AWS '23 Notes

Niven Achenjang

March 2023

These are notes on talks given in "Arizona Winter School" which took place at University of Arizona. Unfortunately for the reader, these notes are live-texed and so their quality is upper bounded both by my (quite) limited ability to understand the material in real time and by my typing speed. With that in mind, they are doubtlessly missing content/insight present in the talks and certainly contain confusions not present in the talks. Despite all this, I hope that you can still find some use of them. Enjoy and happy mathing.

The website for this seminar is available here.

Contents

List of Figures

List of Tables

1 Laura DeMarco: Arithmetic dynamics and intersection problems

1.1 Lecture 1 (3/4)

Can think of this series as methods to avoid using model theory. What methods from complex analysis and dynamical systems can be used to give alternative solutions to unlikely intersection problems.

Goal. Introduce methods from (complex) dynamical systems.

We would like to talk about *unlikely* intersections as well as *likely* intersections. Even when we expect intersections to happen/to be common, it is not always easy to prove that they do occur. Topics that will come up will start with

- currents, plurisubharmonic functions in the context of height theory
- equidistribution results.

We're really interested in the dynamics of morphisms $f : \mathbb{P}^N \to \mathbb{P}^N$ over $\mathbb{C}$. Can write these in homogeneous coordinates as a collection

$$f = (f_0 : f_1 : \cdots : f_N)$$

of homogeneous polynomials of some degree d such that $\{f_0 = \cdots = f_N = 0\} = \emptyset \subset \mathbb{P}^N$. From the dynamical point of view it is natural to assume $d > 1$ (automorphisms of $\mathbb{P}^N$ are too easy). We want to study the iterates $f^n = f \circ \cdots \circ f$ as $n \to \infty$.

Definition 1.1.1. The `orbit` of $z_0 \in \mathbb{P}^N$ is the set $\{f^n(z_0)\}_{n\geq 0}$. ◇

Example 1.1.2. Say $N = 1$, and consider the squaring function $f(z) = z^2$ from $\mathbb{P}^1 \to \mathbb{P}^1$. This is one of the only examples that can be described from start to finish.

- The only fixed points are $0, \infty$
- Everything strictly inside the unit circle $S^1 \subset \mathbb{C}$ converges to 0 under iteration, i.e. $|z| < 1 \implies f^n(z) \to 0$. Similarly, $|z| > 1 \implies f^n(z) \to \infty$.
- f preserves the unit circle (as a set). In $\mathbb{C}^\times$, a point z_0 has finite orbit $\iff$ z_0 is a root of unity. Restricted to the unit circle, note that

  $$f\left(e^{2\pi i\theta}\right) = e^{2\pi i(2\theta)}$$

  simply doubles the angle. This (i.e. $f|_{S^1}$) is (an/the simplest) example of a *chaotic* dynamical system. △

Above, note the relationship between the dynamics of f and the group structure (on S^1).

Example 1.1.3 (`Lattès maps`)**.** Say $E/\mathbb{C}$ is an elliptic curve, e.g. $E_t : y^2 = x(x-1)(x-t)$ (fixed $t \in \mathbb{C} \setminus \{0, 1\}$). Take $\varphi : E \to E$ be multiplication by 2, i.e. $\varphi(P) = P + P = 2P$. This fits into a diagram[1]

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E \\ \pi\downarrow & & \downarrow\pi \\ \mathbb{P}^1 & \xrightarrow{f} & \mathbb{P}^1 \end{array}$$

[1]This is related to the fact that $[2]^*\mathscr{O}(0) \simeq \mathscr{O}(40)$, where $0 \in E(\mathbb{C})$ is the identity. Alternatively, its related to the fact that $\varphi(-P) = -\varphi(P)$

Above, $\pi : E \to \mathbb{P}^1$ is the degree 2 map identifying $P \leftrightarrow -P$. Note that $\deg f = 4$. If $E = E_t$, then $\pi_t(x, y) = x$ and

$$f_t(x) = \frac{(x^2 - t)^2}{4x(x-1)(x-t)}.$$

These are called Lattés examples. He studied them because they are chaotic on all of $\mathbb{P}^1$, e.g. their periodic points are dense on all of $\mathbb{P}^1$. Indeed, note that a point $P \in E$ has finite orbit under $\varphi \iff P$ is torsion $\iff \pi(P) \in \mathbb{P}^1$ has finite orbit for f. From this one sees that the preperiodic points of f are dense in $\mathbb{P}^1$, and what's called the *Julia set* (or *chaotic set*) of f is all of $\mathbb{P}^1$. △

Definition 1.1.4. A point with finite orbit is said to be `preperiodic`. ⋄

More generally, we say a map on $\mathbb{P}^N$ is Lattès if it arises from this type of construction.

Definition 1.1.5. A map $f : \mathbb{P}^N \to \mathbb{P}^N$ is `Lattés` if there exists some abelian variety A, and some endomorphism $\varphi \in \mathrm{End}(A)$ making

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & A \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ \mathbb{P}^N & \xrightarrow{f} & \mathbb{P}^N \end{array}$$

commute, where π is a quotient $A \twoheadrightarrow A/G \cong \mathbb{P}^N$ for some finite $G \subset \operatorname{Aut} A$. ⋄

Warning 1.1.6. Such examples are rare in higher dimensions, so much so that people rarely study them when $N > 1$. •

Question 1.1.7 (Audience)**.** *If you have an endomorphism on $\mathbb{P}^N$ which have a dense set of preperiodic points, does it have to be a Lattes map?*

Answer. No. Maps whose (pre)periodic points are dense are surprisingly common (in the sense of moduli, e.g. they have positive Lebesgue measure in the space of coefficients, if I heard correctly), but most are not Lattès maps. ⋆

Remark 1.1.8 (Fakhruddin). Consider $\varphi : A \to A, P \mapsto 2P$ of any abelian variety. Then, there is an embedding $A \hookrightarrow \mathbb{P}^M$ so that φ extends to a morphism of $f : \mathbb{P}^M \to \mathbb{P}^M$. ○

Can get this e.g. by choosing any symmetric, very ample line bundle on A

(Laura said more about how this let's you encompass some standard conjectures involving abelian varieties (e.g. uniformity questions) inside of standard conjectures about dynamical systems, but I missed the deats).

1.1.1 Canonical measures

Theorem 1.1.9 (Lyubich, Mañé, Briend-Duval)**.** *Given $f : \mathbb{P}^N \to \mathbb{P}^N$ of degree $d > 1$ over $\mathbb{C}$, there exists a unique probability measure μ_f on $\mathbb{P}^N(\mathbb{C})$ such that*

- $\mu_f(V) = 0$ *for any proper subvariety $V \subsetneq \mathbb{P}^N$*
- *Note that d^N is the topological degree of f, i.e. points have d^N preimages. We require*

$$\frac{1}{d^N} f^* \mu_f = \mu_f.$$

- *This μ_f is the unique measure of maximal entropy.*

What is the pullback of a measure? Usually, you can pushfoward a measure – via

$$f_*\mu(S) := \mu(f^{-1}(S))$$

– but you typically can't pull one back. In this particular case, f is finite degree and is almost everywhere a submersion, so things are nice to pullback. One way of definite the pullback is via integration:

Remember: (TODO: look up correct statement) The space of measures is dual to the space of continuous functions

$$\int g(f^*\mu) = \int \left(\sum_{f(x)=y} g(x) \right) \mu(y).$$

Let's end by observing that

$$f_*\mu_f = \mu_f.$$

Exercise. Convince yourself this is true, and follows from the pullback relation.

Example 1.1.10. $f(z) = z^2$ on $\mathbb{P}^1$. The chaotic set here is S^1. In this case, μ_f is the Haar measure on S^1. △

Example 1.1.11. Say $f : \mathbb{P}^1 \to \mathbb{P}^1$ is Lattes map for $E \xrightarrow{[2]} E$. In this case, $\mu_f = \pi_*\mu_E$, where μ_E is the Haar measure on E and $\pi : E \to \mathbb{P}^1$ is the quotient map. △

Goal of second lecture is to give us some of the analytic tools needed to connect complex analysis to the theory of height functions.

1.2 Lecture 2 (3/5)

Let $f : \mathbb{P}^N \to \mathbb{P}^N$ be a morphism defined over $\mathbb{C}$. Recall this means that

$$f = (f_0 : \cdots : f_N)$$

with coordinate functions homogeneous polynomials of degree $d > 1$.

Assumption. Actually, for today, say f is defined over $\overline{\mathbb{Q}}$.

Let's define the canonical height attached to f. Start with $h : \mathbb{P}^N(\overline{\mathbb{Q}}) \to \mathbb{R}$, the absolute logarithmic Weil height. The canonical height $\widehat{h}_f$ will measure the growth of h along oribts. Specifically,

$$\widehat{h}_f(\alpha) := \lim_{n\to\infty} \frac{h(f^n(\alpha))}{d^n}.$$

This was introduced by Call-Silverman in 1994. This is a well-defined function (i.e. the limit exists) and

- $\exists C = C(f)$ such that $\left| h - \widehat{h}_f \right| \leq C$ (for all $\alpha \in \mathbb{P}^n(\overline{\mathbb{Q}})$)
- $\widehat{h}_f(\alpha) = 0 \iff \alpha$ is preperiodic (has finite orbit)

  Proof. The $\Longleftarrow$ direction follows directly from the definition of $\widehat{h}_f$ (the numerator in the limit is bounded). For the converse, use Northcott. If $\widehat{h}_f(\alpha) = 0$, then $\widehat{h}_f(f^n(\alpha)) = 0$ for all $n \geq 1$ (in general, $\widehat{h}_f(f(\beta)) = d\widehat{h}_f(\beta)$), so $\{f^n(\alpha)\}_{n\geq 0}$ is a set of points (defined over a fixed number field) of bounded height. Northcott (1950) observed that there are only finitely many points of bounded height (+ bounded degree over $\mathbb{Q}$), so α must have finite orbit. ∎

Remark 1.2.1. Apparently Northcott proved his theorem in order to study dynamics. In particular, to prove that the set of preperiodic points is finite (because it's of bounded height). ◦

Example 1.2.2. $f(z) = z^2$ on $\mathbb{P}^1$. For this example, one can directly compute $\widehat{h}_f = h$, the standard logarithmic Weil height already behaves nicely w/ taking powers. △

Example 1.2.3. Lattès example on $\mathbb{P}^1$

$$\begin{tikzcd} E \arrow[r, "\varphi"] \arrow[d, "\pi"'] & E \arrow[d, "\pi"] \\ \mathbb{P}^1 \arrow[r, "f"] & \mathbb{P}^1 \end{tikzcd}$$

In this case, $\widehat{h}_f(\pi(P)) = (\text{constant})\widehat{h}_E(P)$ where $\widehat{h}_E$ is the Néron-Tate height (attached to $\pi^*\mathscr{O}(1)$?). △

1.2.1 Local heights

Say $\alpha \in K$, a number field. Then,

$$h(\alpha) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \log \max\{1, |\alpha|_v\}$$

(where $n_v = [K_v, \mathbb{Q}_p]$?). Note how this decomposes into a bunch of local terms, attached to each place.

Let's look at an archimedean place (e.g. $K = \mathbb{Q}$ and $v = \infty$). Set $\log^+(z) := \log \max\{1, z\}$. Then, the local function here is $V(z) := \log^+|z|$. This is both continuous and `subharmonic`. Recall from complex analysis that harmonic functions are equal to their averages over circles. For subharmonic functions, one requires

$$V(z_0) \le \frac{1}{2\pi} \int_0^{2\pi} V\left(z_0 + re^{i\theta}\right) \mathrm{d}\theta$$

(`sub-mean value property`). Equivalently,

$$\Delta V \ge 0$$

(Take Laplacian in the sense of distributions). Recall that $\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}$. Since V is not necessarily C^2, this condition really means that

$$\int V \Delta\varphi \mathrm{d}x\mathrm{d}y \ge 0$$

for all smooth $\varphi : \mathbb{C} \to \mathbb{R}_{\ge 0}$ w/ compact support.

Recall $V(z) = \log^+|z|$ is subharmonic (recall $\log z$ is harmonic away from 0). I missed some stuff, but

$$\frac{1}{2\pi} \Delta V \mathrm{d}x\mathrm{d}y = m_{S^1}$$

turns out to be the Haar probability measure on the unit circle.

Exercise. Prove/compute this.

Recall that $h = \widehat{h}_f$ for $f(z) = z^2$. Also recall that the unit circle S^1 was the Julia/chaotic set for this f. Finally, recall that the canonical measure μ_f was this Haar probability measure m_{S^1}. The dynamical canonical measure, for this example, coincides with the Laplacian of the local height function for this canonical height. This generalizes.

Recall 1.2.4 (Last time)**.** Say $f : \mathbb{P}^N \to \mathbb{P}^N/\mathbb{C}$ of degree $d > 1$. There is a unique probability measure μ_f s.t.

- $\mu_f(V) = 0$ for all subvarieties
- $\frac{1}{d^N} f^* \mu_f = \mu_f$ ⊙

We want to say a bit about how this is constructed from a dynamical point of view.

Recall 1.2.5. We ultimately want to describe tools from complex dynamics which have been useful in unlikely intersection problems. One of the main tools is these height functions/canonical measures. ⊙

Laura thinks of heights as (families of) metrics on certain line bundles.

It's convenient to pick coordinates. Write $f = (f_0, \ldots, f_N)$ as a tuple of homogeneous polynomials of degree d. This lifts f to a map F on $\mathbb{C}^{N+1} \setminus \{0\}$. Let $\tau : \mathbb{C}^{N+1} \setminus \{0\} \to \mathbb{P}^N$ be the usual projection.

Remark 1.2.6. F behaves dynamically kinda like the squaring function. E.g. it has a `totally invariant fixed point` at 0, i.e. $F(0) = 0 = F^{-1}(0)$. ○

Consider

$$G_F(z) := \lim_{n\to\infty} \frac{1}{d^n} \log \|F^n(z)\| \text{ for any } z \in \mathbb{C}^{N+1}.$$

We would take any norm, but we'll fix the following choice

$$\|(z_0, \ldots, z_N)\} := \max\{|z_0|, \ldots, |z_N|\}.$$

Note that $G_F(0) = -\infty$. However, G_F is continuous and plurisubharmonic on $\mathbb{C}^{N+1} \setminus \{0\}$. What is a plurisubharmonic function? A function $V : \Omega \to \mathbb{R} \cup \{-\infty\}$ ($\Omega \overset{\text{open}}{\subset} \mathbb{C}^m$) is said to be `plurisubharmonic` (`psh`) if it is upper semi-continuous and is subharmonic on every $\Omega \cap L$ for complex lines $L \hookrightarrow \mathbb{C}^M$.

Warning 1.2.7. plurisubharmonic is not the same as subharmonic as a function on $\mathbb{R}^{2m}$. The latter is about averages on spheres, while the former is about averages on circles. It's harder to be plurisubharmonic. •

Example 1.2.8. $\log|z|$ is subharmonic since we allow $-\infty$ in the values of our functions. In general, the (-1)-set of a psh function can play an important role. △

An equivalent definition for psh is that $\mathrm{dd}^c V \geq 0$ in the sense of distributions.

Remark 1.2.9. In the theory of complex geometry, we can write $\mathrm{d} = \partial + \overline{\partial}$, where ($M$ is dimension of manifold)

$$\partial g = \sum_{j=1}^{M} \frac{\partial g}{\partial z_j} \mathrm{d}z_j \text{ and } \overline{\partial} g = \sum_{j=1}^{M} \frac{\partial g}{\partial \overline{z}_j} \mathrm{d}\overline{z}_j.$$

This is the d appearing above. d^c is slightly nonstandard, but the normalization Laura prefers is $\mathrm{d}^c = \frac{1}{2\pi i}(\partial - \overline{\partial})$. The normalization is so that d^c is a real operator. ○

Example 1.2.10. In the one dimensional case, we said $\frac{1}{2\pi}\Delta V \mathrm{d}x\mathrm{d}y = m_{S^1}$ for $V(z) = \log^+|z|$. Actually, $\mathrm{dd}^c V = \frac{1}{2\pi}\Delta V \mathrm{d}x\mathrm{d}y$. △

When we say $\mathrm{dd}^c V \geq 0$, we really means that it is a "positive (1,1)-current."

Anyways, recall we had lifted f to $F : \mathbb{C}^{N+1} \to \mathbb{C}^{N+1}$ and then formed G_F, which we claimed was plurisubharmonic. Hence, $\mathrm{dd}^c G_F$ is a positive (1,1)-current. By definition, on the fibers of $\mathbb{C}^{N+1} \setminus \{0\} \xrightarrow{\tau} \mathbb{P}^N$, G_F is just the logarithm function, and so is harmonic. Since $\mathrm{dd}^c G_F$ measure failure of being harmonic, it doesn't see those lines. The upshot is that there is a unique positive (1,1)-current T_f on $\mathbb{P}^N$ such that $\tau^* T_f = \mathrm{dd}^c G_F$. In the case of a 1-dimensional dynamical system, $T_f = \mu_f$ (measures are (1,1)-objects in this case). In higher dimensions, measures are (N, N)-forms. In general, $\mu_f = T_f \wedge \cdots \wedge T_f$.

Warning 1.2.11. Such wedge projects are not defined in general for currents (if I heard correctly). See notes for how to make sense of it here. •

Remark 1.2.12 (Response to Audience Question). Sounds like you can alternatively describe T_f as the limit as pulling back the Fubini-Study metric on $\mathbb{P}^N$ along iterations of f (and dividing by $1/d^n$?), and that this limit exists only as a current, not as a metric/volume form. ◦

1.3 Lecture 3 (3/6)

The theme for today is families.

An `algebraic family of maps` on $\mathbb{P}^N$ is a B-morphism

$$f : B \times \mathbb{P}^N \longrightarrow B \times \mathbb{P}^N,$$

where, say, B is a quasi-projective algebraic curve. Hence, for eacy $b \in B(\mathbb{C})$, get morphism $f_b : \mathbb{P}^N \to \mathbb{P}^N$.

What's special in this dynamical world? Here, `special points` $\leftrightarrow$ preperiodic points. A `special subvariety` $\leftrightarrow$ `preperiodic subvariety` (this means $f^n(V) = f^m(V)$).

Remark 1.3.1. The neighborhoods below are analytic neighborhoods. ◦

We want to define stability (see notes for many more definitions). To keep life simple, say $N = 1$, so we have $f : B \times \mathbb{P}^1 \to B \times \mathbb{P}^1$. Say that f is `periodic-point stable` at $b_0 \in B$ if in a neighborhood of b_0, we can parameterize these periodic points, and there are no collisions. Alternatively, say that f is `critically stable` at $b_0 \in B$ if in a neighborhood of b_0, a certain current $\widehat{T}_f \wedge [\mathrm{Crit}(f)] = 0$ vanishes. Here, $\mathrm{Crit}(f)$ is the hypersurface of critical points, where the Jacobian determinant vanishes, and $[\mathrm{Crit}(f)]$ is the corresponding current of integration.

Remark 1.3.2. For each $b \in B$, $f_b : \mathbb{P}^1 \to \mathbb{P}^1$ will have $2d-2$ critical points, e.g. by Riemann-Hurwitz. ◦

The $\widehat{T}_f$ is a certain positive (1,1)-current on $B \times \mathbb{P}^1$, similar to the T_f from yesterday, which exists in the whole family. Note, in dimension one, $\widehat{T}_f|_{\{b\}\times\mathbb{P}^1} = \mu_f$ is a measure.

Remark 1.3.3. $\widehat{T}_f \wedge [\mathrm{Crit}(f)]$ is a measure supported on $\mathrm{Crit}(f)$ which detects intersections with $\operatorname{supp} \mu_f$. ◦

Theorem 1.3.4. *critically stable = periodic-point stable*

In practice, critical stability is the only condition which one can check.

This theorem was proved originally by Mañé-Sad-Sullivan and Lynbich, independently, both in '83.

Example 1.3.5. Consider $f_b(z) = z^2 + b$ for $b \in \mathbb{C}$. This is the family giving rise the famous Mandelbrot set (Laura drew this on her slide). This is the set

$$\mathcal{M} = \{b \in \mathbb{C} : J(f_b) := \operatorname{supp} \mu_{f_b} \text{ is connected}\}$$

($J(f_b)$ is `Julia set`). It is exactly the topological boundary of the Mandelbrot where stability fails. That is, stability $\iff$ $b_0 \notin \partial\mathcal{M}$, "the boundary is the bifurcation locus for this family."

As you move around e.g. the main cardiod of the Mandelbrot set (where e.g. $b_0 = 0$ is), you can follow the periodic point upstairs. However, when you reach the boundary, some pair of periodic points will collide. △

Example 1.3.6 (Lattès family)**.** Say we have an elliptic surface $\mathcal{E} \to B$, and fit this in

$$\begin{tikzcd} \mathcal{E} \arrow[rr] \arrow[dr] & & B \times \mathbb{P}^1 \arrow[dl] \\ & B & \end{tikzcd}$$

Choose some endomorphism $\mathcal{E} \to \mathcal{E}$ (e.g. multiplication by [2]). This will induce a family $f : B \times \mathbb{P}^1 \to B \times \mathbb{P}^1$. In this case, b/c coming from a group, no collisions of periodic points. This is an example which is stable on all of B. The critical values in this example are the images of 2-torsion points (at least, when your endomorphism is [2]). △

Theorem 1.3.7 (McMullen, 1987)**.** *If $f : B \times \mathbb{P}^1 \to B \times \mathbb{P}^1$ is an algebraic family of maps, and if f is stable on all of B, then*

- *f is isotrivial; or*
- *f is a Lattès family.*

Theorem 1.3.8 (MSS,L)**.** *Stability is an open and dense condition in B.*

Remark 1.3.9 (Response to audience question)*.* These theorems hold in any dimension. The McMullen theorem is only for algebraic families, but the MSS,L one is for any complex manifold base. ∘

Theorem 1.3.10 (Dujardin-Favre, D.)**.** *Say $f : B \times \mathbb{P}^1 \to B \times \mathbb{P}^1$ is an algebraic family. Assume f is not isotrivial. Take any algebraic curve $C \subset B \times \mathbb{P}^1$. Then, $\widehat{T}_f \wedge [C] = 0$ if and only if C is a preperiodic curve.*

Let's see an already well-known consequence of this statement. Say $\mathcal{E} \to B$ is an elliptic surface over B (in particular, this map is smooth). Following torsion points in fibers gives the Betti foliation. The only algebraic leaves of this (holomorphic) foliation are the torsion leaves. One way to see this is as a consequence of the above theorem.

1.4 Lecture 4 (3/7)

We been introduced to various idea coming from complex dynamics. In practice, when using dynamical techniques to prove cases of Zilber-Pink, we need to combind these complex idea with arithmic ideas, such as arithmetic equidistribution. We want to state a really powerful version of this.

1.4.1 Arithmetic Equidistribution

This is really many different theorems. The initial versions come from work in the late 1990s of Szpiro-Ullmo-Zhang (AVs/$\overline{\mathbb{Q}}$), Bilu ($\mathbb{G}_m^n/\overline{\mathbb{Q}}$), Rumely ($\mathbb{A}^1/\overline{\mathbb{Q}}$), etc. This all led up to a version we'll talk about today appearing in a manuscript of Yuan-Zhang, posted in a 2021 preprint.

Theorem 1.4.1. *Let X be a quasi-projective, smooth algebraic variety over a number field K. Let $N = \dim X$. Let $h : X(\overline{K}) \to \mathbb{R}$ be a height function w/ lots of good properties. If $\{x_n\} \subset X(\overline{\mathbb{Q}})$ is a* `generic sequence of poinsts` *– i.e. no subsequence is contained in a proper algebraic subvariety – and suppose $h(x_n) \xrightarrow{n\to\infty} h(X) := \underbrace{\overline{\mathcal{L}} \cdot \ldots \cdot \overline{\mathcal{L}}}_{n+1}$, a top intersection number of some metrized line bundle ("minimal value"). Then,*

$$\frac{1}{\#} \sum_{x \in \mathrm{Gal}(\overline{K}/K)\cdot x} \delta_x \longrightarrow \mu_h$$

converges to some probablity measure μ_h on $X(\mathbb{C})$.

Example 1.4.2. Standard logarithmic Weil height on $\mathbb{P}^N(\overline{\mathbb{Q}})$. △

Example 1.4.3. Dynamical canonical heights $\widehat{h}_f$ for maps $f : \mathbb{P}^N \to \mathbb{P}^N/\overline{\mathbb{Q}}$. Here, the limit measure is the canonical measure μ_f. In this case $h(\mathbb{P}^N) = 0$, the minimal value is 0 and achievable. △

In these examples, h is the height for some metrized line bundle $\overline{\mathscr{L}}$, i.e. $\mathscr{L}$ is equipped w/ a family of metrics $\{|\cdot|_v\}$, one for each place of K. Given this, the height of a point $\alpha \in X(\overline{K})$ is (something like)

$$h(\alpha) = \frac{1}{[K(\alpha) : K]} \sum_v n_v(-\log |s(\alpha)|_v),$$

where s is a locally defined section of $\mathscr{L}$. At each place, can define "curvature form" $c_1(\overline{\mathscr{L}})_v = dd^c(-\log |s(z)|_v)$ in local coordinates (on $X(\mathbb{C})$ if v is archimedean. Use Berkovich spaces otherwise, but let's ignore that). One wants $c_1(\overline{\mathscr{L}}) \geq 0$ in the sense of distributions, i.e. it should be a positive (1,1)-current.

Example 1.4.4. For dynamical systems on $\mathbb{P}^N$, $c_1(\overline{\mathscr{L}}) = T_f$ ($\overline{\mathscr{L}}$ metrized line bundle associated to $\widehat{h}_f$). Furthermore, the canonical measure $\mu_f := c_1(\overline{\mathscr{L}}) \wedge \cdots \wedge c_1(\overline{\mathscr{L}})$. △

(This line bundle perspective on canonical heights was first introduced by Shou-Wu Zhang)

In dynamical case, over $\mathbb{C}$, certain equidistribution results were already known. For example

$$\frac{1}{\#} \sum_{x \in \mathrm{Per}_n} \delta_x \longrightarrow \mu_f$$

(Per_n = all points satisfying $f^n(x) = x$) was already known. This was first proved by Briend-Duval.

However, if your map was defined over $\overline{\mathbb{Q}}$, the arithmetic statement Theorem 1.4.1 is even stronger. You can take points w/ heights tending towards 0 instead of with height 0 (i.e. instead of only (pre)periodic points). Also, even if you just take peridioc points of period n (as $n \to \infty$), you *don't have to take all of them.* It's enough to take some Galois-stable subsets.

1.4.2 Example Problem

Laura first saw this problem in a 2007 paper of Bogomolov-Tschinkel, which was developed into a conjecture in a later paper of Bogomolov-Fu-Tschinkel (preprint 2017).

Let E_1, E_2 be two elliptic curves/$\mathbb{C}$. Want to compare geometry of torsion points in E_1 to those in E_2. Project both down to $\mathbb{P}$ in the usual way; call maps $\pi_1, \pi_2 : E_1, E_2 \rightrightarrows \mathbb{P}^1$ (choose coordinates on $\mathbb{P}^1$ arbitrarily). They were interested in providing bounds on $\pi_1(E_1^{\mathrm{tors}}) \cap \pi_2(E_2^{\mathrm{tors}})$.

Observation 1.4.5 (the first one they made). This is a finite intersection unless $E_1 = E_2$ and $\pi_1 = \pi_2$. By this, we really mean, there's an isomorphism $\varphi : E_1 \to E_2$ such that

$$\begin{tikzcd} E_1 \arrow[rr, "\varphi"] \arrow[dr, "\pi_1"'] & & E_2 \arrow[dl, "\pi_2"] \\ & \mathbb{P}^1 & \end{tikzcd}$$

commutes (want an isomorphism since $\deg \pi_1 = \deg \pi_2$).

The moduli space of pairs $\{(E_1, \pi_1), (E_2, \pi_2)\}$ is 5-dimenional. 1-dimensional space of E_1's, 1-dimensional space of E_2's, and 3-dimensional space of maps to $\mathbb{P}^1$ ($3 = \dim \mathrm{PGL}_2$).

Theorem 1.4.6 (Poineau 2022, Kühne 2021, Gao-Ge-Kühne 2021, D.-Kriegu-Ye, D.-Mavraki)**.** *Uniform bounds on the size of these intersections exist.*

The (recent) proof by DeMarco-Mavraki is based on the sort of ideas she has sketched in these aws lectures.

Why is $I := \pi_1(E^{\text{tors}}) \cap \pi_2(E_2^{\text{tors}})$ finite? Use Manin-Mumford conjecture (e.g. version proved by Raynaud) in the following way. Consider abelian surface $A = E_1 \times E_2$ with its degree 4 projection $\pi = (\pi_1, \pi_2) : E_1 \times E_2 \to \mathbb{P}^1 \times \mathbb{P}^1$. The intersection of the projection of the torsion points are the torsion points in A which project to the diagonal in $\mathbb{P}^1 \times \mathbb{P}^1$. Let $C = \pi^{-1}(\Delta)$. Then, elements of I correspond to torsion points of A in C. If C is not special, then this is a finite number (by Raynaud). One can use Riemann-Hurwitz to show that C is irreducible and $g(\widetilde{C}) \geq 2$ unless the branch points of π_1 are the same as the branch points of π_2 (note $g(\widetilde{C}) = 1$ if C it a torsion coset) $\iff$ $E_1 \cong E_2$ compatibly with π_1, π_2.

The above was the perspective of Bogomolov-Tschinkel. Let's give an alternative argument as well.

Proof of finiteness of I, using equidistribution. Suppose first that E_1, E_2 are defined over $\overline{\mathbb{Q}}$. The points of I are preperiodic for a pair of Lattès maps $f_1, f_2 : \mathbb{P}^1 \to \mathbb{P}^1$. Thus, $\widehat{h}_{f_1}(\alpha) = 0 = \widehat{h}_{f_2}(\alpha)$ for all $\alpha \in I$. If I is infinite, then it is generic, so Theorem 1.4.1 tells us that the Galois orbits of these points equidistribute w.r.t. two measures, μ_{f_1} and μ_{f_2}, so $\mu_{f_1} = \mu_{f_2}$. Now, these measures know the branch points of the corresponding curves. Indeed, Recall $\mu_{f_i} = \pi_{i,*}\mu_E$ $(i = 1, 2)$ with E the Lebesgue measure upstairs, so μ_{f_1} is extra concentrated near the branch points. Thus, π_1, π_2 must have the same branch points, so $E_1(\mathbb{C}) \cong E_2(\mathbb{C})$ compatibly over $\mathbb{P}^1$.

What if E_1, E_2 are define over $\mathbb{C}$ instead? Spread out to a family of elliptic curves over $\overline{\mathbb{Q}}$. The intersection points will spread out over the family. It's a Lattes family, so no collision. Specialize to a $\overline{\mathbb{Q}}$ fiber and run above argument there. ■

See notes for sketch of proof by D.-Mavraki. Also, we'll note that their proof was crucially based on ideas by an earlier paper of Mavraki-Schmidt. Another key ingredient is that Theorem 1.4.1 holds when X is quasi-projective, not necessarily proper.

Remark 1.4.7. In fact, via complex-dynamical argument (via stability), one can prove that $\#\pi_1(E^{\text{tors}}) \cap \pi_2(E_2^{\text{tors}}) \geq 5$ for a Zariski dense in the (5-dimensional) moduli space of $\{(E_1, \pi_1), (E_2, \pi_2)\}$. ○

Open Question 1.4.8. *Is this optimal? Is there a Zariski open where the intersection always has size* > 5*?*

Sounds like Laura thinks it might be.

Sounds like Fu and Stoll have an example where they product such an intersection of size 34.

2 Jonathan Pila: Point-counting and applications

2.1 Lecture 1 (3/4)

We want to talk about point counting and its application to diophantine problems. In order to get to the diophantine stuff as soon as possible, we'll postpone a discussion of model theory/o-minimality until lecture 3.

In algebraic geometry, one has a good understanding of when a curve can only have finitely many rational points (e.g. Faltings). In higher dimensions, have conjectures of Bombieri and Lang. We want to talk about something that's a bit analogous.

Example 2.1.1. All solutions to $w^5 + x^5 = y^5 + z^5$ has only trivial solutions, $\{w, x\} = \{y, z\}$. This is a conjecture.

What's known is that the trivial solutions outnumber the non-trivial ones. We first define the `height` of a rational number $q = a/b$ to be $H(q) = \max(|a|, |b|)$. If you take integers up to height H, get roughly H^2 trivial solutions.

Theorem 2.1.2. *For $\varepsilon > 0$, $H \geq 1$, there are $\ll_\varepsilon H^{13/8+\varepsilon}$ nontrivial solutions.*

(Somehow related to a Warring problem). Observe that $13/8 < 2$. △

A Bombieri-Lang type conjecture would say that there are only finitely many solutions outside the geometrically defined set $\{x = y \text{ and } z = w\} \cup \{x = z \text{ and } y = w\}$.

2.1.1 Analogue for certain, non-algebraic sets

The non-algebraic sets will be definable sets in certain structures defined in the *real numbers*, in particular in $\mathbb{R}^n$.

Let's first consider the case of curves (= real dimension 1).

Theorem 2.1.3. *Let $f(x)$ be a non-algebraic function that is real analytic on $[0, 1]$. Let $X \subset \mathbb{R}^2$ be the graph of a function. Choose $\varepsilon > 0$. Then, there is a constant $c(f, \varepsilon)$ such that*

$$N(X, H) \leq c(f, \varepsilon)H^\varepsilon,$$

where

$$N(X, H) = \#\left\{x \in X \cap \mathbb{Q}^2 : H(x) \leq H\right\},$$

where $H(x)$ is the maximum height of the coordinates of x.

This of this theorem as saying that X has only "few rational points."

Proof Sketch. Want to subdivide $[0, 1]$ into smaller intervals, say of length L, so that all rational points on the graph above the subdivision must be contained in some algebraic curve of degree d (independent of L). We want L chosen so that H^ε such subintervals cover $[0, 1]$. Since f is a non-algebraic function, it'll intersect an algebraic curve in a small set.

Given ε, choose d so that $8/(d + 3) < \varepsilon$. Set $D = d + 1$, the number of degree d monomials in two variables. Consider functions $x^a f(x)^b$ with $0 \leq a, b \leq a + b \leq d$. There are D such functions. Above $[0, L]$, consider all points of $X \cap \mathbb{Q}^n$ up to height H, and suppose we have D of them $x_1, \ldots, x_D$. Let

$$\Delta := \det\bigl(x_1^a f(x_1)^b\bigr)_{a+b=d}$$

(a $D \times D$ matrix).

Theorem 2.1.4 (H.A. Schwarz, 1880's)**.** $\Delta = V(x_1, \dots, x_D)\det\left(i - 1_j^{(\varphi)}(\xi_{ij})/(i-1)!\right)$ *where* $\Delta := \det(\varphi_j(x_i))$*. The* $V(-)$ *is a vandermonde determinant, so of size* $L^{D(D-1)/2}$*. The right factor is independent of* x *(?)*

Somehow (involving reasoning about rows of matrices and denominators?), one concludes that if $|\Delta| \le \frac{1}{H^{2dD}}$, then $\Delta = 0$. In our application, if $L \asymp H^{-8/(d+3)}$, then $\Delta = 0$, so every point of height H will lie on one curve of degree D. In each subinterval, have $X \cap C_d$ (C a degree d algebraic curve), which is a finite intersection since X is non-algebraic. The size of this intersection is bounded independent of the curve, $\#X \cap C_d < c(f, d)$. ■

Let's look at higher dimensional sets $X \subset \mathbb{R}^n$. Say $f : [0,1]^k \to \mathbb{R}^n$ is analytic.

Definition 2.1.5. A `semi-algebraic set` in $\mathbb{R}^n$ is a finite union of sets, each defined by finitely many equations/inequalities w/ real coefficients. ⋄

Example 2.1.6. Open balls in $\mathbb{R}^n$ are semi-algebraic, $x_1^2 + \cdots + x_n^2 < r$. △

Definition 2.1.7. For a set $X \subset \mathbb{R}^n$, its `algebraic part` X^{alg} is the union $\bigcup A$ of all connected, positive dimensional semi-algebraic $A \subset X$. Its `transcendental part` $X^{\text{trans}} := X \setminus X^{\text{alg}}$. ⋄

Theorem 2.1.8 (Pila-Wilkie)**.** *Let* $X \subset \mathbb{R}^n$ *be definable (e.g.* $X = \operatorname{im} f$*), and choose* $\varepsilon > 0$*. Then, there exists a constant* $c(X, \varepsilon)$ *such that*

$$N(X^{trans}, H) \le c(X, \varepsilon) H^{\varepsilon}.$$

by which we mean definable in an o-minimal structure, more on this in a later lecture

2.1.2 Diophantine Application

Let's end w/ a Diophantine application (we'll talk about a true unlikely intersection problem tomorrow).

Warning 2.1.9. We're about to talk about complex algebraic sets, so dimension will mean $\mathbb{C}$-dimension. •

Question 2.1.10 ("Toy problem of Lang")**.** *Let* F *be a Laurent polynomial in two variables, i.e. element of* $\mathbb{C}[X, X^{-1}, Y, Y^{-1}]$*. Let*

$$V = \left\{(x, y) \in (\mathbb{C}^\times)^2 : F(x, y) = 0\right\}.$$

We want to consider points of V *that are torsion points in* $(\mathbb{C}^\times)^2$*, i.e.* (ζ, η) *roots of unity.*

In paper discussing this, Lang gives proofs of following theorem (which he says are due to the people indicated)

Theorem 2.1.11 (Ihara,Serre,Tate)**.** *The number of points is finite, unless* F *is of the form* $x^n y^m = \zeta$ *where* $n, m \in \mathbb{Z}$ *(not both* 0*) and* ζ *is a root of unity.*

Such exceptional cases $x^n y^m = \zeta$ are "torsion cosets" (translate of a subgroup, irreducible if $\gcd(n, m) = 1$).

Theorem 2.1.12. *Let* $V \subset X = (\mathbb{C}^\times)^n$*. Let* X_{tors} *be the torsion points (i.e. those w/ coordinates all roots of unity). Note that the algebraic subgroups are all defined by conditions of the form*

$$x^{k_1} \dots x_{k^n} = 1$$

(get a `torsion coset` *if you replace* 1 *w/ a torsion coset* ζ*). There are finitely many torsion cosets* $X_i \subset V$ *which account for all torsion points of* X *which are in* V*.*

This follows from a stronger result of Laurant from '83. She proved a version of Mordell-Lang in this setting.

We want to indicate a point-counting approach (following a strategy suggested by Zannier). Consider

$$\begin{array}{rccc} e: & \mathbb{C}^n & \longrightarrow & (\mathbb{C}^\times)^n \\ & (z_1,\dots,z_r) & \longmapsto & \left(e^{2\pi i z_1},\dots,e^{2\pi i z_n}\right) \end{array}$$

(note that the preimages of torsion points are exactly the rational points).

Slogan. Studying torsion points on V is the same as studying rational points on $e^{-1}(V)$.

In order to apply counting theorems, we'll view $\mathbb{C}^n \cong \mathbb{R}^{2n}$. Note that $e^{-1}(V)$ is not definable because e is a periodic function. However, because e is periodic, we only need to understand slices of it. The exponential function restricted to

$$F = \{(z_1,\dots,z_r) \in \mathbb{C}^n : 0 \le \operatorname{Re} z_i < 1\}$$

is a definable function, so $Z := e^{-1}(V) \cap F$ is a definable set. We have $e : Z \to V$ turning rational points on Z into roots of unity on V.

Slogan. Roots of unity have high degree, they have lots of conjugates over $\mathbb{Q}$.

If you want, replace V by some $V^*/\overline{\mathbb{Q}}$. If $(\zeta_1,\dots,\zeta_n) \in V^*$ are torsion points of order $(N_1,\dots,N_n)$, and $N := \max_i N_i$, then (e.g. Hardy & Wright)

$$[\mathbb{Q}(\eta) : \mathbb{Q}] \gg_\delta N^{1-\delta}$$

for any δ. By taking e.g. $\delta = 1/2$ and $\varepsilon = 1/3$, get $N^{1/2}$ points where the counting theorem only allows for $N^{1/3}$ points.

Need to understand algebraic part. If $A \subset Z$ is semi-algebraic, must be some complex algebraic $W \subset e^{-1}(V)$. When can you have $e(W) \subset \mathbb{C}^n$? This can only happen if W is a translate of a rational line subspace. See notes, things got rushed at end

Question 2.1.13 (Audience)**.** *Is there a simple example of something with no algebraic part?*

Answer. Graph of real exponential, $\{(x_1,\dots,x_n,e^{x_1},\dots,e^{x_n})\} \subset \mathbb{C}^{2n}$. An example of the other extreme is $z = x^y$ with $x, y \in [1,2]$. Everytime y is rational, get a little piece of something algebraic. ⋆

2.2 Lecture 2 (3/5)

Sounds like Thomas stated Zilber-Pink for $\mathbb{G}_m^n$ in the previous lecture. In this lecture, we'd like to state Zilber-Pink for curves in powers of a modular curve.

Conjecture 2.2.1 (Zilber-Pink for curve $V \subset \mathbb{G}_m^n$)**.** *Say $V \subset \mathbb{G}_m^n$ is a parameterized curve, e.g.*

$$V = \left\{(t, 1+t^2, 1-t, 1+t+t^3, 2, 3, 5, 6\right\}_{t\in\mathbb{C}} \subset \mathbb{G}_m^8.$$

Note that you expect V to not meet any $(n-2)$-dimensional algebraic subgroups (such an intersection is called atypical).

Suppose V is not contained in any proper algebraic subgroup (i.e. no atypical components which are the full curve). ZP in this case amounts to saying that V has only finitely many intersections w/ subgroups of codim ≥ 2, *i.e. V has only finitely many points that satisfy ≥ 2 independent multiplicative conditions.*

Note 1. Missed some stuff (dealing w/ technical difficulties), but Pila made some remarks of relating conjecture to Lang's conjecture, to multiplicative Mordell-Lang, and to other things.

The statement of the conjecture above is in the spirit of the formulation by Bombieri-Masser-Zannier (BMZ).

Theorem 2.2.2 (Mauran (spelling?))**.** *ZP holds for a curve $V/\overline{\mathbb{Q}} \subset \mathbb{G}_m^n$.*

(BMZ extended this to $V/\mathbb{C}$)

For $V/\mathbb{C}$, could consider e.g. $\{(2, \pi, t, t-1, t-\pi)\}$. There should be only finitely many t given 2 independent multiplicative conditions on these coordinates, e.g. $t = \pi/2$. In contrast to Manin-Mumford, note that the points you're looking for move around (depend on the curve as opposed to e.g. being roots of unity). Also, these points are not necessarily defined over $\overline{\mathbb{Q}}$, so the passage from $\overline{\mathbb{Q}}$ to $\mathbb{C}$ is non-trivial.

2.2.1 ZP for curve $V \subset Y(1)^n$ (is open)

Remark 2.2.3. Various special cases are known ○

Remark 2.2.4. As a variety, $Y(1) \simeq \mathbb{A}^1$. ○

Before stating Zilber-Pink, we should probably say what the "special subvarieties" of $Y(1)^n$ are. Recall that $Y(1)$ parameterizes elliptic curves/$\mathbb{C}$ (up to isomorphism).

Recall 2.2.5. An elliptic curve is of the form $E = \mathbb{C}/\Lambda$ for some lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. The curve is invariant under scaling the lattice, so might as well assume $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ for some $\tau \in \mathbb{H}$. The j-invariant of the curve $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau)$ is a function $j : \mathbb{H} \to \mathbb{C}$ of τ. Since elliptic curve is invariant under change of basis of the lattice, this is invariant under the action $\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \mathbb{H}$, i.e.

$$j\left(\frac{az+b}{cz+d}\right) = j(z) \text{ if } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

If E is an elliptic curve, endomorphisms of E corresponding to $\lambda \in \mathbb{C}$ such that $\lambda\Lambda \subset \Lambda$. In general, only have $\lambda \in \mathbb{Z}$. Sometimes, have other λ. This happens iff $\mathbb{Z} + \mathbb{Z}\tau$ has `quadratic` τ, i.e. $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$. Then $j(\tau)$ is "`special`" and classically (19th centure) called a "`singular modulus`." ⊙

The singular moduli, Σ, are the analogues of torsion points in $\mathbb{G}_m$ (roots of unity).

Remark 2.2.6. Torsion points are the ones that modify the exponential function $e^{2\pi i z}$ at rational numbers. The singular moduli are the values of the j function at (imaginary) quadratic numbers. ○

If E, E' are elliptic curves, might have $\varphi : E \to E'$ w/ cyclic kernel of degree N. This amounts to $\Lambda' \subset \Lambda$ with $\Lambda/\Lambda' \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. There is a `modular polynomial` $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$ such that

$$\Phi_N(j(E), j(E')) = 0$$

if and only if E, E' admit a cyclic isogeny of degree N between them.

Example 2.2.7. $\Phi_1(X, Y) = X - Y$. △

Definition 2.2.8. In $Y(1)^2 = \mathbb{C}^2$, the `special subvarieties` are

- `special points` Σ^2 (both coordinates singular moduli)
- `modular curves` $\Phi_N(X, Y) = 0$
- $\sigma \times Y(1)$ and $Y(1) \times \sigma$ for any $\sigma \in \Sigma$

- $Y(1)^2$ ◇

Theorem 2.2.9 (Andre, Analogue of Lang's Problem for $\mathbb{G}_m^2$, Andre-Oort for $Y(1)^2$)**.** *If $V \subset Y(1)^2$ is a curve with infinitely many special points (i.e. $V \cap \Sigma^2$ is Zariski dense in V), then V is special.*

Let's now discuss special subvarieties of $Y(1)^3$. These are essentially subvarieties where two of the coordinates are required to have some special relation (e.g. an isogeny between them), or some coordinates are required to belong to a fixed set of special points.

Say $V \subset Y(1)^3$ is a curve. A one-dimensional special subvariety looks like

- $\Phi_N(x,y) = 0$ and $\Phi_M(y,z) = 0$ (note these imply a modular relation between x and z)
- $x = \sigma \in \Sigma$ and $\Phi_N(y,z) = 0$

These are essentially all possibilities.

Conjecture 2.2.10 (Zilber-Pink for curve $V \subset Y(1)^3$)**.** *Only finitely many points on V satisfying two independent modular conditions, unless V satisfies such a condition identically.*

To say this the other way around, if $g \in \mathrm{GL}_2(\mathbb{Q})^+$ (so g acts on $\mathbb{H}$), then τ and $g(\tau)$ will have lattices related by a (cyclic?) isogeny of order $N = N(g)$ (determinant of g after clearing denominators), so $\varphi_N(j(z), j(gz)) = 0$.

Remark 2.2.11. Think of this as analogue of functional equation for exponentiation $e^{x+y} = e^x e^y$. ○

This is telling us, that under

$$\begin{array}{c} \mathbb{H}^n \\ {\scriptstyle j}\big\downarrow \\ Y(1)^n, \end{array}$$

special subvarieties downstairs come from $\mathrm{GL}_2(\mathbb{Q})^+$-relations upstairs.

2.2.2 Point counting approach

Say we have $V \subset Y(1)^3$. How would we approach Theorem 2.2.9 using point-counting?

Say $V \subset Y(1)^2$. Look at preimage in $\mathbb{H}^2$. If you have $(x_1, x_2) \in V$, get preimages (in some fixed fundamental domain) satisfying e.g. some modular polynomial. [I didn't catch what you do next...]

Say $V \subset Y(1)^3$ and $(x_1, x_2, x_3) \in V$ satisfies $\Phi_N(x_1, x_2) = 0 = \Phi_M(x_2, x_3)$. These can be lifted to $z_1, z_2, z_3 \in F \subset \mathbb{H}$, a fundamental domain. Count matrices, not special points. There is some $g_1, g_2 \in \mathrm{GL}_2(\mathbb{Q})^+$ sending $g_1 : z_1 \mapsto z_2$ and $g_2 : z_2 \mapsto z_3$. So (x_1, x_2, x_3) "unlikely" leads to $g_1, g_2 \in \mathrm{GL}_2(\mathbb{Q})^+$ giving a rational piont on some set. Say $Z = j^{-1}(V) \cap F^3$. For $\alpha, \beta \in \mathrm{GL}_2(\mathbb{Q})^+$, consider

$$Y_{\alpha,\beta} := \left\{(z_1, z_2, z_3) \in \mathbb{H}^3 : z_2 = \alpha z_1 \text{ and } z_3 = \beta z_2\right\}$$

as well as

$$W := \left\{(\alpha, \beta) \in (\mathrm{GL}_2(\mathbb{R})^+)^2 : Y_{\alpha,\beta} \cap Z \neq \emptyset\right\} \subset \mathbb{R}^{2\cdot 2^2}.$$

The (x_1, x_2, x_3) from before give a rational point on W. The point is that $Z, Y_{\alpha,\beta}, W$ are all definable sets, so Pila-Wilkie applies.

Warning 2.2.12. There is a slight problem with this. Points in the upper half plane have stabilizers in $\mathrm{GL}_2(\mathbb{R})$. $W^{\mathrm{alg}} = W$ since you can modify points by stabilizers, so Pila-Wilkie as stated gives not useful.

However, that counting theorem (or, rather, its proof) really says something more precise. Recall you divide your set and say all the pieces lie on some small number of intersections.

I don't follow what's happening, but somehow if you have H^{ε} pieces, this is insufficient to generate H^{δ} conjugates. Somehow this means as you move in one of the pieces, you must get points not coming from stabilizers, and this is what eventually leads to your contradiction. •

2.3 Lecture 3 (3/6)

Today we'll say something about O-minimality.

Note 2. Pila said something about structures that I missed, structures as in $(\mathbb{C}, \times, +, 0, 1)$ or $(\mathbb{R}, <, \times, +, 0, 1)$ or $(\mathbb{R}, <, \times, +, 0, 1, \exp)$ or what have you.

In any of these structures, there's a corresponding language and an induced notion of a definable set. Given a structure $(M, \dots)$, a `definable set` $A \subset M^n$ is a set of the form

$$A = \{(x_1, \dots, x_n) \in M^n : \varphi(\vec{x}) \text{ holds}\},$$

where $\varphi \in \mathrm{Form}(\mathcal{L})$ is some formula in the corresponding language.

Warning 2.3.1. Strictly speaking, this means you can only use numbers definable in your language, e.g. built out of 0's, 1's, and arithmetic operations. •

One also talks about `definable sets with parameters` where you allow $\varphi \in \mathrm{Form}(\mathscr{L}, \{c_m\}_{m \in M})$, so you allow constants attached to elements of M.

Assumption. In O-minimality, definability always means *with parameters*

Note that you can define $<$ in $(\mathbb{R}, \times, +, 0, 1)$, e.g. by saying $y - x = z^2$ (for $x < y$), so this has the same definable sets as $(\mathbb{R}, <, \times, +, 0, 1)$. In O-minimality, though, the order is rather important.

Remark 2.3.2. If you just have $(\mathbb{R}, <)$ then the only sets you can define in $\mathbb{R}$ are basically (finite unions of) points and intervals. ○

Let's talk about minimal structures.

Example 2.3.3. Say work with $(\mathbb{C}, \times, +, 0, 1)$. For $A \subset \mathbb{C}$ definable, you can really only say some polynomial is zero or nonzero, so definable sets here will always be finite or cofinite. In $\mathbb{C}^n$, you have algebraic varieties. This is an example of a minimal structure. △

Example 2.3.4. A structure, like $(\mathbb{R}, <, \dots)$, with an ordering won't be minimal because you can define intervals. △

O-minimality ('O' = Order) is the best you can do in the presence of an order.

Remark 2.3.5. Some people make the 'O' big, some people make is small, and some people make it scripty. ○

Definition 2.3.6. A structure $(M, <, \dots)$ expanding a dense linear order w/o endpoints is `O-minimal` if the definable (w/ parameters) subsets of M are just finite unions of points and open intervals, i.e. just the definable (w/ parameters) sets (in M) in $(M, <)$ ◇

(Above, give M the order topology)

The most interesting examples are when M expands a field, e.g. $(M, <, +, \times, 0, 1, \dots)$. In that case, M will be a real closed field.

Apparently sometimes people say this O-minimality is a "fulfillment of Groethendieck's vision of a tame topology," whatever that means. Van dan Dres was studying the real exponential field $(\mathbb{R}, <, 0, 1, \times, +, \exp : \mathbb{R} \to \mathbb{R})$. Tarski has proven in the 30's that the real field was decidable; he then asked if the real exponential field is decidable (note: get something undeciable if you had in sin b/c then you can define the integers). Sounds like Van dan Dres asked if the definable sets have this nice structure (what we now call O-minimality). Later, some people proved the cell decomposition theorem (one of its consequences being that o-minimal structures are strongly o-minimal, e.g. all structures with the same theory are o-minimal are something like that?).

Anyways, let's list some properties of $(\mathbb{R}, <, 0, 1, \times, +, \exp)$

- Every definable function is continuous away from finitely many points.

  The condition to be continuous is some first order thing, so the points where you're not continuous is definable, so a finite union of points and intervals. One then shows a definable function can't be discontinuous on an entire interval.

- Uniformity finiteness

  A `definable family` is a definable set $X \subset M^k \times M^n$, which you view as the family of fibers

  $$\left\{X_{\vec{y}} : \vec{y} \in M^k\right\}$$

  (Somehow it's useful to think of the parameter as being in the *first* factor). One general gets uniformity results when working w/ definable families.

  Example 2.3.7 (Not 100% sure I heard this example correctly)**.** Say $X = \left\{(x, f(x)) \in \mathbb{R}^2 : x \in [0,1]\right\}$ with f analytic (not algebraic), and C is a algebraic curve. Then, $X \cap C$ will be finite, w/ size bounded independently of f. $\triangle$

Remark 2.3.8. A function is `definable` if its graph is definable, so can think in terms of functions or in terms of their graphs. $\circ$

Let's look at examples of o-minimal sets.

Example 2.3.9. $\mathbb{R}_{\text{alg}} = (\mathbb{R}, <, +, \times, 0, 1)$ is o-minimal, by work of Tarski (follows from quantifier elimination, whatever that means) $\triangle$

Example 2.3.10. $\mathbb{R}_{\text{an}} = (\mathbb{R}, <, +, \times, 0, 1, \{f : B \to \mathbb{R}\})$ as f ranges over all functions $f : B \to \mathbb{R}$ where $B \subset \mathbb{R}^n$ is a closed bounded box, and f is real analytic in some neighborhood of B. Such f are called `restricted analytic functions`. This is o-minimal. $\triangle$

Example 2.3.11. $\mathbb{R}_{\exp} = (\mathbb{R}, <, +, \times, 0, 1, \exp)$ is o-minimal. $\triangle$

Example 2.3.12. $\mathbb{R}_{\text{an,exp}} = (\mathbb{R}, <, +, \times, 0, 1, \{f : B \to \mathbb{R}\}, \exp)$ is o-minimal. $\triangle$

Non-example. The complex exponential $\exp : \mathbb{C} \to \mathbb{C}$ can never be definable ($\mathbb{C} = \mathbb{R}^2$), because then you can define the integers. However, something like $\exp|_{\mathbb{R}\times[-1,1]}$ can be definable (an is e.g. in $\mathbb{R}_{\text{an,exp}}$) $\triangledown$

2.3.1 Counting Theorem

Suppose that $Z \subset (0,1)^n$ is definable and $r \geq 1$ is a positive integer. Say $\dim Z = k$.

Definition 2.3.13. An r`-parameterization` of Z is a finite set Φ of $\{\varphi : (0,1)^k \to (0,1)^n\}$ such that $Z = \bigcup \operatorname{im} \varphi$, each φ is differentiable up to order r, and all partial derivatives of order $\leq r$ are bounded in absolute value by 1. $\diamond$

Definition 2.3.14. Let $Z \subset P \times (0,1)^n$ be a definable family of sets in $(0,1)^n$. A `definable r-parameterization of Z` is a finite set $\Phi = \{\varphi : P \times (0,1)^k \to (0,1)^n\}$ such that for each $\vec{y} \in P$, the functions

$$\varphi_{\vec{y}} : (0,1)^k \longrightarrow (0,1)^n$$

form an r-parameterization of the fiber $Z_{\vec{y}}$. $\diamond$

Theorem 2.3.15. *If Z is a definable family of sets in $(0,1)^n$, and $r \geq 1$, then there exists a definable r-parameterization of Z.*

This was proved by Yomden for semi-algebraic sets, and then later by Gromov in the above formulation.

To prove the counting theorem, one starts with a definable family $Z \subset P \times \mathbb{R}^n$. By reflecting, taking -1, and such things, you can replace Z by a finite number of families $Z \subset P \times (0,1)^n$. You then r-parameterize this family, to realize is as a collection of maps $P \times (0,1)^k \to (0,1)^n$.

Remark 2.3.16. Everything will be uniform in parameters, so we'll drop them from now on to unclutter notation. $\circ$

Note form determinants as in the first lecture. You'll get that, after possibility subdividing $(0,1)^k$, can force all points in the image to land on some hypersurface of degree d. Pila made some additional remarks about subtleties and how to deal with them...

Theorem 2.3.17. *If $Z \subset P \times \mathbb{R}^n$ definable family and $\varepsilon > 0$, then*

$$N(Z_{\vec{y}}^{trans}, H) \leq c(Z, \varepsilon) H^{\varepsilon}.$$

(If one's more careful, one doesn't need to remove the entire algebraic part, but only some other sort of certain large sets) One can also prove a result like this for quadratic points, or even for points of bounded degree. Pila mentioned some other further directions for improving this statement.

2.4 Lecture 4

Let's return to our discussion of Zilber-Pink. We've seen (in Thomas' lectures) CIT. This says something about torsion cosets in $X = \mathbb{G}_m^n$, or X an abelian variety, or about special subvarieties in $X = Y(1)^n$ or X a Shimura variety.

Let's give another example. Recall the `Legendre surface`

$$\mathcal{E} = \big((x,y,t) : y^2 = x(x-1)(x-t)\big) \longrightarrow Y(2) = \mathbb{C} \setminus \{0,1\}.$$

This is the simplest example of a "*mixed Shimura variety*." It has some special subvarieties.

- The `special points` are torsion points in CM fibers
- The `special curves` come in two forms:
  - Torsion sections
  - Fibers over CM points

2.4.1 General Picture for Zilber-Pink

Let X be a mixed Shimura variety along with its (countable[2]) collection $\mathcal{S}$ of "special subvarieties." Let $V \subset X$.

Definition 2.4.1. A subvariety $A \subset V$ is atypical (of V in X) if A is a component if $V \cap S$ fo some $S \in \mathcal{S}$ satisfying

$$\dim A > \dim V + \dim S - \dim X. \qquad \diamond$$

Conjecture 2.4.2 (Zilber-Pink). *With X a MSV and $V \subset X$, the union $\bigcup A$ of all atypical components is a finite union.*

(Equivalently, this union is Zariski dense $\iff$ V is special)

Sounds like Pink was led to a statement like this in an effort to unify things like Mordell-Lang, Manin-Mumford, André-Oort, etc.

Let's discuss relative Manin-Mumford (RMM). Consider a family over $Y(2)$ where the fiber over t is two copies of $E_t : y^2 = x(x-1)(x-t)$. Call the total space $\mathcal{E}^{(2)}$, a 3-dimensional MSV. Say we have a curve $V \subset \mathcal{E}^{(2)}$.

Remark 2.4.3. For curves in surfaces, ZP reduced to special point problems (like Manin-Mumford and André-Oort). This is why we looked at $\mathcal{E}^{(2)}$ above instead of $\mathcal{E}$. This also means things are less interesting if V is fibral/vertical than if it is horizontal. $\circ$

Say V is horizontal. For each $t \in Y(2)$, ask, is V_t torsion? The conclusion is that it should only be torsion finitely many times, unless V is a torsion section. Masser-Zannier looked at such things. They had a particular example of

$$V = \left\{(t, \sqrt{2(2-t)}, \sqrt{6(3-t)})\right\} \subset \mathcal{E}^{(i)}2$$

(points on E_t with x-coordinates $2, 3$). Unclear to me in which cases they proved relative Manin-Mumford. Sounds like maybe Gao-Habegger have recent results resolving it in a large number (all?) of cases?

Theorem 2.4.4 ((Example of) Relative Manin-Mumford?)**.** *If $V \subset \mathcal{E}^{(2)}$, then the set of points on V which are torsion in their fiber is finite.*

This theorem does not yet imply Zilber-Pink in this setting, because you also have to worry about (vertical) special curves. That is, have to think about points on V whose t-coordinate is special/CM and where the two E_t points are linearly independent over $\operatorname{End}(E_t)$. Proving such points are finite (unless your curve is fibral) is a theorem of Banvere (spelling?).

What if you go up to $\mathcal{E}^{(3)}$? Even in the fibral case $V \subset E_{t_0}^3$, you get unlikely intersection problems. Sounds like this case was resolved (over $\overline{\mathbb{Q}}$) by Habegger-P. and also over $\mathbb{C}$, but I can't read the names of the people it's due to.

Theorem 2.4.5 (Can't read names)**.** *Say $V \subset \mathcal{E}^{(n)}$ and $p_1(t), \ldots, p_n(t)$ are generically linearly independent over $\mathbb{Z}$, then there exists only finitely many t such that $p_1(t), \ldots, p_n(t)$ satisfy two independent linear relations over $\mathbb{Z}$.*

2.4.2 Analogue of ZP

Take $X = \mathbb{A}^n/\mathbb{C}$. The special subvarieties will be all irreducible $T/\overline{\mathbb{Q}}$. Take $V \subset X$ (V defined over $\mathbb{C}$), and ask the same question. The special point problem is known: the $\overline{\mathbb{Q}}$-points of V will lie on some union of subvarieties defined over $\overline{\mathbb{Q}}$. In particular, there are Zariski dense $\iff$ $V/\overline{\mathbb{Q}}$ (i.e. $\iff$ V is special).

[2] If $\dim X > 0$

Theorem 2.4.6 (Chazidakis,Ghioca,Masser,Maurin (spelling?))**.** *"ZP" holds in this situation.*

Remark 2.4.7. If you have an analytic curve $V \subset \mathbb{A}^3$, conjecture says its intersection with all algebraic curves form a finite union of points. However, this points are not necessarily algebraic, so this really is a new theorem. $\circ$

Consider situation of $V \subset Y(1)^3$ a curve. Some previous theorem (the above?) implies that if $V/\mathbb{C}$ is not contained in any hypersurface over $\overline{\mathbb{Q}}$, then V satisfies ZP. In fact,

Theorem 2.4.8. *ZP holds for any curve $V/\mathbb{C}$ which is not defined over $\overline{\mathbb{Q}}$.*

2.4.3 $\mathbb{G}_m^n$ case

Recall 2.4.9. ZP for a curve in $\mathbb{G}_m^n$ is a theorem (of Maurin?). $\odot$

It is open already for surfaces, though.

Say $V \subset \mathbb{G}_m^n$ is a general subvariety. Expect the atypical components of V to be a finite union (of points and positive dimensional things). The best known general result is the following.

Theorem 2.4.10 (Habegger)**.** *(Pila didn't write down the statement, only described it aloud. Something like getting finiteness of points if you remove intersections with weakly special subvarieties, or something like this?)*

2.4.4 Multiplicative dependence of singular moduli

Suppose $\sigma_1, \ldots, \sigma_n$ are singular moduli (j-invariants of CM elliptic curves). Take $V \subset Y(1)^n \times \mathbb{G}_m^n$ to be the diagonal (so $V \cong \mathbb{G}_m^n$). An n-tuple w/ singular moduli which are multiplicative dependent lies on a special subvariety of codimension $n+1$. Thus, ZP implies something in this case. Sounds like Jonathan and Jacob proves the implication of ZP in this case, but did not prove ZP itself (even for $n = 3$).

2.4.5 ZP $\implies$ UZP

(Zilber-Pink implies uniform Zilber-Pink)

Consider case of $V \subset Y(1)^3$.

Theorem 2.4.11. *Assume ZP for all powers $Y(1)^n$. Given $d \geq 1$, then there is a number $N_d \in \mathbb{Z}$ such that if $V \subset Y(1)^3$ is a curve of degree d, then the number of atypical points on it is at most N_d (or infinite).*

3 Thomas Scanlon: Model theoretic origins and approaches to unlikely intersection problems

3.1 Lecture 1 (3/4)

Want to talk about how Zilber-Pink (unlikely intersection) type problems are related to mathematical logic. In particular, their connection to the complex exponential function. We will spend some time talking about how to axiomatize this function.

Start with (structure?)

$$\mathbb{C}_{\exp} = (\mathbb{C}, +, \cdot, \exp, 0, 1)$$

(over the language?) $\mathcal{L}(+, \cdot, E, 0, 1)$. We interpret

$$E^{\mathbb{C}_{\exp}} = \exp\,, \quad \exp(z) = \sum_{n \geq 0} \frac{z^n}{n!}.$$

Could also consider $\mathbb{R}_{\exp} = (\mathbb{R}, +, \cdot, \exp, 0, 1)$.

Theorem 3.1.1 (Wilkie)**.** *The theory* $\mathrm{Th}(\mathbb{R}_{\exp})$ *is* `model complete`*, i.e. any definable set in any number of variables is defined by an existential statement (or something like this). In this case, this implies that* $\mathbb{R}_{\exp}$ *is o-minimal.*

Proposition 3.1.2. $\mathrm{Th}(\mathbb{C}_{\exp})$ *is undecidable.*

Proof. Suffices to show you can define the integers. Consider formula

$$\varphi(x) := \forall z[E(z) = 1 \implies E(xz) = 1],$$

i.e. x is a multiplicative stabilizer of the kernel of the exponential function. Then, $\varphi(\mathbb{C}_{\exp}) = \mathbb{Z}$. From a decision procedure for $\mathrm{Th}(\mathbb{C}_{\exp})$, we can now get a decision produce for $\mathrm{Th}(\mathbb{Z}, +, \cdot, 0, 1)$, but this is impossible by Gödel. ■

I guess, really, $2\pi i\mathbb{Z}$

"This is the first operation people usually make about the theory of complex expoentiation, and hence the last."

Somehow, Boris didn't let this bother him.

Note 3. Missed a couple remarks.

Remark 3.1.3. O-minimality and undecidability are not technically opposed to one another. Decidability of $\mathbb{R}_{\exp}$ is an interesting question. We might say more about this later. ∘

We work in a logical called $\mathcal{L}_{\omega_1,\omega}(Q)$. What does this mean?

- Here, ω_1 is the first uncountable ordinal.
- We allow countable conjunction and countable disjunction.
- We allow the usual first order operations $(\neg, \forall, \exists, \dots)$
- "Qx" is the quantifier "there are uncountably many x such that blah"

  In practice, we usually care about there being at most countably many of some thing, i.e. about $\neg Q$.

Remark 3.1.4. In general, can talk about $\mathcal{L}_{\kappa,\lambda}$. The first cardinal indicates you're allowed disjunctions/conjunctions of $< \kappa$ many formulas. The second means you are allowed $< \lambda$ quantifiers, i.e. $(\exists x_i)_{1\le i<\lambda}\,\varphi$. ○

Let's define a theory of pseudo-exponentiation.

Example 3.1.5 (T_{exp}, `theory of pseudo-exponentiation`)**.** This will be a formal theory. If the world is as nice as we think it is, it secretly describes theory of complex exponentiation.

- ELA "exponential logarithmic algebraically closed field"
  - Includes axioms ACF_0 for algebraically closed fields of characteristic 0, e.g.

    $$\forall x \forall y \forall z\, x\cdot(y+z) = x\cdot y + x\cdot z.$$

    Also need to say it is characteristic 0, so

    $$(1+1)\neq 0,\ \ (1+1+1)\neq 0,\ldots.$$

    Also need it be algebraically closed, every polynomial which does not obviously not have a zero, does have a zero:

    $$\forall a_0 \forall a_1 \ldots \forall a_n \exists x\, x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$
  - Need exponentiation E. This boils down to $\forall x\forall y : E(x+y) = E(x)E(y)$. Also need $E(0) = 1$ (this also follows from the existence of logarithms below).
  - Logarithmic part is
    $$\forall y[y = 0 \vee \exists x : E(x) = y].$$
- SK "standard kernel"

  $\ker E \cong \mathbb{Z}$ as a group. Can write this as

  $$\exists \varpi \forall x \left[E(x) = 1 \to \bigvee_{n\in\mathbb{Z}} \underbrace{\varpi + \cdots + \varpi}_{n \text{ times}} = x \right]$$

  (note use countably disjunction, which is OK in $\mathcal{L}_{\omega_1,\omega}$)
- SC "Schanuel's conjecture"

  $$\forall \alpha_1 \ldots \forall \alpha_n \left[\dim_{\mathbb{Q}} \left(\sum_{i=1}^n \mathbb{Q}\alpha_i \right) = n \to \operatorname{trdeg}_{\mathbb{Q}} \mathbb{Q}(\vec{\alpha}, \vec{E(\alpha)}) \geq n \right]$$

  Example 3.1.6. Take $\varpi \in \ker E$. Then, ϖ is transcendental, because $1 \le \operatorname{trdeg}_{\mathbb{Q}}(\varpi, E(\varpi)) = \operatorname{trdeg}_{\mathbb{Q}}(\varpi)$. △

  Example 3.1.7. If SC holds over $\mathbb{C}$, one could get that e, π are algebraically independent, which is currently open. △

  This conjecture can be phrased in a way expressible in the logic we described, e.g. to say the α_i's span an n-dimensional vector space is to say there is no linear relation among them. For the conclusion, write something like

$$\bigwedge_{\substack{f_1,\dots,f_m\in\mathbb{Q}[x_1,\dots,x_n,y_1,\dots,y_n]\\ \dim V(\vec{f})<n}} \neg(f_1(\alpha,E(\alpha))=0\wedge\cdots\wedge f_m(\alpha,E(\alpha))=0)\,.$$

- sEac (strong exponential algebraic closedness), related to Nullstellensatz

  This is related to the following.

  Conjecture 3.1.8 (Schanuel's Reverse Conjecture)**.** *If $\mathcal{K}=(K,+,\cdot,E,0,1)$ is a countable field satisfying ELA + SK + SC, then there exists an embedding (as an exponential field!) $K\hookrightarrow\mathbb{C}_{\exp}$.*

  Sounds like can formulate sEac as a generalization of this conjecture, but this is not the way one usually formulates this axiom.

  Say $X\subset\mathbb{G}_a^g\times\mathbb{G}_m^g$ is an algebraic variety (irreducible), and there is no obvious reason by $X\cap\Gamma_{\exp}=\emptyset$, then this intersection is nonempty. Formally, if X is rotund and additively and multiplicatively free, then $\exists a=(a_1,\dots,g)\in\mathbb{G}_a^g(K)$ such that $(a,E(a))\in X(K)$.

  - additively free: there is not tuple $\ell_1,\dots,\ell_g\in\mathbb{Z}^g\setminus\{0\}$ such that the function $\ell_1x_1+\cdots+\ell_gx_g$ is constant on X. multiplicatively free is the same, but with multiplication, i.e. no $(\ell_1,\dots,\ell_g)\in\mathbb{Z}^g\setminus 0$ such that the function $y_1^{\ell_1}\dots y_g^{\ell_g}$ is constant on X.
  - rotund: If $M=(M_{ij})\in M_{g\times m}(\mathbb{Z})$, can define

    $$\begin{array}{rccc}\Phi_M: & \mathbb{G}_a^g\times\mathbb{G}_m^g & \longrightarrow & \mathbb{G}_a^g\times\mathbb{G}_m^g\\ & (x_1,\dots,x_g,y_1,\dots,y_g) & \longmapsto & \left(\sum M_{1j}X_j,\dots,\sum M_{gj}x_j,\prod y_j^{M_{1j}},\dots,\prod y_g^{M_{gj}}\right).\end{array}$$

    Rotund means that $\dim\Phi_M X\geq\operatorname{rank}M$ always.

- CCP "[I can't read what it says]" $\triangle$

We'll see next time that Zilber-Pink (for torii?) is equivalent to characterizing some of these in first order ways.

4 Jacob Tsimerman: Special point problems and their arithmetic

4.1 Lecture 1 (3/4)

Let's start by introducing the simplest special points problem, Lang's conjecture. There are several different proofs of it, so it works as a sort of testing ground for harder cases. If you want to try out a technique on a harder special points problem, first try to use it to reprove Lang.

Question 4.1.1. *Say $f \in \mathbb{C}[x, y, x^{-1}, y^{-1}]$ is a Laurent polynomial. Assume it has infinitely many solutions with x, y both roots of unit*

Think about this question as taking place in $(\mathbb{C}^\times)^2 = \mathbb{G}_m(\mathbb{C})^2$. From this perspective, note that

$$\{(x, y) : x, y \text{ roots of unity}\} = (\mathbb{C}^\times)^2_{\text{tors}}.$$

Example 4.1.2. If $f = x^m y^n - \zeta$ for some $(m, n) \in \mathbb{Z}^2 \setminus 0$ and ζ a root of unity, then f has infinitely many solutions with x, y both roots of unity. △

Theorem 4.1.3 (Lang)**.** *These are all the examples.*

Remark 4.1.4. $Z(x^m y^n - 1)$ is an algebraic subgroup of $\mathbb{G}_m^2$. In fact, all algebraic subgroups arise in this way. Say $G \subset (\mathbb{C}^\times)^2$ is an algebraic curve subgroup, consider the two projections $G \overset{\pi_1}{\underset{\pi_2}{\rightrightarrows}} \mathbb{C}^\times$. The first gets us an extension

$$1 \longrightarrow K \longrightarrow G \xrightarrow{\pi_1} \mathbb{C}^\times \longrightarrow 1$$

with K some finite group, say of order n. Hence, $\exists \psi : \mathbb{C}^\times \to G$ so that $\pi_1 \circ \psi : z \mapsto z^n$. Now $\pi_2 \circ \psi : \mathbb{C}^\times \to \mathbb{C}^\times$ will be of the form $z \mapsto z^m$ for some m. ○

Definition 4.1.5. Say $T \subset \mathbb{G}_m^2$ is a `torus`, i.e. a connected subgroup. If $\zeta \in \mathbb{G}_m^2(\mathbb{C})_{\text{tors}}$, then ζT is called a `torsion coset`. ◇

Theorem 4.1.6. *Say $C \subset \mathbb{G}_m^2$ is an irreducible curve. Then,*

$$\# C \cap \left(\mathbb{C}^\times\right)^2_{\text{tors}} = \infty \iff C \text{ torsion coset.}$$

Tsimerman feels the study of special points isn't super theory heavy, but there are lots of "tricks of the trade" that come up repeatedly. Also, sometimes old techniques fall out of favor as new ones are discovered, but it's still worth knowing them (never know which techniques will be best suited to a new problem), so let's spend some time introducing some well known techniques.

4.1.1 Galois orbits

Let $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $\mu_n(\mathbb{C}) \subset \mathbb{C}^\times$ denote the nth roots of unity, and let $\mu_\infty(\mathbb{C}) := \bigcup_n \mu_n(\mathbb{C})$ be all roots of unity. Note that

$$\mathrm{Aut}(\mu_\infty(\mathbb{C})) \simeq \varprojlim \mathrm{Aut}(\mu_n(\mathbb{C})) \simeq \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times \simeq \widehat{\mathbb{Z}}^\times.$$

Note that $G_{\mathbb{Q}} \twoheadrightarrow \widehat{\mathbb{Z}}^\times$ via its action on $\mu_\infty(\mathbb{C})$.

Corollary 4.1.7. *If $\zeta \in (\mathbb{C}^\times)^n$ and $\mathrm{ord}(\vec{\zeta}) = m$, then $\# G_{\mathbb{Q}} \cdot \vec{\zeta} = \varphi(m) = m^{1+o(1)}$.*

For the argument Jonathan (Pila) gave (at the end of his first lecture), its enough to know that this orbit is big. For other arguments, one needs to know more about what these Galois-conjugates look like.

"Intersection" proof of Theorem 4.1.6. Let $C \subset \mathbb{G}_m^2$ be a curve contradicting the statement. For simplicity, assume C is defined over $\mathbb{Q}$.[3] Choose $\vec{x} \in C(\mathbb{C}) \cap (\mathbb{C}^\times)^2_{\text{tors}}$. Let $m = \text{ord}(\vec{x})$. Let p be a prime such that $(p, m) = 1$ and $p = O(\log m) = m^{o(1)}$.

Fact. $\prod_{p \le \log x} p \text{``} \sim \text{''} x$ because $\sum_{p \le \log x} \log p \sim \log x$ by PNT.

$\vec{x} \in C \implies \vec{x}^p \in C$ (b/c they're Galois conjugate), so $\vec{x} \in C \cap C^{1/p}$ ($C^{1/p}$ is inverse image of C under the pth power map).

(Case 1) Suppose $C \neq C^{1/p}$.

In this case, $\deg(C^{1/p}) \le p \deg C$ (take equations for C and replace variables w/ their pth powers in order to get $C^{1/p}$). By Bezout, $\# C \cap C^{1/p} \le p \deg(C)^2 = m^{o(1)}$. On the other hand $\# G_{\mathbb{Q}} \cdot \vec{x} = \varphi(m) = m^{1+o(1)}$. If m is really big, this is a contradiction.

(Case 2) Suppose $C = C^{1/p}$. We'll show that C is a torsion coset.

By translating, we may assume $1 \in C$. Let $U = \log(C)$, analytic germ around 0.[4] By assumption, $U = pU = p^2 U = p^3 U = \dots$. This is only possible if U is linear which means that C is a subgroup. ■

Let's briefly consider the higher dimensional case: if you have a subvariety of $(\mathbb{C}^\times)^n$, what do the torsion points inside of it look like.

Warning 4.1.8. It's possible to have $\Delta \subset S \subset (\mathbb{C}^\times)^3$, where $\Delta \cong \mathbb{C}^\times$ is the diagonal. In this case, even if S isn't special in any sense, it will have infinitely many torsion points. •

Theorem 4.1.9 (Laurent, Lang's Conjecture)**.** *Say $V \subset \mathbb{G}_m^n$ is irreducible, and suppose that $V \cap (\mathbb{C}^\times)^n_{\text{tors}}$ is Zariski dense in V, i.e.*

$$\left(V \cap (\mathbb{C}^\times)^n_{tors}\right)^{Zar} = V.$$

Then, V is a torsion coset.

The first proof by Laurent was of a much harder statement involving S-units, and using a lot of analytic machinery. This is a little sad, because it means the above statement didn't get a proper treatment in the literature.

We're a little low on time, so we won't give the full proof of this theorem.

Proof Sketch of Theorem 4.1.9, when $n = 3$ and $\dim V = 2$. Consider things of the form $V \cap V^{1/p}$. The new issue is that you could have a sequence $C_1, \dots, C_n, \dots$ of torsion coset curves in V such that for each prime p, you get a different torsion coset. Write $C_i = x_i \cdot T_i$ with x_i torsion. There are a couple of ways of dealing with this.

- o-minimality: look at "slopes" of the T_i. This is definable and discrete, and so must be finite.[5]
- equidistribution: more on this later
- More Bezout:

  Let $m_i := \text{ord}(\overline{x}_i)$, where $\overline{x}_i \in (\mathbb{C}^\times)^3/T$. Two cases to look at:

[3] Since C has infinitely many (= Zariski dense) torsion points, it must be defined over $\overline{\mathbb{Q}}$, so it will be defined over a number field K. Sometimes its easier to work over K, and sometimes its easier to work with the union of C's conjugates (which is defined over $\mathbb{Q}$). Here, we sidestep this issue by assuming $K = \mathbb{Q}$ to start.

[4] C is a subset of $(\mathbb{C}^\times)^2$, and there's a log map $\log : \mathbb{C}^\times \to \mathbb{C}$ defined near 1 (though globally multi-valued, not a function). This is why we work only w/ germs.

[5] Sounds like this is a common way to use o-minimality. Show something is simultaneously definable and rational/discrete, so finite.

(1) m_i are unbounded

Pick a prime p, ans consider $V \cap V^{1/p}$, which contains $\varphi(m_i)$ many cosets of T_i. This will contradict Bezout.

Theorem 4.1.10 (Fulton's Version of Bezout)**.** *Say $V_1, \ldots, V_m \subset \mathbb{P}^n$. Then,*

$$\deg\Big(\bigcap V_i\Big) \leq \prod \deg V_i.$$

(2) m_i are bounded, assume $m_i = 1$.

Observe that each $T = T^2$, so $V = V^2$. Use this to conclude that V is a subgroup. ■

4.1.2 Equidistribution

Remark 4.1.11. There is an equidistrubtion version of André-Oort, which is still wildly open in general. ○

Say $\vec{x} \in (\mathbb{C}^\times)^n_{\text{tors}}$. Consider the Dirac/Delta measure $\delta_{\vec{x}}$. "Smooth things out" by considering

$$\mu_{\vec{x}} := \sum_{\vec{z} \in G_{\mathbb{Q}} \cdot \vec{x}}{}' \delta_{\vec{z}} = \int_{G_{\mathbb{Q}}} \delta_{g\vec{x}} \mathrm{d}g.$$

Notation 4.1.12. Above (and elsewhere), $\sum'$ with the prime means to average, so about is really $\frac{1}{\#\mathbb{G}_{\mathbb{Q}} \cdot \vec{x}} \sum \delta_{\vec{z}}$.

We will make use of the bijection

$$\begin{Bmatrix} \text{sub-tori of} \\ \mathbb{C}^n \end{Bmatrix} \longleftrightarrow \begin{Bmatrix} \text{closed, connected subgroups} \\ \text{of } (S^1)^n \end{Bmatrix}.$$

This is given by $T \mapsto T \cap (S^1)^n$ and $H^{\text{zar}} \leftarrow\!\shortmid H$.

Given $H \subset (S^1)^n$, let μ_H be the Haar (probability) measure on H, and set

$$\mu_{\vec{H}} = \int_{G_{\mathbb{Q}}} \mu_{g\vec{x} \cdot H} \mathrm{d}g.$$

Theorem 4.1.13 (Bilu)**.** *The set $\{\mu_S : S$ torsion coset$\}$ is weak-$*$ closed, i.e. if you have a covergent sequence of such measures, then the limit is one of them too.*

This implies Lang (I missed how, sad).[6]

Proof Sketch of Bilu. Let $\chi : (S^1)^n \to S^1$ is a character. For equidistribution, it suffices to integrate against characters (since working in a compact group). For all k, one needs to show that

$$\int t^k \mathrm{d}\mu_n(t) \xrightarrow{n \to \infty} 0.$$

Averaging characters over roots of unity amounts to looking at their images (getting new roots of unity), and then averaging those. This let's one reduce to the 1-dimensional case. ■

[6]Something like your roots of unity will be archimedean dense in something like S^1 and so Zariski dense in a torus

4.1.3 One last proof sketch

This approach is the least generalizable, but is really nice. This is due to Zhang.

Consider $f = \sum_{v \in S} a_v x^v$ with $S \subset \mathbb{Z}^n$. If $f(\xi) = 0$, then $f(\xi^a) = 0$ for a punch of different a's. Find an arithmetic progression of a's, and think of this relation for different ξ's as an inner product. Thinking along these lines will show that some Vandermonde determinant vanishes, and so $\xi^{v-w} = 1$ for some $v, u \in S$. This is your torsion coset.

4.2 Lecture 2 (3/5)

Today we'll talk about one (or two?) more special point problems. We'll start with something along the lines of Lang's conjecture/mulitplicative Manin-Mumford.

Let $E/\mathbb{C}$ be an elliptic curve, i.e. a smooth projective connected algebraic group of dimension 1.

Example 4.2.1. $E : y^2 = x^3 + Ax + B$ $\triangle$

As a complex Lie group, one has $E(\mathbb{C}) \cong \mathbb{C}/L$, where L is some lattice. One can recover L in terms of the geometry of E. If ω is a regular one-form on E, one can take

$$L = \left\langle \int_{\gamma_1} \omega, \int_{\gamma_2} \omega \right\rangle,$$

where $\gamma_1, \gamma_2 \in \mathrm{H}_1(E; \mathbb{Z})$ form a basis. Note that, as a real Lie group, $E(\mathbb{C}) \cong (S^1)^2$, so e.g. $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ and $E_{\text{tors}} \cong (\mathbb{Q}/\mathbb{Z})^2$. For something like Lang's conjecture, we'll want to understand distribution of torsion points in powers of E.

Fact. If $H < E^n$ is an irreducible, algebraic subgroup, then there is an isogeny $\psi : H \twoheadrightarrow E^m$ for some m. One can reverse this (maybe raise something to some power to kill kernel), and so conclude that there is a map $\varphi : E^m \to E^n$ with $\# \ker \varphi < \infty$ such that $H = \operatorname{im} \varphi$.

Theorem 4.2.2 (Raynaud, `Manin-Mumford Conjecture`)**.** *Let $V \subset E^n$. Then, V contains only finitely many maximal (under inclusion) torsion cosets.*

(Raynaud's proof is interesting, but a bit afield from this course, so we won't talk about it here)

Exercise. Show this statement is equivalent to "irreducible V is a torsion coset $\iff$ its torsion points are Zariski dense."

We'll prove in two steps, first over $\overline{\mathbb{Q}}$ and then reduce $\mathbb{C} \rightsquigarrow \overline{\mathbb{Q}}$.

- Say $K \subset \overline{\mathbb{Q}}$ is a number field so E/K.

  Let
  $$\rho_E : G_K \longrightarrow \operatorname{Aut}(E_{\text{tors}}) = \varprojlim_n \operatorname{Aut}(E[n]) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}})$$
  be the Galois action on torsion points. We now break into two cases.

  (1) Suppose $\operatorname{End}(E) = \mathbb{Z}$.

  In this case, `Serre's open image theorem` says that $\operatorname{im} \rho_E \subset \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is open, and in particular of finite index.

  (2) Suppose $\operatorname{End}(E) = R$, $\operatorname{rank}_{\mathbb{Z}} R = 2$, and $R \subset L = \mathbb{Q}(\sqrt{-d})$.

  In this case, one can show (modulo a tiny bit of lying[7]) that $\operatorname{im} \rho_E \subset \left(R \otimes \widehat{\mathbb{Z}}\right)^{\times}$.

[7] Get a bit more (a $\mathbb{Z}/2\mathbb{Z}$ or so?) coming from automorphisms of the ring of integers, if I heard correctly

In either case, we will use something weaker than both of these. It suffices to know there's some $H \overset{\text{open}}{\subset} \widehat{\mathbb{Z}}^\times$ such that $H \subset \operatorname{im} \rho_E$. Let's say a bit about some proofs.

- The intersection theory proof is the same as before.
- The equidistribution proof almost works the same way. The main point here is

$$\left\{\begin{matrix}\text{alg. subgrps.}\\ G < E^n\end{matrix}\right\} \hookrightarrow \left\{\begin{matrix}\text{closed subgroups}\\ \text{of } E(\mathbb{C})^n \cong (S^1)^{2n}\end{matrix}\right\}$$

  Not all closed real lie groups of E^n are algebraic (e.g. take $S^1 \subset (S^1)^2 \cong \mathbb{E}(\mathbb{C})$ with irrational slope). Using H, can define measures μ_S for *real* torsion cosets $S \subset (S^1)^{2n}$. One can then prove that

$$\{\mu_S : S \subset (S^1)^{2n}\}$$

  is weak-$*$ closed.

  Proof of Theorem 4.2.2/$\overline{\mathbb{Q}}$. Consider (topological closure)

$$\overline{\bigcup_{\substack{S \subset V\\ \text{torsion cosets}}} S} = \bigcup_{i=1}^m T_i$$

  which is contained in finite union of real torsion cosets T_i. Now $T_i^{\text{Zar}} \subset V$ are torsion cosets. Question: Why?
  These must be the maximal ones. ■

- Reduction from $\mathbb{C}$ to $\overline{\mathbb{Q}}$

  One idea for doing this is to spread out.

  Example 4.2.3. Say $E : y^2 = x^3 + x + \pi$. How do you study this? Consider the elliptic curve $\mathcal{E}/\overline{\mathbb{Q}}(t)$ given by $\mathcal{E} : y^2 = x^3 + x + t$. Note that E is the base chance of $\mathcal{E}$ when you specialize $t \rightsquigarrow \pi$. Note that $\mathcal{E}$ is nonsingular whenever $4 + 27t^2 \neq 0$. Hence, we get a family $\mathcal{E} \to \mathbb{A}^1 \setminus \{\pm\sqrt{-4/27}\}$ s.t. $\mathcal{E}_\pi = E$. △

  Given $E/\mathbb{C}$ and $V \subset E^n$, we can find some smooth $B/\overline{\mathbb{Q}}$ along with some "`generic`" $i \in B(\mathbb{C})$ (i.e. smallest $\overline{\mathbb{Q}}$-variety containing i is B) and some $\mathcal{E}/B$ and $\mathcal{V} \subset \mathcal{E}^n$ so that

$$(\mathcal{E}, \mathcal{V})_i = (E, V).$$

  Warning 4.2.4. Worry that if you specialize $\mathcal{V}$ to different $\overline{\mathbb{Q}}$-points, then you could get more and more torsion cosets showing up. •

  Proof of Theorem 4.2.2/$\mathbb{C}$. Let $S_1, \dots, S_n, \dots \subset V$ be (algebraic) torsion cosets. Then, there exists torsion cosets $S_1', \dots, S_n', \dots \subset \mathcal{V}$ over B s.t. $(S_n')_i = S_n$. Take an analytic disk $i \in \Delta \subset B(\mathbb{C})$. As a real Lie group, one has

$$\mathcal{E}^n_\Delta(\mathbb{C}) \cong (S^1)^{2n} \times \Delta.$$

  Let $T_1, \dots, T_m$ be real torsion cosets such that $\bigcup_{i=1}^m T_i \supset \bigcup_{n \geq 1} S_n$, and $\bigcup_{i=1}^m T_i$ is minimum[8]. By Manin-Mumford/$\overline{\mathbb{Q}}$, for each $q \in \Delta(\overline{\mathbb{Q}})$, one has $\bigcup_{i=1}^m T_i \subset \mathcal{V}_q$. Since $\mathcal{V}$ is closed, this means $\bigcup_{i=1}^m T_i \subset V_p = V$. To finish, teke Zariski closures, $\bigcup_{i=1}^m T_i^{\text{Zar}} = V$. ■

  Somehow by passing to the real category, get some uniformity statement with these T_i's or some-thing? I'...

[8]Can do this because of a descending chain condition holding in the background of this argument.

4.2.1 André-Oort

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field, with ring of integers $\mathscr{O}_K$. Consider also the class group $\mathrm{Cl}(K)$ (think of as "shapes of lattices that you get as ideals inside K"). There is a bijection $\mathrm{Cl}(K) \xrightarrow{\sim} Y(1)_{CM,d}$ w/ the RHS being elliptic curves E s.t. $\mathrm{End}(E) = \mathscr{O}_K$. This map is simply

$$[I] \mapsto \mathbb{C}/I.$$

This description also tells us how the Galois group acts. $G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Cl}(K) \curvearrowright \mathrm{Aut}(Y(1)_{CM,d})$. Here, $\mathrm{Cl}(K)$ acts by multiplication on $\mathrm{Cl}(K) \simeq Y(1)_{CM,d}$; alternatively, by tensoring with an elliptic curve. One knows

$$\# \mathrm{Cl}(K) = d^{1/2+o(1)},$$

and this is the source of our large Galois orbits.

For $Y(1)^2$, the special curves are

(i) Hecke correspondences $T_N \subset Y(1)^2$, $T_N = Z(\Phi_N)$ (this is abstractly isomorphic to $Y_0(N)$)

(ii) Fibers $Y(1) \times \{p\}$ or $\{p\} \times Y(1)$, with P a CM point

Theorem 4.2.5 (André)**.** *If $C \subset Y(1)^2$ is an irreducible curve, and $(C \cap Y(1)^2_{CM})$ is infinite (i.e. Zariski dense), then C is special.*

Let's end by indicating why the intersection theory proof does not go through here (apparently, it does if you assume Riemann).

Say $(x, z) \in C$ and $x, z \in Y(1)_{CM,d}$ (apprently easier when they have CM by different discriminants). Let $\mathfrak{p} \subset \mathscr{O}_K$ be a prime with $[\mathscr{O}_K : \mathfrak{p}] = p$. Then, $([\mathfrak{p}]x, [\mathfrak{p}]y) \in G_{\mathbb{Q}} \cdot (x, y)$, and will be contained in $C \cap (T_p \times T_p)C$. By Bezout, if the degree of this intersection is too small compared to the number of Galois orbits, we'll have a problem.

One needs $p \leq d^{1/4+o(1)}$, i.e. we need small split primes. This is implied by GRH. Given this, one concludes that $C \subset (T_p \times T_p)C$. One then needs an additional argument to conclude that C is one of these Hecke curves.

4.3 Lecture 3 (3/6)

Would like to say something about Shimura varieties today.

Let $\mathcal{H}$ be a Hermitian symmetric space, so its some complex space for which there is a semisimple group G (say, defined over $\mathbb{Q}$) such that $G(\mathbb{R}) \curvearrowright \mathcal{H}$ (via complex biholomorphisms) transitively, so that

$$G(\mathbb{R})/K \cong \mathcal{H},$$

where K is a maximal compact. In practice, there aren't so so many choices of $\mathcal{H}$ that arise, so while the definition is useful, can also just get acquainted with some key players.

Example 4.3.1. The `Seigal upper half space`

$$\mathbb{H}_g := \left\{ Z \in M_g(\mathbb{C}) : Z = Z^t \text{ and } \operatorname{Im} Z > 0. \right\}$$

This has an action by the symplectic group $G = \mathrm{Sp}_{2g}$ via

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} Z = (AZ + B)(CZ + D)^{-1} \quad \text{where} \quad \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{C}).$$

In finer arithmetic contexts, have to worry e.g. about taking Sp_{2g} v.s. GSp_{2g}, but for this purely complex analytic picture, doesn't really matter. △

To get a Shimura variety, want to quotient out by a discrete subgroup. So take $\Gamma = G(\mathbb{Z})$ or something `commensurable` with $G(\mathbb{Z})$, i.e.

$$[\Gamma : G(\mathbb{Z}) \cap \Gamma] < \infty \text{ and } [G(\mathbb{Z}) : \Gamma \cap G(\mathbb{Z})] < \infty.$$

Remark 4.3.2. Because we only care about Γ being commensurable with $G(\mathbb{Z})$, it does not matter what integral model we choose to define $G(\mathbb{Z})$. ∘

The resulting `Shimura variety` is

$$S = S_\Gamma = \Gamma \backslash \mathcal{H}.$$

Theorem 4.3.3. *This S is a quasi-projective variety/$\mathbb{C}$. Furthermore, S has a canonical model over some number field ("reflex field").*

Example 4.3.4. $\mathcal{A}_g := \mathrm{Sp}_{2g}(\mathbb{Z}) \backslash \mathbb{H}_g$ is a Shimura variety. This is in fact the moduli space of principally polarized abelian varieties of dimension g. △

Definition 4.3.5. A point $x \in \mathcal{H}$ is `CM` if $\mathrm{Stab}_{G(\mathbb{R})}(x) \supset T(\mathbb{R})$ for some maximal torus $T \subset G$ defined over $\mathbb{Q}$. We similarly say the corresponding $[x] \in S_\Gamma$ is `CM` as well. ⋄

(One can show that this is a countable set, and that these are defined over some bounded degree number field)

Exercise. Prove that this is the same as the usual definition of CM for $\mathcal{H} = \mathbb{H}$ (usual definition = $\tau \in \mathbb{H}$ is a quadratic irrational)

These CM points are our `special points` in this context. What are the special subvarieties? Which do we expect to have a Zariski dense set of special points?

Suppose we have $G' \subset G$ both semisimple algebraic groups defined over $\mathbb{Q}$. Suppose you further have some $x \in \mathcal{H}$ such that $G'(\mathbb{R}) \cdot x$ is complex analytic (note $G(\mathbb{R}) \cdot x = \mathcal{H}$ is complex analytic). Then, $W := [G'(\mathbb{R}) \cdot x] \subset S_\Gamma$ will be algebraic, and we say this image W is `weakly special`, not necessarily special.

Remark 4.3.6. Why not special? In the multiplicative case, have $\mathbb{C}^\times$ (or $(\mathbb{C}^\times)^n$) with universal cover $\mathbb{C}^n$. Your tori all pull back to vector spaces in $\mathbb{C}^n$. If you take an arbitrary vector space upstairs, its image will be a translate by a torus, but not necessarily a translate by a torsion point. The issue is the analytic theory doesn't easily see the algebra. ∘

We say W is `special` if it contains a CM point. In this case, act on it by $G'(\mathbb{R})$ to get a dense subset of CM points.

Remark 4.3.7. Say $G'(\mathbb{R}) \cdot x$ is analytic. One can see that $W = [G'(\mathbb{R}) \cdot x] \subset S_\Gamma$ will be algebraic using o-minimality. Check that W is definable, and then use definable Chow to say complex analytic definable things are algebraic. ∘

Theorem 4.3.8 (André-Oort)**.** *Let $V \subset S_\Gamma$. Then, V contains finitely many maximal special subvarieties.*

(Apparently, André and Oort both say the history of this conjecture given on Wikipedia is wrong)

Question 4.3.9 (Audience)**.** *Is the version with weakly special subvarieties false?*

Answer. Yes. Think about the multiplicative case. Then you're asking if you contain only finitely many torus cosets (as opposed to torsion cosets). Take e.g. $\mathbb{C}^\times \times S$ for your favorite $S \subsetneq (\mathbb{C}^\times)^{n-1}$. ⋆

4.3.1 Galois Orbits

Let $X \in \mathcal{A}_g$ be a CM field. Then, the corresponding abelian variety will be

$$A_x = \mathbb{C}/I,$$

where $[I] \in \mathrm{Cl}(K)$ and $K/\mathbb{Q}$ is some CM field of degree $2g$. Call the set of CM points that look like this M_K. One can show that

$$\#M_K \sim \frac{\#\,\mathrm{Cl}(K)}{\#\,\mathrm{Cl}(K_0)} \sim \left|\frac{D_K}{D_{K_0}}\right|^{1/2+o(1)}$$

(K_0 is the totally real subfield). In the elliptic curve case, M_K is a single Galois orbit, but this is no longer true in general. Let $L = K^{\mathrm{Gal}}$ be the Galois closure. Then, there is a map

$$\varphi : \mathrm{Cl}(L) \longrightarrow \mathrm{Cl}(K)$$

such that $\operatorname{im} G_{\mathbb{Q}} \approx \operatorname{im}\varphi$.[9] Instead of the Galois group action looking like a class group, it looks like the image of one class group inside another. We need $\operatorname{im}\varphi$ to be large.

Example 4.3.10. Say $L = K$ and φ is multiplication by m. In this case

$$|\operatorname{im}\varphi| = |\mathrm{Cl}(K)/\,\mathrm{Cl}(K)[m]|\,.$$

We know the class group is large, so just need to know that it's not all m-torsion. This is surprisingly hard in general.

Conjecture 4.3.11 (Zhang, Brumer-Silverman)**.** $\#\,\mathrm{Cl}(K)[m] = |D_K|^{o(1)}$ *for fixed* m*.*

In general, can't prove anything better than the trivial bound $|D_K|^{1/2+o(1)}$. △

Remark 4.3.12. Now that we have (independently) lower bounds for Galois orbits, could reverse engineer them to obtain upper bounds for Galois orbits. Sound like no one's done this, and doing so might be tricky. ○

This approach does not work to bound Galois orbits, but we do learn something from it. We learn that all points in M_K are defined over the same number field. Hence, if one of them has small Galois orbits, then many of them have small Galois orbits.

What else could one try?

Slogan. Upper bounds for heights give lower bounds for Galois orbits

How do you get upper bounds for heights? That's hard to.

Let's explain how this works e.g. for multiplicative groups.

Example 4.3.13. Imagine you were bad at arithmetic (so couldn't compute $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$), but knew o-minimality and point counting, and you wanted to prove roots of unity have large fields of definition. Here's an idea due to Schmidt. Consider

$$\mu_n^\times = \left\{x \in \mathbb{C}^\times : \mathrm{ord}(x) = n\right\}.$$

Consider also

$$I = \left\{(t, e^{2\pi i t}) : t \in [0,1]\right\} \subset \mathbb{C} \times \mathbb{C}^\times.$$

[9] $\operatorname{im} G_{\mathbb{Q}}$ under its action on CM points, i.e. $G_{\mathbb{Q}} \to \mathrm{Aut}(M_K)$ (bijections of the set), and we mean its image under this map

Note that if $x \in \mu_n^\times$, then $H(x) = 1$ (height, appropriately defined). Hence,

$$H\Big(\frac{a}{n}, e^{2\pi ia/n}\Big) = H\Big(\frac{a}{n}\Big) = n.$$

Exercise. $I^{\text{alg}} = \emptyset$ (Hint: I is one-dimensional)

Thus, we learn that

$$N_{\mathbb{Q}(\mu_n)}(I, n) \geq \#\mu_n^\times = n^{1-o(1)}.$$

If we could apply Pila-Wilkie counting, we'd get a contradiction b/c this would need to grow slower than any power of n.

Remark 4.3.14*.* This gives a new proof that roots of unity are not defined over $\mathbb{Q}$ or any field of bounded degree. ○

Need a version of Pila-Wilkie that let's you degree grow. This was recently obtained (by Binyamini?), e.g. saying

$$N_K(X \setminus X^{\text{alg}}, T) = T^{o(1)}[K : \mathbb{Q}]^{O(1)}.$$

This no longer holds in a general o-minimal structure, but in practice, we don't work w/ arbitrary o-minimal structures. This now shows that

$$[\mathbb{Q}(\mu_n) : \mathbb{Q}] \geq n^\delta \text{ for some } \delta > 0.$$

Note this is using the (easy) fact that all elements of $\mu_n^\times$ are defined over the same number field. △

Theorem 4.3.15 (Binyahini-Schmidt-Yafaev)**.** *Upper bounds for heights (of CM points) imply lower bounds for Galois orbits.*

Let's end by saying a little bit about where these upper bounds come from.

Proof of upper bounds. One uses something called the `Colmez conjecture`: say $s \in \mathcal{A}_g$ is CM. Then,

$$h_{\text{Fal}}(x) = \sum (L\text{-values}).$$

If you know this conjecture, to bound heights of CM points, just bound some values of some L-functions, which people are better at. This conjecture is not known, but an average version is known.

Theorem 4.3.16 (Average Colmez)**.** *If you average over many CM points, then you get an equality like this.* ■

There's a more concrete proof for elliptic curves.

Proof "Sketch" of upper bounds for $Y(1)$. Given a CM point $x \in Y(1)$, its height is $h(x) = h(j(x))$. CM curves has everywhere potentially good reduction, so $j(x)$ is an algebraic integer, and the only contribution to the height is the infinite place. Hence,

$$h(x) = h(j(x)) = \sideset{}{'}\sum_{z \in Y(1)_{CM,d}} \log|j(z)| \sim \sum_{z \in Y(1)_{CM,d}} y.$$

(the log of the j-function is essentially the y coordinate). Somehow this then amounts to bounding the number of ideal classes of norm $\leq k$. ■

4.4 Lecture 4 (3/7)

Goal. "My goal of the final lecture is to one up Jonathan" – Jacob

Sounds like we want to set up a very general picture using Hodge theory.

4.4.1 Hodge Theory

(from the perspective of special point problems)

Let V be an algebraic variety.

Assumption. For now, assume V is smooth and projective.

The idea behind Hodge theory is that algebraic variety are complicated, nonlinear objects. We want to recover properties of them from complicated, linear objects instead, so we study cohomology. We have

- Betti cohomology $\mathrm{H}^n(V, \mathbb{C})$
- de Rham cohomology $\mathrm{H}^n_{dR}(V)$. This is isomorphic to the above (Poincaré)

  So far have no moduli. All complex vector space of given dimension are isomorphisc.

We have more data though. We have $\mathrm{H}^n(V, \mathbb{Z}) \subset \mathrm{H}^n(V, \mathbb{C})$ a lattice. All $\mathbb{C}$-vector spaces w/ lattice are isom, so no moduli yet. However, we also have Hodge decomposition

$$\mathrm{H}^n_{dR}(V) = \bigoplus_{i+j=n} \mathrm{H}^{i,j}$$

with $\mathrm{H}^{i,j}$ being closed (i,j)-forms modulo exact (i,j)-forms. An (i,j)-form locally looks like $\mathrm{d}z_1 \wedge \cdots \wedge \mathrm{d}z_i \wedge \mathrm{d}\overline{z}_1 \wedge \cdots \wedge \mathrm{d}\overline{z}_j$. This by itself would not give us moduli, but taken with the lattice, it does.

Definition 4.4.1. A `Hodge structure of weight` n is a tuple

$$\left(L, L_{\mathbb{C}} = \bigoplus_{i+j=n} L^{i,j} \right)$$

with L a lattice (free $\mathbb{Z}$-module), $L_{\mathbb{C}} = L \otimes_{\mathbb{Z}} \mathbb{C}$, and $\overline{L^{i,j}} = L^{j,i}$. $\diamond$

Example 4.4.2. Say $E = \mathbb{C}/L$ ia an elliptic curve. In fact, say $L = \langle 1, \tau \rangle$. Then,

$$\mathrm{H}^1(E, \mathbb{Z}) \simeq L^\vee = \mathrm{Hom}(L, \mathbb{Z}) \text{ and } \mathrm{H}^1_{\mathrm{dR}}(E) = \mathbb{C}\mathrm{d}z \oplus \mathbb{C}\mathrm{d}\overline{z}.$$

The Poincaré isomorphism $\mathrm{H}^1_{dR}(E) \xrightarrow{\sim} \mathrm{H}^1(E, \mathbb{C})$ is integration

$$\omega \mapsto \left[\gamma \mapsto \int_\gamma \omega \right].$$

Hence,

$$\mathrm{d}z \mapsto ([1] \mapsto 1 \text{ and } [\tau] \mapsto \tau).$$

This information is in fact enough to recover the full elliptic curve. Note $\mathrm{H}^1(E, \mathbb{C}) / \mathrm{H}^{1,0} \xrightarrow{\sim} \mathbb{C}$ via $f \mapsto f([\tau]) - f([1]) - \tau$. Therefore,

I feel like this should be $f([\tau]) - f([1]) - (\tau - 1)$

$$\frac{\mathrm{H}^1(E, \mathbb{C})}{\mathrm{H}^{1,0} + \mathrm{H}^1(E, \mathbb{Z})} \xrightarrow{\sim} \frac{\mathbb{C}}{\langle -\tau, 1 \rangle} \simeq E. \qquad \triangle$$

Remark 4.4.3 (Technicalities).

- Need to work with primitive cohomology $\mathrm{H}^k_{\mathrm{prim}} \subset \mathrm{H}^k$.
- Work w/ polarizations, so add some quadratic form $Q : L \times L \to \mathbb{Z}$
- There's some positive condition we're not talking about (related to $\mathbb{H}$ vs. $\mathbb{C} \setminus \mathbb{R}$) ◦

This is what a Hodge structure is; it is this weird linear data. Can we make sense of Hodge structures being CM/special? For abelian varieties/elliptic curves, we relied on endomorphisms. The special ones had the most possible endomorphisms. Can do something similar here, but we'll take a different approach instead.

4.4.2 CM Hodge structures

Say $L^\bullet = \left(L, L_{\mathbb{C}} = \bigoplus_{i+j=n} L^{i,j}\right)$ is a Hodge structure, and assume $2 \mid n$.

Definition 4.4.4. We say $v \in L_{\mathbb{Z}}$ is a `Hodge class` (or that v is `Hodge`) if $v \in L^{n/2,n/2}$. We say $L^\bullet$ is `CM` if it has "many" Hodge classes. ⋄

This is not quite the write definition of CM. For example, it gives nothing for odd n. We can fix this can looking at tensor powers.

Definition 4.4.5. $L^\bullet$ is `CM` if $(L^\bullet)^{\otimes m}$ has many Hodge classes. ⋄

Question 4.4.6 (Audience)**.** *What is many?*

Answer. It is as many as possible. A little more concretely, it means you have enough that you cannot deform the decomposition (while preserving Hodge classes) at all. We'll talk about moduli theory in a second. ⋆

Example 4.4.7. Say E is a CM elliptic curve. Then, $\mathrm{H}^1(E, \mathbb{Z})$ will have no Hodge classes because 1 is odd. However, $\mathrm{H}^1(E, \mathbb{Z})^{\otimes 2} \supset \mathrm{H}^2(E \times E, \mathbb{Z})$ and this latter group contains the class $[\Gamma_\varphi]$ of the graph Γ_φ of $\varphi \in \mathrm{End}(E)$. These will turn out to be Hodge classes. △

What's the motivation? Say we have a smooth, projective V and $W \subset V$ w/ $\operatorname{codim}_{\mathbb{C}} W = k$. Then, we get a class $[W] \in \mathrm{H}^{2k}(V, \mathbb{Z})$. Furthermore,

$$\int_W \omega = 0 \text{ if } \omega \text{ is } (i,j) \text{ and } (i,j) \neq (k,k).$$

This is simply because, in this case, $\omega|_W = 0$ since the only $2k$ forms W supports are (k,k)-forms.

Conjecture 4.4.8 (`Hodge conjecture`)**.** *All Hodge classes in* $\mathrm{H}^{2k}(V)$ *are algebraic up to* $\mathbb{Q}$*-coefficients.*

Conjecture 4.4.9 (`André-Oort for Hodge Structures`, Klingler)**.** *Let $\pi : X \to B$ be a smooth, projective family (imagine a family of Hodge structures). Fix an integer $k \in \mathbb{N}$, and let*

$$B_{CM} := \left\{ b \in B : \mathrm{H}^k(H_b, \mathbb{Z}) \text{ is CM.} \right\}$$

If this set is Zariski dense in B, the there exists some $\varphi : B \to S$ to a Shimura variety such that $B_{CM} = \varphi^{-1}(S_{CM})$.

When talking about elliptic curves, we don't work with an arbitrary family, we work e.g. with $Y(1)$ and powers.

Warning 4.4.10. There's no biggest, universal family of Hodge structures. •

4.4.3 Moduli

Fix some (polarized) Hodge structure $L^\bullet = \left(L, L_\mathbb{C} = \bigoplus_{i+j=n} L^{i,j}, Q\right)$. Consider

$$D = \left\{\{A^{i,j} \subset L_\mathbb{C}\} : \left(L, L_\mathbb{C} = \bigoplus A^{i,j}, Q\right) \text{ is still a H.S. and } \dim A^{i,j} = \dim L^{i,j}\right\}.$$

This will be an (analytic) open in some Grassmannian, but won't be a Hermitian symmetric space in general. Let $G = \mathrm{Aut}(L, Q)$, so $G(\mathbb{R}) \curvearrowright D$. Now,

$$G(\mathbb{Z})\backslash D$$

will be the `moduli space of Hodge structures` "which look like $L^\bullet$."

Warning 4.4.11 (Griffiths + ...)**.** In general, $G(\mathbb{Z})\backslash D$ has no algebraic structure. •

As a result, there is no universal algebraic family of Hodge structures. Given any family $X \to B$, we get a family of Hodge structures by varying the basepoint $b \in B$ and looking at the Hodge structure on the fiber. Hence, we still get these period maps

$$\begin{array}{rccc} \varphi : & B & \longrightarrow & G(\mathbb{Z})\backslash D \\ & b & \longmapsto & \mathrm{H}^k(X_b). \end{array}$$

So we get a locus $(\mathbb{G}(\mathbb{Z})\backslash D)^{\text{geom}} \subset G(\mathbb{Z})\backslash D$, a countable union of algebraic varieties (the union of images of period maps).

Remark 4.4.12. Sounds like (pretty much) the only time you get something algebraic is when you get a Shimura variety. ∘

Shimura varieties are great, but limited (there are so few of them). Hodge structures are much more flexible, but have fewer nice properties in general. It'd be great if we can extend our technology to them.

"Hodge structures are the future, and you should all learn them."

Question 4.4.13. *Does $(G(\mathbb{Z})\backslash D)^{geom}$ have an arithemtic structure? Does it have a Galois action?*

Why wouldn't we be able to get a Galois action. These thing is coming from algebraic varieties, and those have Galois actions.

Question 4.4.14. *Does there exists a pair of varieties V, W such that $\mathrm{H}^k(V) \cong \mathrm{H}^k(W)$ as Hodge structures, but $\exists \sigma \in \mathrm{Aut}(\mathbb{C})$ such that $\mathrm{H}^k(\sigma(V)) \not\cong \mathrm{H}^k(\sigma(W))$?*

If so, we're sad.

Conjecture 4.4.15 (`Absolute Hodge conjecture`)**.** *Say $\ell \in \mathrm{H}^k_{dR}(V)$ is Hodge and $\sigma \in \mathrm{Aut}(\mathbb{C})$. Is $\sigma(\ell) \in \mathrm{H}^k_{dR}(\sigma(V))$ Hodge as well? The conjecture says the answer is yes.*

Hodge conjecture $\implies$ absolute Hodge conjecture. Hodge says $\ell = [W]$ for some $W \subset V$, so then $\sigma(\ell) = [\sigma(W)]$ is Hodge as well. AHC would allow us to get an arithmetic action on our geometric locus.

Theorem 4.4.16 (Deligne)**.** *Absolute Hodge conjecture holds for abelian varieties.*

(Voisin, Urbanic, ... have extended the techniques of Deligne's proof)

Sounds like Deligne's proof using that we have this large family $\mathcal{A}_g$ with a dense set of CM points (defined over $\overline{\mathbb{Q}}$) where things are well understood.

Warning 4.4.17. We do not know HC for abelian varieties (we do for H^2) •

AHC implies that for any $X \to B$ defined over $\overline{\mathbb{Q}}$, B_{CM} is also defined over $\overline{\mathbb{Q}}$. Moreover, the Galois action on B_{CM} would still be described by some sort of "theory of complex multiplication." You'd get new reflex maps. If we knew enough about this kind of picture, we could prove all sorts of results (e.g. conjecture on torsion in class groups).

The discussion so far includes the picture of Shimura varieties. If you pass from Hodge structures to mixed Hodge structures, then you'll include the world of mixed Shimura varieties. A mixed Hodge structure is the sort of thing you get from looking at $\mathrm{H}^k(V)$ for V not necessarily smooth or proper.

Example 4.4.18. Pick point $p \in \mathbb{C}^\times \setminus \{1\}$. Look at $\mathrm{H}^1_{\mathrm{rel}}(\mathbb{C}^\times, \{1, p\})$. This is an extension

$$0 \longrightarrow \mathbb{Z} \cdot ([p] - [1]) \longrightarrow \mathrm{H}^1_{rel}(\mathbb{C}^\times, \{1, p\}) \longrightarrow \mathrm{H}^1(\mathbb{C}^\times) \longrightarrow 0.$$

The (co)kernel are trivial Hodge structures. The moduli space of such things is $\mathbb{G}_m$, and the CM points are exactly the torsion points in $\mathbb{G}_m$. △

5 Boris Zilber

5.1 Lecture 1 (3/4): Classification theory, stability and analyticity

Note 4. Slide talk, so little chance I keep up...

`Structures` are given as $M := (M, \sigma)$ with σ a vocabulary (singature, language).

Example 5.1.1. $\mathbb{C}_{\text{field}} = (\mathbb{C}; +, \cdot)$. Note that the metric is not definable in this structure. △

Goal. Classify (theories of) structures w.r.t. their definability (expressibility) properties in the given language.

Example 5.1.2 (?)**.** The property of $\mathrm{Th}(M)$ to define its model of cardinarlity κ uniquely up to isomorphism: κ-`categoricity`. In fact (Morley, 1964), if $\kappa_1, \kappa_2 > \aleph_0$, then κ_1-categorcity $= \kappa_2$-categoricity. △

Note 5. I'm not sure where this is going, so I think gonna go ahead and stop...

See the winter school's webpage for slides probably

6 List of Marginal Comments

Index