}(\xi_1) \in K[\xi_1], \ \deg_{\xi_1} a_{i2} \leq N - i$$

Now, $K(\xi_1, \xi_2)$ has a $K(\xi_1)$-basis $\{1, \xi_2, \dots, \xi_2^{N-1}\}$

and in fact $K[\xi_1, \xi_2]$ is a free $K[\xi_1]$-module on N generators.

Likewise, $K(C\times C) = k(\xi_1, \xi_2, \xi_1', \xi_2')$

(using the embedding $C\times C \xrightarrow{\Phi_{NA}\times\Phi_{NA}} \mathbb{P}^n \times \mathbb{P}^N$)

$K(C\times C)$ has basis $\mathcal{B} = \{\xi_2^i \xi_2'^j : 0\le i,j\le N-1\}$ over $K(\xi_1, \xi_1')$.

Finally, using $\Phi_B : C\times C \hookrightarrow \mathbb{P}^m$ we can write

$$\frac{y_i}{y_0} = \frac{P_i(\xi_1,\xi_2,\xi_1',\xi_2')}{Q_i(\xi_1,\xi_2,\xi_1',\xi_2')} \quad \text{with} \quad P_i, Q_i \in \mathcal{O}_K[\xi_1,\xi_2,\xi_1',\xi_2'].$$

We are looking for $F_i(\underline{\xi},\underline{\xi}') \in K[\underline{\xi},\underline{\xi}']$ s.t.

$$(P_i Q_j)^d F_i = (P_j Q_i)^d F_j \qquad 0\le i,j\le m \quad \text{and} \quad \deg_{\underline{\xi},\underline{\xi}'} F_i \le (\delta_1,\delta_2).$$

Let $V_1 := \{F\in K(C\times C) : F\in K[\underline{\xi},\underline{\xi}'] \text{ of deg } \le(\delta_1,\delta_2)\}$.

$$V_3 := \left\{ (F_0,\dots,F_m)\in K[\underline{\xi},\underline{\xi}']^{m+1} : \begin{array}{l} \deg F_i \le(\delta_1,\delta_2) \\ (P_iQ_j)^d F_i = (P_jQ_i)^d F_j \end{array} \right\}$$

$$V_2 := V_1 \cap K[\xi_1,\xi_2,\xi_1',\xi_2']$$

We will only look for solutions in V_2.

$$\dim V_1 = (N\delta_1 - g+1)(N\delta_2 - g+1)$$

$$\dim V_2 = \left(N\delta_1 - \tfrac{1}{2}N(N-3)\right)\left(N\delta_2 - \tfrac{1}{2}N(N-3)\right)$$

$$\dim\left(V_2^{m+1}\cap V_3\right) \ge \dim V_3 - \left(\dim V_1^{m+1} - \dim V_2^{m+1}\right) \overset{(1.2.(a))}{\ge} \left[d_1d_2 - gd^2 - (g-1)(d_1+d_2)\right] -$$

$$-(m+1)(N\delta_1-g+1)(N\delta_2-g+1) + (m+1)\left(N\delta_1 - \tfrac{1}{2}N(N-3)\right)\left(N\delta_2 - \tfrac{1}{2}N(N-3)\right) \ge$$

$$\ge d_1d_2 - gd^2 + \mathcal{O}(d_1+d_2) \underset{\text{assumption}}{\ge} \gamma d_1 d_2 + \mathcal{O}(d_1+d_2)$$

We can now apply Siegel's lemma with:

"N" $\leq (m+1)N^2\delta_1\delta_2 + \mathcal{O}(d_1+d_2+d)$

"$N-M$" $\geq \gamma d_1 d_2 + \mathcal{O}(d_1+d_2)$

$h(\text{constraints}) \leq C_2 \cdot d$

So we can find $\mathcal{F}$ $(\leftrightarrow s \in L(\Omega))$

with $h(\mathcal{F}) \leq C_4 \dfrac{(m+1)N^2\delta_1\delta_2 + \mathcal{O}(d_1+d_2+d)}{\gamma d_1 d_2 + \mathcal{O}(d_1+d_2)} \cdot d$

Recall now that $\delta_i = \dfrac{d_i+Md}{N}$, $d_1 d_2 > g d^2$ and we calculate:

$\delta_1\delta_2 \approx d_1 d_2$, M, m, N fixed, $d_1, d_2, d >> 0$, $d_1+d_2 > d$.

So $h(\mathcal{F}) \leq C_5 \dfrac{d_1+d_2}{\gamma} + \mathcal{O}(d_1+d_2)$

Step 2: Case when $s(z,w) = 0$.

(A) Bound $h_{\Omega}(z,w) \geq -h(\mathcal{F}) - \mathcal{O}(\text{index of } s \text{ at } (z,w)) - (\text{expression depending on the leading coeff of } s \text{ at } (z,w))$

(B) $h(\text{leading coeffs}) \leq$ expression of $|z|^2$, $|w|^2$, $\text{Ind}_{(z,w)}(s)$.

(C) Roth's lemma, to bound $\text{Ind}_{(z,w)}(s)$.

A) Choose local parameters ξ, ξ' of C at z resp. w, and define $(C \times C)$

$\partial_i := \dfrac{1}{i!}\dfrac{\partial^i}{\partial \xi^i}$, $\partial'_i := \dfrac{1}{i!}\dfrac{\partial^i}{\partial \xi'^i}$ $\leftarrow$ diff-operators at (z,w).

We'll assume $\begin{cases} x_j(z) \neq 0 & 0 \leq j \leq n \\ x'_j(w) \neq 0 & 0 \leq j \leq n \\ y_0(z,w) \neq 0 \end{cases}$

(because this $\Rightarrow$ wrong at finitely-many points of $(C \times C)(\overline{K})$

(cont'd)

We are looking $\tilde{F} \in V_3 \cap V_2^{m-1}$ of dim $\geq \gamma d_1 d_2 + O(d_1+d_2)$

inside V_2^{m-1}, which has dimension $\leq (m+1)N^2\delta_1\delta_2 + O(d_1+d_2+d)$.

We want linear constraints describing $V_3 \cap V_2^{m+1} \subseteq V_2^{m+1}$, and bound the height of their coefficients.

Let $F_i \in V_2$. We can write (uniquely) $F_i = \sum_{\nu \in \mathcal{B}} u_{ikk'\nu}\, \xi_1^k\, \xi_1'^{k'}\, \nu$

We view $u_{ikk'\nu}$ as our variables. $\quad k,k' \geq 0,\ \deg(\xi_2)\,\nu + k \leq \delta_1,\ \deg \xi_2'\,\nu + k' \leq \delta_2$

Lemma 1.4: The constraints on the $(u_{ikk'\nu})_{ikk'\nu}$ forcing $\tilde{F} = \{(\sum_{\nu,k,k'} u_{ikk'\nu}\, \xi_1^k \xi_1'^{k'} \nu)_i\}$ to lie in $V_2^{m+1} \cap V_3$ have coefficients of

height $h(\text{coeff}) \leq C_2 \cdot d$

(where C_2 depends on C, K, Φ_{NA}, Φ_B, but NOT on d_1, d_2, d).

Pf (Sketch):

The coeffs of the constraints come from "$(P_i Q_j)^d$". More precisely, we write $(P_i Q_j)^d = \sum_{\nu \in \mathcal{B}} P_{ij\nu d}(\xi_1, \xi_1')\,\nu$ (in the basis $\mathcal{B}$).

It turns out that $h(P_{ij\nu d}) \leq C_3 \cdot d$ $\quad (C_3 = C_3(P_i, Q_j, \pi_2(C)))$

(and also depends on the structure constants of $K[\xi_1, \xi_1', \xi_2, \xi_2']$ in terms of $\mathcal{B}$)

Apply algebra results to get the Lemma.

Let $s \in L(\mathcal{L}(d_1, d_2, d))$ given by $\mathcal{F} = (F_i)_{0 \le i \le m}$.

Set $f := \dfrac{y_0^d s}{x_0^{\delta_1} x_0'^{\delta_2}} = \left(\dfrac{y_0}{y_i}\right)^d F_i\left(\dfrac{x}{x_0}, \dfrac{x'}{x_0'}\right) \in K(c,c)$ (independent of i).

We can apply ∂_i^*, $\partial_{i'}'^*$ to f at (z,w)

Def: $\mathrm{Ind}_{(z,w)}(s) = \min\left\{ \dfrac{i_1}{\delta_1} + \dfrac{i_2}{\delta_2} \;\middle|\; i_1, i_2 \ge 0 \text{ and } \partial_{i_1} \partial_{i_2}' f(z,w) \neq 0 \right\}$.

A point (i_1^*, i_2^*) is called "admissible" if it realizes the index, i.e. $\dfrac{i_1^*}{\delta_1} + \dfrac{i_2^*}{\delta_2} = \mathrm{Ind}_{(z,w)}(s)$ and $\partial_{i_1^*} \partial_{i_2^*}' f(z,w) \neq 0$.

Note: if $(i_1, i_2) < (i_1^*, i_2^*)$, then $\partial_{i_1} \partial_{i_2}' f(z,w) = 0$

(i.e. $i_1 \le i_1^*$, $i_2 \le i_2^*$ and $i_1 + i_2 < i_1^* + i_2^*$).

Lemma 2.1: Suppose (i_1^*, i_2^*) is admissible, and $g \in K(c,c)$ s.t. $g(z,w) \notin \{0, \infty\}$.

Then $\partial_{i_1^*} \partial_{i_2^*}' f(z,w) = \left(\dfrac{\partial_{i_1^*} \partial_{i_2^*}' (fg)}{g} \right)(z,w)$

Pf Leibniz rule + previous note. //

Prop 2.2: Let $s \in L(\mathcal{L}) \sim \mathcal{F}$. Let (i_1^*, i_2^*) be admissible.

Then $h_{c,c,\mathcal{L}}(z,w) \ge -h(\mathcal{F}) - (i_1^* + i_2^* + 2\delta_1 + 2\delta_2 + 2n)|M_K^\infty| -$

$$- \sum_v \max_{i_1 + \cdots + i_{\delta_1} = i_1^*} \sum_{k=1}^{\delta_1} \max_{0 \le \ell \le n} \min_j \log \left| \left(\partial_{i_k} \frac{x_\ell}{x_j} \right)(z) \right|_v -$$

$$- \sum_v \max_{i_1' + \cdots + i_{\delta_2}' = i_2^*} \sum_{k=1}^{\delta_2} \max_{0 \le \ell \le n} \min_j \log \left| \left(\partial_{i_k}' \frac{x_\ell'}{x_j'} \right)(z) \right|_v .$$

↓

Pf (of long-statement lemma)

Recall $h_{\mathcal{L}}(z,w) = \delta_1 h\left(\Phi_{N+}(z)\right) + \delta_2 h\left(\Phi_{N+}(w)\right) - d\,h\left(\Phi_D(z,w)\right) =$

$$= -\sum_v \max_i \max_{j,j'} \log \left| \left(\frac{y_i^d}{x_j^{\delta_1} x_{j'}^{\delta_2}} \right)(z,w) \right|_v$$

Since $\partial_{i_1}^* \partial_{i_2}^{\prime *} f(z,w) \neq 0$, we have $\sum_v \log \left| \partial_{i_1}^* \partial_{i_2}^{\prime *} f(z,w) \right|_v = 0$.

So by subtracting 0, we get:

$$h_{\mathcal{L}}(z,w) \overset{\text{equality, actually}}{\geq} -\sum_v \max_i \min_{j,j'} \log \left| \left(\frac{y_i^d \, \partial_{i_1}^* \partial_{i_2}^{\prime *} f}{x_j^{\delta_1} x_{j'}^{\delta_2}} \right)(z,w) \right|_v$$

Since $x_0(z) \neq 0$, $x_0'(z) \neq 0$, $y_0(z,w) \neq 0$, the product formula also implies that $\sum_v \log \left| \frac{y_0^d}{x_0^{\delta_1} x_0'^{\delta_2}}(z,w) \right|_v$

Adding this, we get:

$$h_{\mathcal{L}}(z,w) \geq -\sum_v \max_i \min_{j,j'} \log \left| \frac{\left(y_i/y_0\right)^d \, \partial_{i_1}^* \partial_{i_2}^{\prime *} f}{\left(x_j/x_0\right)^{\delta_1} \left(x_{j'}'/x_0'\right)^{\delta_2}}(z,w) \right|_v$$

Apply now lemma 2.1, with $g := \left[\frac{\left(y_i/y_0\right)^d}{\left(x_j/x_0\right)^{\delta_1} \left(x_{j'}'/x_0'\right)^{\delta_2}} \right]^{-1}$

& do (v,i,j,j'), to get:

$$\frac{\left(y_i/y_0\right)^d \partial_{i_1}^* \partial_{i_2}^{\prime *} f}{\left(x_j/x_0\right)^{\delta_1} \left(x_{j'}'/x_0'\right)^{\delta_2}}(z,w) = \partial_{i_1}^* \partial_{i_2}^{\prime *} \left(\frac{\left(y_i/y_0\right)^d f}{\left(x_j/x_0\right)^{\delta_1} \left(x_{j'}'/x_0'\right)^{\delta_2}} \right)(z,w) \overset{\text{def of } f,\ + F_i \text{ are bilinear}}{=}$$

$$= \left[\partial_{i_1}^* \partial_{i_2}^{\prime *} F_i \left(\frac{x}{x_j}, \frac{x'}{x_{j'}'} \right) \right](z,w).$$

□

(cont pf)
we plug this in, to get

$$h_{\mathcal{D}_2}(z,w)\,\xi_i = \sum_v \max_i \min_{j,j'} \log \left| \partial_{i\hat{1}} \partial'_{i\hat{2}} F_i\left(\frac{x}{x_j}, \frac{x'}{x'_{j'}}\right)^{(\#)} \right|_v$$

we need to estimate the $\log|\cdots|_v$, and this will prove the proposition.

Lemma 2.3: Let $\xi_0, \dots, \xi_n \in K(C)$ be regular at z,
and $\xi'_0, \dots, \xi'_n \in K(C)$ be regular at w.
Let $F(\underline{\xi}, \underline{\xi}')$ be bihomogeneous of deg $= (\delta_1, \delta_2)$, and suppose
that ξ, ξ' are uniformizers at z, w.

Then: $\forall v \in M_K$,

$$\left|\partial_{i_1^*} \partial'_{i_2^*} F(\underline{\xi}, \underline{\xi}')(z,w)\right|_v \le 2_v^{\,i_1^* + i_2^* + 2\delta_1 + 2\delta_2 + 2n} \cdot |F|_v \times$$

$$\times \max_{i_1 + \cdots + i_{\delta_1} = i_1^*} \prod_{\kappa=1}^{\delta_1} \max_{0 \le \ell \le n} \left|(\partial_{i_\kappa} \xi_\ell)(z)\right|_v \times \max_{i'_1 + \cdots + i'_{\delta_2} = i_2^*} \prod_{\kappa=1}^{\delta_2} \max_{0 \le \ell \le n} \left|(\partial_{i'_\kappa} \xi'_\ell)(w)\right|_v$$

where $2_v = \begin{cases} 2 & v \in M_K^\infty \\ 1 & \text{else} \end{cases}$

pf:
- $2_v^{\delta_1+\delta_2+2n}$ from replacing each coeff of F by the v-maximal.
- number of monomials of bidegree (δ_1, δ_2) is $\le 2^{\delta_1+\delta_2+2n}$
(+ use the ultrametric ineq.).

~~Use chain rule and~~

Exercise for the reader.

(Prop)

We now want to estimate $\left|\partial_{i_\kappa} \frac{x_\ell}{x_j}(z)\right|_v$ above,
as they appear in the statement of the Prop 2.2.

$\frac{X_\ell}{X_j} \in K(C)$, $\partial_i = \frac{1}{i!}\frac{\partial^i}{\partial z^i}$. Recall that z is a local parameter at $\mathfrak{z}$.

So $\mathfrak{z}: C \to \mathbb{P}^1$ is a morphism of some degree (locally).

If $\xi \in K(C)$, $\exists\, P(X,Y)$ over K of degree $\leq [K(C):K(\mathfrak{z})]$

s.t. $P(\xi(z), \zeta(z)) = 0$ for $|z| \ll 1$ $\quad P_Y(\xi(z), \zeta(z)) \neq 0$ (where $P_Y = \frac{\partial}{\partial Y} P$)

Then the implicit function theorem implies that $\xi(\zeta) = \sum_{j \geq 0} \left(\partial_i \xi(\mathfrak{z})\right) \zeta^i$

Prop 2.4: Let $P(\xi, \zeta) \in K[\xi, \zeta]$ of degree D; Let $a \in K$: $P(a,0) = 0$,

and $P_\xi(a,0) \neq 0$. Let $\xi = \xi(z)$ be the function defined by

$$P(\xi(\zeta), \zeta) = 0 \text{ and } \xi(0) = a.$$

Then for each valuation $v \in M_K$, we have:

$$|\partial_i \xi(0)|_v \leq (2D)_v^{4i} \left(\frac{|P|_v}{|P'_\xi(a,0)|_v} \right)^{2i-1} \cdot \max\{1, |a|_v\}^{2iD}$$

(where for $N \in \mathbb{N}$, $N_v = \begin{cases} N & \text{if } v \in M_K^\infty \\ 1 & \text{if } v \in M_K^0 \end{cases}$)

Pf (Sketch):

For any $i \geq 1$, there is a polynomial $q_i(\xi, \zeta)$ s.t. $q_i + (P_\xi)^{2i-1} \frac{\partial^i \xi}{\partial \zeta^i} = 0$.

The q_i are defined as follows:

$q_1 = P_\zeta$ (using $\frac{\partial}{\partial \zeta}(P(\xi,\zeta) = 0)$).

and $q_{i+1} = -(q_i)_\xi P_\zeta P_\xi + (q_i)_\xi P_\xi^2 + (2i-1) q_i (-P_{\xi\xi} P_\zeta + P_{\xi\zeta} P_\xi)$ $\quad (i \geq 1)$.

To obtain the desired estimates, we use:

(0) A bound on the degree of q_i (in terms of the degree of P, which is D)

(i) $|\prod_{i=1}^r f_i|_v \leq$ (expression in $\deg f_i$ for $i \geq 2$) $\cdot \prod_{i=1}^r |f_i|_v$ (thanks to Bombieri) (B.7.4 in Bom.

(ii) $|\sum_{i=1}^r f_i|_v \leq r_v \max |f_i|_v$; (iii) $\left|\frac{\partial f}{\partial x_j}\right|_v \leq (\deg f)_v |f|_v$

Proposition 2.5: Let $s \in L(\Omega(d_1,d_2,d))$ be given by $\mathcal{F}=(F_i)_{0\le i\le m}$, and let (i_1^*, i_2^*) be an admissible pair for s at (z,w).

Then there is a finite set $E \subseteq C(\bar{k})$ s.t. $\forall (z,w) \notin E$ we have

$$h_{C\times C,\Omega}(z,w) \ge -h(\mathcal{F}) - c_1\left(i_1^*(z)^2 + i_2^*(w)\right)^2 - c_2\cdot\left(i_1^* + i_2^* + \delta_1+\delta_2+1\right)$$

Pf (sketch):

Exclude all points $u \in C(\bar{k})$ where $\frac{x_1}{x_0} - \frac{x_1}{x_0}(u)$ is not a local parameter (only finitely many such points).

Look at the composite

$$C \xrightarrow{\Phi_{NA}} \mathbb{P}^n \longrightarrow \mathbb{P}^1\times\mathbb{P}^1 \xrightarrow{\text{Segre}} \mathbb{P}^3 \xrightarrow{\text{proj}^{\text{al}}} \mathbb{P}^2$$

$$u \longmapsto \left([x_\ell : x_j], [x_0 : x_i]\right)$$

$$([a,b],[c,d]) \longmapsto [ac : bd : bc : ad]$$

$$[x,y,z,w] \longmapsto [x:y:z].$$

The map $C \longrightarrow \mathbb{P}^2$, given by $[x_\ell x_0 : x_j x_1 : x_j x_0]$ is a birational morphism onto its image, a degree $2N$ curve in $\mathbb{P}^2$.

Exclude points of C for which this is not an isomorphism.

So on $\mathrm{im}(C)$, we have $G_{\ell j}(x_\ell x_0, x_j x_1, x_j x_0) = 0$ for some $G_{\ell j}$ of degree $2N$ (and homogeneous).

Dehomogenizing by $\frac{1}{(x_j x_0)^{2N}}$, get $g_{\ell j}\left(\frac{x_\ell}{x_j}, \frac{x_1}{x_0}\right) = 0$ of deg $\le 2N$.

Set $P_{\ell j}(S,T) := g_{\ell j}\left(S, T + \frac{x_1}{x_0}(z)\right)$. Note that $|P_{\ell j}|_v \le c_3(v)\cdot \max\left\{1, \left|\frac{x_1}{x_0}(z)\right|_v\right\}^{2N}$.

where $c_3(v) = 1$ for almost all v.

Now, apply 2.4 w/ $i = i_k$; $\xi = \frac{x_\ell}{x_j}$; $\zeta = \frac{x_1}{x_0} - \frac{x_1}{x_0}(z)$; $P = P_{\ell j}$; $a = \xi(0) = \frac{x_\ell}{x_j}(z)$

and $D = \deg P_{\ell j} \le 2N$.

↓

we also exclude the points where $|P_{ij}(a,0)|_v = 0$ (in the denom. of the estimate)

i.e. points for which $(g_{ej})_{\xi}\left(\frac{x_\ell}{x_j}(u), \frac{x_i}{x_0}(u)\right) = 0$.

With this, we get $\left|\left(\partial_{i_k} \frac{x_\ell}{x_j}\right)(z)\right|_v \leq (4N)_v^{4i_k} \cdot \left(\frac{|P_{ej}|_v}{|(P_{ej})_{\xi}(a,0)|_v}\right)^{2i_k-1} \cdot \max\left\{1, \left|\frac{x_\ell}{x_j}(z)\right|_v^{4i_kN}\right\}$

Using that $\min_j a_j b_j \leq \max_j a_j \min_j b_j$, we get:

$$\left|\partial_{i_k} \frac{x_\ell}{x_j}(z)\right|_v \leq (4N)_v^{4i_k} \max_{0\leq j\leq n} \left(\frac{|P_{ej}|_v}{|(P_{ej})_{\xi}(a,0)|_v}\right)^{2i_k-1} \leq \left(\text{replace } |P_{ej}|_v \text{ by a constant}\right)$$

$$\leq (4N)_v^{4i_k} \max_j \left(\frac{C_4(v)}{|(P_{ej})_{\xi}(a,0)|_v}\right)^{2i_k-1} \quad (*)$$

(where $C_4(v) = 1$ for almost all v).

Moreover, $(P_{ej})_{\xi}(a,0) = (g_{ej})_{\xi}\left(\frac{x_\ell}{x_j}(z), \frac{x_i}{x_0}(z)\right)$, so:

$$(*) \leq (4N)_v^{4i_k} \max_{0\leq j\leq n} \left(\frac{C_4(v)}{|(g_{ej})_{\xi}\left(\frac{x_\ell}{x_j}(z), \frac{x_i}{x_0}(z)\right)|_v}\right)^{2i_k-1}$$

Taking log and $\max_{\ell,i}$ we get:

$$\max_{0\leq \ell\leq n} \min_j \log\left|\left(\partial_{i_k} \frac{x_\ell}{x_j}\right)(z)\right|_v \leq \max_{\ell,j} \log\left((4N)_v^{4i_k}\left(\frac{C_4(v)}{|(g_{ej})_{\xi}|_v}\right)^{2i_k-1}\right) \leq$$

$$\leq \underbrace{C_5(v)}_{0 \text{ for almost all } v}\, i_1^* + (2i_k-1)\left\{\sum_{0\leq j,\ell\leq n} \underbrace{\log^+}_{\max\{0,\log\}} \left|(g_{ej})_{\xi}\left(\frac{x_\ell}{x_j}(z), \frac{x_i}{x_0}(z)\right)\right|_v^{-1}\right\} \leftarrow (\S)$$

$\sum_v (\S)$ can be estimated using

- $h\left((g_{ej})_{\xi}\right)$, $\left(\deg\left((g_{ej})_{\xi}\right)\right)_v$
- $h\left(\left[\frac{x_\ell}{x_j}(z) : \frac{x_i}{x_0}(z) : \dots\right]\right) \leq 2h\left(\Phi_{NA}(z)\right) \leq \tilde{C} \cdot |z|^2$ (using functoriality)

$$\Rightarrow \sum_v (\S) \leq C_6\, i_1^* |z|^2 + C_7 i_1^*$$

Putting it altogether, get the estimate

Recall:

1) There's $c_1 > 0$ s.t. $\forall d_1, d_2, d \gg 0$ + condition, and $(z,w) \in \mathbb{C}(k)$,

$$h_{C\times C, \mathcal{L}(d_1,d_2,d)}(z,w) \leq \frac{d_1}{g}|z|^2 + \frac{d_2}{g}|w|^2 - 2d\langle z, w\rangle + c_1(d_1+d_2+d).$$

2) For $s \in L(\mathcal{L})$ given by $\mathcal{F} = (F_i)_{0\leq i\leq m}$, and (i_1^*, i_2^*) admissible for s at (z,w), then $\exists\, c_2, c_3$ s.t.

$$h_{\mathcal{L}}(z,w) \geq -h(\mathcal{F}) - c_2\left(i_1^*|z|^2 + i_2^*|w|^2\right) - c_3\left(i_1^* + i_2^* + \delta_1 + \delta_2 + 1\right)$$

3) For $\gamma > 0$, $d_1, d_2, d > 0$ and $d_1 d_2 - g d^2 \geq \gamma d_1 d_2$, then $\exists\, c_4$ and we can find a global section $s \in L(\mathcal{L})$ s.t.

$$h(\mathcal{F}) \leq c_4 \frac{d_1+d_2}{\gamma} + o(d_1+d_2) \qquad (c_4 \text{ not depending on } d\text{'s and on } \gamma)$$

Step 3: Bounding the index.

Lemma 3.1 (Restatement of Roth's lemma): Let $P \in \bar{\mathbb{Q}}[X_1, X_2]$ be non-zero, $\deg P \leq (r_1, r_2)$ and let $\beta_1, \beta_2 \in \bar{\mathbb{Q}}$.

Suppose $1 \geq \omega > 0$ s.t.

(i) $r_2 \leq \omega r_1$

(ii) $h(P) + 4r_1 \leq \omega \cdot \min\{r_1 h(\beta_1), r_2 h(\beta_2)\}$

Then $\exists\, i_1, i_2 \geq 0$ s.t. $\frac{i_1}{r_1} + \frac{i_2}{r_2} \leq 4\sqrt{\omega}$ and $\partial_{\underline{i}} P(\beta_1, \beta_2) \neq 0$.

Prop 3.2: There is a constant $c_5 > 0$ s.t. for $0 < \varepsilon, \gamma \leq 1$ w/ $\varepsilon^2 d_1 \geq d_2$ and $\min\{d_2|w|^2, d_1|z|^2\} \geq \frac{c_5}{\gamma\varepsilon^2} d_1$ and s.t. $d_1 d_2 - g d^2 \geq \gamma d_1 d_2$.

Let $s \in L(\mathcal{L})$ s.t. $h(\mathcal{F}) \leq c_4 \frac{d_1+d_2}{\gamma} + o(d_1+d_2)$.

Then $\exists\, (i_1^*, i_2^*)$ admissible for s at (z,w) s.t.

$$\frac{i_1^*}{d_1} + \frac{i_2^*}{d_2} \leq 12N\varepsilon.$$

Pf (of 3.2): Let $\xi_i = \frac{x_i}{x_0}$, $\xi_i' = \frac{x_i'}{x_0}$.

we are going to produce $\Phi(\xi_1, \xi_1') = P(x_1, x_2)$, and

$\beta_1 = \xi_1(z)$, $\beta_2 = \xi_1'(w)$.

If $x_0(u) \neq 0$, we have:

$h_{C,\Delta}(u) = \frac{1}{g}|u|^2 + O(1)$ (by functoriality + linearity)

So $h_{C,N\Delta}(u) = h(\mathbb{P}_N(u)) = h([1 : \xi_1(u) : \cdots : \xi_n(u)]) \leq$

$\leq \sum_{i=1}^{n} h(\xi_i(u)) \overset{\text{WLOG}}{\leq} n\, h(\xi_1(u))$

Then, $h(\xi_1(z)) \geq \frac{N}{ng}|z|^2 + O(1)$

$h(\xi_1'(z)) \geq \frac{N}{ng}|w|^2 + O(1)$

As $[K(C\times C) : K(\xi_1, \xi_1')] = N^2 < \infty$,

can set $Q(\xi_1, \xi_1') := \mathrm{Norm}_{K(C\times C)/K(\xi_1,\xi_1')}\left(\frac{F_i(\underline{\xi}, \underline{\xi}')}{(y_i/y_0)^d}\right)$

Note: does not depend on i, because $\frac{F_i}{y_i^d} = \frac{F_j}{y_j^d}$.

Since $x_0(z) \neq 0$, $x_0'(w) \neq 0$, we get that Q is regular at

$\mathbb{A}^1 \times \mathbb{A}^1 \subseteq \mathbb{P}^1 \times \mathbb{P}^1$, so Q is a polynomial in ξ_1, ξ_1' $(\in K[\xi_1, \xi_1'])$

We compute: $\deg_{\xi_i}(Q) \leq N \cdot d_i$ (why?)

Moreover, $h(Q) \leq N^2 h(F)$ (by the formula for the height of the product)

So $h(Q) \leq N^2 h(F) \leq N^2\left(c_4 \frac{d_1+d_2}{\gamma} + o(d_1+d_2)\right) \overset{d_1 \geq d_2}{\leq} c_6 \frac{d_1}{\gamma}$

(cont pf)

Now we can apply (3.1), with $P \in Q$, $r_1 \leftarrow N d_1$, $r_2 \leftarrow N d_2$, $\beta_1 \leftarrow \xi_1(\varepsilon)$, $\beta_2 \leftarrow \xi_1'(w)$, $w \leftarrow \varepsilon^2$.

we have to check that

(i) $r_2 = N d_2 \underset{\text{assumption}}{\leq} N \varepsilon^2 d_1 = w r_1$ ✓.

(ii) $h(P) + 4 r_1 \leq N^2 h(F) + 4 r_1 \leq C_6 \frac{d_1}{\gamma} + N d_1 \leq C_7 \frac{d_1}{\gamma}$

and $w r_1 h(\beta_1) = \varepsilon^2 N d_1 h(\xi_1(\varepsilon)) \geq \varepsilon^2 N d_1 \left(\frac{N}{n_g} |z|^2 + O(1) \right) \geq$

$\geq \frac{N^2 d_1}{n_g} \left(\varepsilon^2 |z|^2 + O(1) \right) \geq C_8 \frac{d_1}{\gamma}$ ← because $d_1 |z|^2 \geq \frac{C_5}{\gamma \varepsilon^2} d_1$

and $w r_2 h(\beta_2) \geq C_8 d_1 / \gamma$

By choosing $C_5 >> 0$, we'll get $C_8 > C_7$, s.t

$$h(P) + 4 r_1 \leq C_7 \frac{d_1}{\gamma} \leq C_8 \frac{d_1}{\gamma} \leq w \min \{ r_1 h(\beta_1), r_2 h(\beta_2) \}$$ ✓.

By (3.1), we conclude that one can find (i_1, i_2) s.t

$$\frac{i_1}{r_1} + \frac{i_2}{r_2} \leq 4\sqrt{w} \quad \text{and} \quad \partial_{\underline{i}} P(\beta_1, \beta_2) \neq 0$$

i.e. $\frac{i_1}{d_1} + \frac{i_2}{d_2} \leq 4 N \varepsilon \leq 12 N \varepsilon$ and $\partial_{i_1}^{\xi} \partial_{i_2}^{\xi'} S(z, w) \neq 0$.

Hence $\exists (i_1^*, i_2^*)$ admissible and $\leq (i_1, i_2)$.

In particular, $\frac{i_1^*}{d_1} + \frac{i_2^*}{d_2} \leq 12 N \varepsilon$ as well.

we have then

4) $\frac{i_1^*}{d_1} + \frac{i_2^*}{d_2} \leq 12 N \varepsilon$; So $i_1^* + i_2^* \leq C_5 \varepsilon (d_1 + d_2)$.

Next: (1) – (4) ⇒ Vojta's inequality.

Recall the statement of Vojta's inequality, which we are going to prove:

Thm: $\exists\, \kappa_1 = \kappa_1(C), \kappa_2 = \kappa_2(g)$ s.t. if $z, w \in C(\bar{k})$ with

$|z| \geq \kappa_1$, $|w| \geq \kappa_2 \cdot |z|$, then $\langle z, w \rangle \leq \frac{3}{4} |z| \cdot |w|$.

Proof: Choose $\kappa_1, \kappa_2 \geq 1$, and κ_1 large enough s.t.

$$\mathcal{Z} \cap \{ x \in C(\bar{k}) : |x| \geq \kappa_1 \} = \emptyset$$

(where $\mathcal{Z}$ = all points u s.t. • $\xi_1 - \xi_1(u)$ is not a uniformizer
or
• $(g e_j)_{\xi_1}(u) = 0$ for some $0 \leq j, l \leq n$)

Choose $1 \geq \varepsilon, \nu > 0$, and $D >> 0$ (D will be sent to ∞ at the end).

Ensure that $D > |w|^2$.

Set
$$(*) \begin{cases} d_1 = N \cdot \lfloor \sqrt{g+\nu}\, \frac{D}{|z|^2} \rfloor \\ d_2 = N \cdot \lfloor \sqrt{g+\nu}\, \frac{D}{|w|^2} \rfloor \\ d = N \lfloor \frac{D}{|z||w|} \rfloor \end{cases}$$

and let $\Omega = \Omega(d_1, d_2, d)$. This is a Vojta divisor:

($g d^2 \leq d_1 d_2 \leq g^2 d^2$ (easy to check).)

We'll estimate $h_\Omega(z, w)$. First choose D large enough so that the section in $L(\Omega) \hookrightarrow \mathcal{F} = \{ F_i \}_{0 \leq i \leq m}$

By estimate (2), $h_\Omega(z, w) \geq -h(\mathcal{F}) - c_2 \left(i_1^* |z|^2 + i_2^* |w|^2 \right) - c_3 \left(i_1^* + i_2^* + \delta_1 + \delta_2 + 1 \right)$

for (i_1^*, i_1^*) admissible for $s \hookrightarrow \mathcal{F}$ at (z, w).

Since $\kappa_1, \kappa_2 \geq 1$, then $|z| > 1$ and $|w| > 1$, so we get:

$$(*') \quad h_\Omega(z, w) \geq -h(\mathcal{F}) - c_{11} \left(i_1^* |z|^2 + i_2^* |w|^2 \right) - c_{12} \left(d_1 + d_2 + d \right)$$

Now, let $K_1 > \frac{1}{\sqrt{\varepsilon}}$ and use (*) to obtain:

$$d_1+d_2+d \leq N\cdot D\cdot\left(\frac{\sqrt{g+\nu}}{|z|^2}+\frac{\sqrt{g+\nu}}{|w|^2}+\frac{1}{|z||w|}\right) \underset{|z|,|w|\geq K}{\leq} C_{13}\frac{D}{K_1^2} \leq C_{13}\,\varepsilon D$$

So:

(A) $h_{\mathcal{I}}(z,w) \geq -h(\mathcal{I}) - C_{11}\left(i_1^*|z|^2+i_2^*|w|^2\right) - C_{14}\,\varepsilon D$

To estimate $h(\mathcal{I})$ above, we need $\gamma>0$, ind. of z,w s.t.:

$d_1d_2 - gd^2 \geq \gamma d_1 d_2$.

Note that $\frac{d_1d_2-gd^2}{d_1d_2} = 1-\frac{gd^2}{d_1d_2} \geq 1-\frac{g\left(\frac{D}{|z||w|}\right)^2}{\left(\sqrt{g+\nu}\frac{D}{|z|^2}-1\right)\left(\sqrt{g+\nu}\frac{D}{|w|^2}-1\right)} =$

$$= 1-\frac{g}{g+\nu}\cdot\frac{1}{1-\frac{|z|^2}{D\sqrt{g+\nu}}}\,\frac{1}{1-\frac{|w|^2}{D\sqrt{g+\nu}}} \simeq 1-\frac{g}{g+\nu}(-\delta) \geq \frac{\nu}{3g}$$

For $D\gg 0$, we can choose $\gamma=\frac{\nu}{3g}$, say.

From this we can get some $\mathcal{I}$ with $h(\mathcal{I}) \leq C_{15}(d_1+d_2) \leq C_{16}\,\varepsilon D$ (B)

(we've bounded d_1+d_2+d; using (3)-estimate.)

Substitute (B) into (A), to get:

(C) $h_{\mathcal{I}}(z,w) \geq -C_{11}\left(i_1^*|z|^2+i_2^*|w|^2\right) - C_{17}\,\varepsilon D$

Next, we use estimate (4) (Prop 3.2) to estimate i_1^*, i_2^*:

Let $K_2 \geq \frac{\sqrt{2}}{\varepsilon}$, to obtain $\frac{d_2}{d_1} \leq \frac{N\sqrt{g+\nu}\,D/|w|^2}{N\left(\sqrt{g+\nu}\frac{D}{|z|^2}-1\right)} \overset{D\gg 0}{\leq} \frac{2|z|^2}{|w|^2} \leq \frac{2}{K_2^2} \leq \varepsilon^2$

The second condition for (Prop 3.2) was that for some constant C_{18},

$\min\{d_2|w|^2, d_1|z|^2\} \geq \frac{C_{18}}{\gamma\varepsilon^2}d_1$

Note that $\frac{d_2|w|^2}{d_1|z|^2} = \frac{\left\lfloor\sqrt{g+\nu}\,D/|w|^2\right\rfloor|w|^2}{\left\lfloor\sqrt{g+\nu}\frac{D}{|z|^2}\right\rfloor|z|^2} = \left(1-\frac{\eta_2|w|^2}{D\sqrt{g+\nu}}\right)\left(1-\frac{\eta_1|z|^2}{D\sqrt{g+\nu}}\right)$ for

some $0\leq\eta_1,\eta_2<1$.

Hence, if $D>>0$, $\frac{1}{2} \leq \frac{d_2|w|^2}{d_1|z|^2} \leq 2$

So to check the second condition of Prop 3.2, we need to check $d_1|z|^2 \geq \frac{2C_{18}}{\gamma\varepsilon^2} d_1$, which we can for $K_1 \geq \sqrt{\frac{2C_{18}}{\gamma\varepsilon^2}}$.

Now, (3.2) $\Rightarrow \frac{i_1^*}{d_1} + \frac{i_2^*}{d_2} \leq 4N\varepsilon \Rightarrow i_1^* \leq 4N\varepsilon d_1$, $i_2^* \leq 4N\varepsilon d_2$

Substitute this into (c), to get:

(D) $\boxed{h_\Omega(z,w) \geq -C_{19}\cdot\varepsilon\cdot(d_1|z|^2 + d_2|w|^2) - C_{17}\cdot\varepsilon\cdot D \geq -C_{20}\,\varepsilon\, D}$ (indep. of z,w)

because $d_1|z|^2$, $d_2|w|^2 \leq c'D$.

Now we use (1), to see that $h_\Omega(z,w) \leq \frac{d_1}{g}|z|^2 + \frac{d_2}{g}|w|^2 - 2d\langle z,w\rangle + C_1(d_1+d_2+d) \leq$

Combining it with (D) and noting that $C_1(d_1+d_2+d) \leq C_{21}\varepsilon D$,

get (F) $\frac{d_1}{g}|z|^2 + \frac{d_2}{g}|w|^2 - 2d\langle z,w\rangle \geq -C_{22}\,\varepsilon D$

Multiply by $\frac{1}{D}$, and then let $D \to \infty$. Note that $\lim_{D\to\infty} \frac{1}{D}\lfloor \alpha D\rfloor = \alpha \ \forall \alpha\in\mathbb{R}$

and use def (☆). ★ get:

$$2\frac{\sqrt{g+\nu}}{g} - 2\frac{\langle z,w\rangle}{|z||w|} \geq -C_{23}\,\varepsilon$$

or equivalently, $\langle z,w\rangle \leq \left(\frac{\sqrt{g+\nu}}{g} + \frac{1}{2}C_{23}\varepsilon\right)|z||w|$.

As $g \geq 2$, get $\frac{\sqrt{g+\nu}}{g} < \frac{3}{4}$, and so, as ε is arbitrary,

we get $\langle z,w\rangle \leq \frac{3}{4}|z||w|$.

Theorem: Let K be a number field, and A/K an abelian variety.

If $X \subseteq A$ is a closed subvariety that does not contain any translate of a positive dimensional abelian subvariety, then $X(K)$ is finite.

↖ Lang's conjecture

Idea involved in the proof:

Choose a line bundle X^m ($m \gg 0$, need that $X^m \to A^{m-1}$ is finite)

Take "rational" line bundles in $\mathrm{Pic}(A^m) \otimes \mathbb{Q}$ ($\mathcal{L}(-\varepsilon, s_1, \dots, s_m)$)

(coming from ample line bdles on A (one of the factors) ...)

Metrize these line bundles.

Try to find lower & upper bounds for $h_{\mathcal{L}}$(rational points in X^m), to get a contradiction.

For the lower inequality, we need to replace Siegel's lemma (as used for Vojta's inequality) ← called Faltings' lemma; also, need to replace Roth's lemma by the called "product theorem".

Metrized Line Bundles

Let X/K be a projective variety, and let $\{\sigma : K \hookrightarrow \mathbb{C}\}$ ← embeddings (total of $n = [K:\mathbb{Q}]$)

For each σ, we get an analytic space $X_\sigma = \left(X \times_{K,\sigma} \mathbb{C}\right)(\mathbb{C})^{an}$, and if $\mathcal{E}$ is a vector bundle on X, we get an analytic vector bundle on X_σ.

Def: A hermitian metric on $\mathcal{E}$ over X is, for each $\sigma : K \hookrightarrow \mathbb{C}$, a hermitian metric $\langle \cdot, \cdot \rangle_\sigma$ on $\mathcal{E}_\sigma$ s.t. $\langle \bar{\ }, \bar{\ } \rangle_{\bar{\sigma}} = \overline{\langle \cdot, \cdot \rangle_\sigma}$

($\bar{\ }$ = complex conjugation).

Rk: A hermitian metric on the analytic vector bundle E_σ over X_σ is a continuously varying family of positive-definite hermitian forms on the fiber $(E_\sigma)_x$, $x \in X_\sigma$.

(Equivalently, it's a continuous section of $(\overline{E_\sigma} \otimes E_\sigma)^*$ which is a positive definite hermitian form on each fiber)

Associated to $\langle \cdot, \cdot \rangle_\sigma$ is a norm $\|\cdot\|_\sigma : C(X_\sigma, E_\sigma) \to C(X_\sigma, \mathbb{R}_{\geq 0})$ (continuous sections)

Def: A metrized line bundle on X is an algebraic line bundle, with a hermitian metric, written $(\mathcal{L}, \|\cdot\|_\sigma)$.

Relation with heights:

Let $X \to \mathrm{Spec}(\mathcal{O}_K)$ be projective integral.
By a metrized line bundle on X we mean $\mathcal{L}$ on X a line bundle, together with an hermitian metric on $\mathcal{L}_K$ over X_K.

Example: $X = \mathrm{Spec}(\mathcal{O}_K)$.

$\mathcal{L} \longleftrightarrow$ invertible ideal I of $\mathcal{O}_K$.

The metric: pos.-def. hermitian form on each $I \otimes_{K,\sigma} \mathbb{C}$

Def: Let $\overset{\circ}{s} \in \Gamma(\mathrm{Spec}\, \mathcal{O}_K, \mathcal{L}) = I$. $\deg(\overset{2}{\mathcal{L}}, \|\cdot\|_\sigma) := \log \#(I/sI) - \sum_\sigma \|s\|_\sigma$

This is the Arakelov degree of $\mathcal{L}$ wrt $\|\cdot\|_\sigma$.

Let $C/\mathbb{F}_p$ be smooth, projective. Let $\mathbb{F}_p[C] = \mathcal{O}_C(U) \subseteq \mathbb{F}_p(C)$.

A divisor D on C w/ support $\subseteq U \hookrightarrow$ ideal in $\mathcal{O}_C(U)$, say I.

If $0 \neq s \in I$, then $\deg(D) = \log_p \# I/sI$

Let now $x \in X(\bar{K})$, and $(\mathcal{L}, \|\cdot\|_\sigma)$ on X.
There is K'/K finite s.t. $x \in X(K') = X(\mathcal{O}_{K'})$ (valuative criterion of properness)

i.e. $x : \operatorname{Spec} \mathcal{O}_{K'} \to X$

$\operatorname{Spec} \mathcal{O}_{K'} \to \operatorname{Spec} \mathcal{O}_K$

We can pull-back the metrized line bundle on X to get:
$x^*(\mathcal{L}, \|\cdot\|_\sigma)$, a metrized line bundle on $\operatorname{Spec}(\mathcal{O}_{K'})$.

Define: $h_{(\mathcal{L}, \|\cdot\|_\sigma)}(x) := \frac{1}{[K':\mathbb{Q}]} \deg\left(x^*(\mathcal{L}, \|\cdot\|_\sigma)\right)$.

Theorem: $h_{(\mathcal{L}, \|\cdot\|_\sigma)}$ is a height function for $\mathcal{L}$.

We will prove it now.
First, recall what we've done so far:

$$\begin{array}{ccccc}
\mathcal{L} & \to & \mathcal{X} & \to & \operatorname{Spec} \mathcal{O}_K \\
\uparrow & & \uparrow & & \downarrow \\
 & & X & \to & \operatorname{Spec} K \\
 & & \uparrow & & \uparrow L^* \\
(\mathcal{L}^{hol}, \|\cdot\|_\sigma) & \to & X_\sigma^{an} & \to & \operatorname{Spec} \mathbb{C} = pt
\end{array}$$

Also, note that $(M, \|\cdot\|_\sigma)$ over $\operatorname{Spec} \mathcal{O}_K$ is equivalent to the giving of M a proj. rk-1 module over $\mathcal{O}_K$, + norms on $M \otimes_{K,\sigma} \mathbb{C}$ ($\mathbb{C}$-dim cx vector space)

Let $0 \neq s \in M$. Then $\deg(M, \|\cdot\|) = \log \#(M/\langle s \rangle) - \sum_{\sigma : K \hookrightarrow \mathbb{C}} \log \|s\|_\sigma$

If $(\mathcal{L}, \|\cdot\|_v)$ is a metrized line bundle on $\mathcal{X}$, and $P \in X(\bar{K})$, then we can extend it to $\bar{P} \in \mathcal{X}(\mathcal{O}_{K'})$, for some $[K':K] < \infty$, and set

$$h_{(\mathcal{L},\|\cdot\|_v)}(P) := \frac{1}{[K':\mathbb{Q}]} \deg\left(\tilde{P}^*(\mathcal{L}, \|\cdot\|_v)\right).$$

Proof (that $h_{(\mathcal{L},\|\cdot\|)}$ is a height function for $(X, \mathcal{L})$.)

First, X_v^{an} is a compact analytic space, so any two norms on $\mathcal{L}_v^{an}$ are equivalent (globally).

In particular, can write $\mathcal{L} = \mathcal{L}_1 \otimes \mathcal{L}_2^{-1}$, w/ $\mathcal{L}_1, \mathcal{L}_2$ are very ample, and assume that $\|\cdot\| = \|\cdot\|_1 \cdot \|\cdot\|_2^*$ (a norm on a vectorspace yields another on its dual).

By the height machine, we may as well assume $X = \mathbb{P}^n$, $\mathcal{L} = \mathcal{O}(1)$.

The sections of $\mathcal{O}(1)$ are locally quotients $\frac{F}{G}$, F, G homogeneous poly's in $x_0, \dots, x_n$, and $\deg F - \deg G = 1$.

Define $\left\|\frac{F}{G}\right\|_v([a_0 \cdots a_n]) := \dfrac{|(GF)(a_0,\dots,a_n)|}{|(cG)(a_0,\dots,a_n)|} \cdot \dfrac{1}{\max\limits_{0\le i\le n} |a_i|}$

Claim: $h_{(\mathcal{O}(1),\|\cdot\|_v)} = h_{\mathbb{P}^n}$ = usual logarithmic height.

Pf: We may (by extending the base fields) assume that $P \in \mathbb{P}^n(K) = \mathbb{P}^n(\mathcal{O}_K)$ and $P^* X_0 \neq 0$. is a section of $P^*\mathcal{O}(1)$. Like $\mathbb{Z}/p \simeq \mathbb{Z}\cdot\frac{1}{p}/\mathbb{Z}$

$$\frac{P^*\mathcal{O}(1)}{\langle P^* x_0\rangle} \simeq \frac{\left(\sum \mathcal{O}_K x_i(P)\right)}{\mathcal{O}_K(x_0(P))} \simeq \frac{\left(\sum \mathcal{O}_K \frac{x_i}{x_0}(P)\right)}{\mathcal{O}_K} \subseteq K/\mathcal{O}_K$$

$$\#\frac{P^*\mathcal{O}(1)}{\langle P^* x_0\rangle} = \prod_{v\in M_K^\circ} \max_{i\le n} \left\|\frac{x_i}{x_0}(P)\right\|_v \overset{\text{product formula}}{=} \prod_{v\in M_K^\circ} \max_{i\le n} \|x_i(P)\|_v \cdot \prod_{v\in M_K^\infty} \|x_0(P)\|_v$$

We need only to compute the degree of $P^*\mathcal{O}(1)$ ∎

$$\deg\left(\{P^*(\mathcal{O}(1), \|\cdot\|_i)\}\right) = \sum_{v \in M_k^0} \log \max_{i \le n} \|x_i(P)\|_v + \sum_{v \in M_k^\infty} \log \|x_0(P)\|_v - \sum_{v \in M_k^\infty} \log \left| \frac{\|x_0(P)\|_v}{\max_{i \le n} \|x_i(P)\|_v} \right|$$

$$= [k : \mathbb{Q}]\, h_{\mathbb{P}^n}(P).$$

Differential operators, index, and the product theorem.

will assume for simplicity $\mathrm{char}(k) = 0$.

Def: (1) Let X/k be a variety. A vector field on X is a k-linear derivation

$$D : \mathcal{O}_X \to \mathcal{O}_X.$$

Equivalently, $D \in \Gamma(X, \mathcal{T}_X)$ where $\mathcal{T}_X = \mathcal{H}om(\Omega^1_{X,k}, \mathcal{O}_X)$.

(2) A differential operator on X of degree $\le r$ is a k-linear map

$L : \mathcal{O}_X \to \mathcal{O}_X$ that is locally of the form $\sum f D_1 \cdots D_s$, $s \le r$ where D_i's are vectorfields on X.

Remark: Let $X = X_1 \times \cdots \times X_m$. Then any vectorfield D on X can be written uniquely as $D_1 + \cdots + D_m$, where D_i is a "vectorfield in the i^{th}-direction", which means that its projection to $\prod_{j \ne i} X_j$ is 0.

This is because $\Omega^1_{X/k} \cong \bigoplus_{i=1}^m p_i^* \Omega^1_{X_i/k}$.

Def: (3) $L : \mathcal{O}_X \to \mathcal{O}_X$ is a differential operator of multidegree $\le (r_1, \ldots, r_m)$ if it can be locally expressed as $\sum f D_1 \cdots D_s$, where each D_j is on the direction of some X_i, and at most r_i go in the direction of X_i.

(4) Let $(d_1,\dots,d_m)$ be integers ≥ 0, then L is of weighted degree $\text{wt.deg}_{\underline{d}}(L) \leq r$ if it is locally of multidegree $\leq \underline{r}$, such that $\frac{r_1}{d_1} + \cdots + \frac{r_m}{d_m} \leq r$

(5) Let $\mathcal{L} \to X = X_1 \times \cdots \times X_m$ be a line bundle, and $0 \neq f \in \Gamma(X, \mathcal{L})$. Let $x \in X$ (not necessarily closed), and s a generator of $\mathcal{L}_x$ as a $\mathcal{O}_{X,x}$-module; then $f = g \cdot s$ for some function $g \in \mathcal{O}_{X,x}$. We define $\text{Ind}_{\underline{d}}(f,x) := \max\{\sigma \in \mathbb{Q}_{\neq 0} : L(g)(x) = 0 \text{ if } \text{wt.deg}(L) < \sigma\}$ (independent of the choice of s) and L is defined on a nbhd of x

Example: $X_i = \mathbb{A}^1$, $\mathcal{L} = \mathcal{O}_X$. Get the ordinary order w.r.t. $\underline{d}$ (at closed points).

Def (6) Given $X = X_1 \times \cdots \times X_m$, and $\mathcal{L}$ a line bdle on X, and $f \neq 0$, $\underline{d}$, and $\sigma \in \mathbb{R}$, Define $Z_\sigma := \{x \in X : \text{Ind}(f,x) \geq \sigma\} \subseteq X$ is a closed subscheme, with ideal sheaf locally generated by $L(g)$, w/ $\text{wt.deg } L < \sigma$, $f = g \cdot s$, s a local generator of $\mathcal{L}$.

Remark: if $\sigma' \geq \sigma$, then $Z_{\sigma'} \subseteq Z_\sigma$

Theorem (Product Thm): Suppose $k = \bar{k}$. Let $n_1, \dots, n_m \geq 0$ be integers. Let $\mathcal{P} = \mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_m}$. For every $\varepsilon > 0$, $\exists\, r \in \mathbb{R}$ s.t., If

(1) $(d_1,\dots,d_m)$ satisfies $\frac{d_i}{d_{i+1}} \geq r$

(2) $0 \neq f \in \Gamma(\mathcal{P}, \mathcal{O}(d_1,\dots,d_m))$ ← $\mathcal{O}(d_1,\dots,d_m) = p_1^*\mathcal{O}(d_1) \otimes p_2^*\mathcal{O}(d_2) \otimes \cdots \otimes p_m^*\mathcal{O}(d_m)$

(3) For some σ, Z is an irreducible component of Z_σ and $Z_{\sigma+\varepsilon}$

Then: a) $Z = Z_1 \times \cdots \times Z_m$, $Z_i \subseteq \mathbb{P}^{n_i}$ a closed subscheme.

b) $\deg(Z_i) \leq C(\varepsilon, n_1 + \cdots + n_m)$.

Application: Suppose $N > \dim \mathcal{P}$, and $\mathrm{Ind}(f, x) \geq \sigma$.

Then there is a chain $\mathcal{P} \neq Z_1 \supseteq Z_2 \supseteq \cdots \supseteq Z_N \ni x$,

where Z_i is a component of $(Z_i)_{\sigma/N}$.

Because $N > \dim \mathcal{P}$, $Z_{i+1} = Z_i$ for some i.

We can then apply the product theorem, w/ $\varepsilon = \sigma/N$

(!! σ depends on $\underline{d}$, and $\underline{d}$ depends on σ !! But this can be taken care of).