Projective geometries arising from Elekes-Szabó problems

Martin Bays
Joint work with Emmanuel Breuillard

13-11-2018
Oxford

Elekes-Szabó

- Suppose $f \in \mathbb{C}[X, Y, Z]$ is an irreducible polynomial in which each of X, Y, Z appears.
- Set $V := \{(x, y, z) \in \mathbb{C}^3 : f(x, y, z) = 0\}$.
- Consider intersections with finite "grids" $A \times B \times C$ with $|A|, |B|, |C| \leq N \in \mathbb{N}$.
- We have

$$|V \cap (A \times B \times C)| \leq O(N^2).$$

- Say V "admits no powersaving" if for no $\epsilon > 0$ do we have

$$|V \cap (A \times B \times C)| \leq O(N^{2-\epsilon}).$$

- Example: if $f(x, y, z) = z - x - y$ then arithmetic progressions $A = B = C := [-m, m]$ witness that V admits no powersaving.

Theorem (Elekes-Szabó 2012)

V admits no powersaving iff V is in co-ordinatewise algebraic correspondence with the graph of addition on a 1-dimensional algebraic group.

Pseudofinite dimension

Hrushovski "On Pseudo-Finite Dimensions" (2013)

- $\mathcal{U} \subseteq \mathbb{P}(\omega)$ non-principal ultrafilter.
- $K := \mathbb{C}^{\mathcal{U}}$.
- $X \subseteq K^n$ is **internal** if $X = \prod_{s \to \mathcal{U}} X_s$ for some $X_s \subseteq \mathbb{C}^n$, and **pseudofinite** if each X_s is finite.
- For X internal, set $|X| := \lim_{s \to \mathcal{U}} |X_s| \in \mathbb{R}^{\mathcal{U}} \cup \{\infty\}$.
- $|X| \in \mathbb{R}^{\mathcal{U}}$ if X is pseudofinite, $|X| := \infty$ else.
- Fix $\xi \in \mathbb{R}^{\mathcal{U}}$ with $\xi > \mathbb{R}$.

Definition (Coarse pseudofinite dimension δ)

For X internal,

$$\boldsymbol{\delta}(X) = \boldsymbol{\delta}_\xi(X) := \operatorname{st}\left(\log_\xi(|X|)\right) \in \mathbb{R}_{\geq 0} \cup \{-\infty, \infty\}.$$

- Note that internality is closed under cardinality quantifiers: if $R \subseteq K^n \times K^m$ is internal and $\alpha \in \mathbb{R}^{\mathcal{U}}$, then $\{\overline{y} \in K^n : \exists_{\geq \alpha} \overline{x}. R(\overline{x}, \overline{y})\}$ is internal.

$\mathcal{L}_{\text{int}}$ monster

- $\mathcal{L}_{\text{int}}$: predicate for each internal $X \subseteq K^n$.
- $\mathbb{K} \succ K$ monster model in $\mathcal{L}_{\text{int}}$.
- For $\phi \in \mathcal{L}_{\text{int}}$, set $\boldsymbol{\delta}(\phi) := \boldsymbol{\delta}(\phi(K))$.
- $\boldsymbol{\delta}$ has a unique extension to $(\mathcal{L}_{\text{int}})_{\mathbb{K}}$ such that

$$\mathrm{tp}(\overline{b}) \mapsto \boldsymbol{\delta}(\phi(\overline{x}, \overline{b}))$$
$$S_{\overline{y}}(\emptyset) \to \{-\infty\} \cup \mathbb{R} \cup \{\infty\}$$

  is well-defined and continuous for each $\phi(\overline{x}, \overline{y}) \in \mathcal{L}_{\text{int}}$.
- Explicitly, $\boldsymbol{\delta}(\phi(\overline{x}, \overline{a})) := \sup\{q \in \mathbb{Q} : \mathbb{K} \models \exists_{\geq \xi^q} \overline{x}.\ \phi(\overline{x}, \overline{a})\}$.

$\mathcal{L}_{\text{int}}$ monster

- $\mathcal{L}_{\text{int}}$: predicate for each internal $X \subseteq K^n$.
- $\mathbb{K} \succ K$ monster model in $\mathcal{L}_{\text{int}}$.
- For $\phi \in \mathcal{L}_{\text{int}}$, set $\boldsymbol{\delta}(\phi) := \boldsymbol{\delta}(\phi(K))$.
- δ has a unique extension to $(\mathcal{L}_{\text{int}})_{\mathbb{K}}$ such that

$$\operatorname{tp}(\overline{b}) \mapsto \boldsymbol{\delta}(\phi(\overline{x}, \overline{b}))$$
$$S_{\overline{y}}(\emptyset) \to \{-\infty\} \cup \mathbb{R} \cup \{\infty\}$$

  is well-defined and continuous for each $\phi(\overline{x}, \overline{y}) \in \mathcal{L}_{\text{int}}$.
- Explicitly, $\boldsymbol{\delta}(\phi(\overline{x}, \overline{a})) := \sup\{q \in \mathbb{Q} : \mathbb{K} \vDash \exists_{\geq \xi^q} \overline{x}.\ \phi(\overline{x}, \overline{a})\}$.
- For Φ a partial type, $\boldsymbol{\delta}(\Phi) := \inf\{\boldsymbol{\delta}(\phi) : \Phi \vDash \phi\}$.
- $\boldsymbol{\delta}(a/C) := \boldsymbol{\delta}(\operatorname{tp}(a/C))$.

Fact

For $C \subseteq \mathbb{K}$ small and $a, b \in \mathbb{K}^{<\omega}$,

- *(**Invariance**): $a \equiv_C b \implies \delta(a/C) = \delta(b/C)$.*
- *(**Additivity**): $\delta(ab/C) = \delta(a/bC) + \delta(b/C)$.*
- *(**Existence**): A partial type Φ over C has a realisation $a \in \Phi(\mathbb{K})$ with $\delta(a/C) = \delta(\Phi)$.*

acl^0

For V a variety over $\mathbb{K}$, eliminate the imaginary to consider elements of $V(\mathbb{K})$ as tuples from $\mathbb{K}$, i.e. $V(\mathbb{K}) \subseteq \mathbb{K}^{<\omega}$.

Definition

Superscript 0 means: reduct to $\mathrm{ACF}_{\mathbb{C}}$.
$(\mathbb{C} \leq \mathbb{C}^{\mathcal{U}} = K \prec \mathbb{K})$

- $d^0(A/B) := \mathrm{trd}(\mathbb{C}(A, B)/\mathbb{C}(B))$ (for $A, B \subseteq \mathbb{K}^{<\omega}$)
- $\mathrm{acl}^0(B) := \{a \in \mathbb{K}^{<\omega} : d^0(a/B) = 0\}$ = field-theoretic algebraic closure of $\mathbb{C}(B)$ in $\mathbb{K}^{<\omega}$.

Remark

$a \in \mathrm{acl}^0(B) \implies \delta(a/B) = 0$.

Coherence (1-dimensional version)

Definition

$P \subseteq \mathbb{K}$ is **coherent** if for any tuple $\overline{a} \in P^{<\omega}$,

$$\delta(\overline{a}) = d^0(\overline{a}).$$

In other words, δ is equal on $P^{<\omega}$ to the dimension function of the pregeometry $(P; \mathrm{acl}^0)$.

Coherence (1-dimensional version)

Definition

$P \subseteq \mathbb{K}$ is **coherent** if for any tuple $\overline{a} \in P^{<\omega}$,

$$\delta(\overline{a}) = d^0(\overline{a}).$$

In other words, δ is equal on $P^{<\omega}$ to the dimension function of the pregeometry $(P; \mathrm{acl}^0)$.

Lemma

Say an irreducible complex variety $V \subseteq \mathbb{A}^n$ "admits no powersaving" if for no $\epsilon > 0$ do we have a bound

$$|V(\mathbb{C}) \cap \prod_i A_i| \leq O(N^{\dim(V)-\epsilon}),$$

for $A_i \subseteq \mathbb{C}$ with $|A_i| = N$.
Then V admits no powersaving iff there exists a generic point $\overline{a} \in V(\mathbb{K})$ with $\{a_1, \ldots, a_n\}$ coherent.

Coarse general position

Definition

$a \in \mathbb{K}^{<\omega}$ is in **coarse general position** (or is **cgp**) if for any $B \subseteq \mathbb{K}$,

$$d^0(a/B) < d^0(a) \Longrightarrow \delta(a/B) = 0.$$

Any $a \in \mathbb{K}$ is cgp.

Definition

Let W be an irreducible variety over $\mathbb{C}$.
A $\mathbb{K}$-definable set $X \subseteq W(\mathbb{K})$ with $\delta(X) \in \mathbb{R}_{>0}$ is **cgp** if for any $W' \subsetneq W$ proper subvariety over $\mathbb{K}$,

$$\delta(X \cap W') = 0.$$

If X is cgp, then any $a \in X$ is cgp.

Coherence

Definition

$P \subseteq \mathbb{K}^{<\omega}$ is **coherent** if

- every $a \in P$ is cgp, and
- for any tuple $\overline{a} \in P^{<\omega}$, $d^0(\overline{a}) = \delta(\overline{a})$.

Then $(P; \mathrm{acl}^0)$ is a pregeometry, and if $d^0(a)$ is constant for $a \in P$, then δ is proportional on $P^{<\omega}$ to its dimension function.

Example

Let G be a complex semiabelian variety, e.g. $G = (\mathbb{C}^\times)^n$.
Let $\gamma \in G(\mathbb{C})$ generic.
Let $X := \prod_{s \to \mathcal{U}} \{-s \cdot \gamma, \ldots, s \cdot \gamma\}$, and set ξ such that $\delta(X) = \dim(G)$.
Then X is cgp, since $|X \cap W'| < \aleph_0$ by uniform Mordell-Lang.
Now $\delta(X^3 \cap \Gamma_+) = 2\delta(X)$.
Let $(a, b, c) \in X^3 \cap \Gamma_+$ with $\delta(abc) = 2\delta(X)$.
Then $\{a, b, c\}$ is coherent.

Szemerédi-Trotter bounds

Suppose $a, e \in \mathbb{K}^{<\omega}$ satisfy (working over some $C \subseteq \mathbb{K}$):
If $e' \equiv e$ and $e' \equiv^0_a e$ but $e' \neq e$, then $\delta(a/ee') = 0$.

Lemma (Trivial bound)

Assume such a e' exists (i.e. $e \notin \mathrm{dcl}(a)$).
Then $\delta(a/e) \leq \frac{1}{2}\delta(a)$.

Proof.

Take $e' \equiv_a e$ with $e' \neq e$ and $\delta(e'/ab) = \delta(e'/a)$.
Then $0 = \delta(a/ee') = \delta(aee') - \delta(ee') = 2\delta(ab) - \delta(a) - \delta(ee') \geq 2\delta(a/e) - \delta(a)$. $\square$

Szemerédi-Trotter bounds

Suppose $a, e \in \mathbb{K}^{<\omega}$ satisfy (working over some $C \subseteq \mathbb{K}$):
If $e' \equiv e$ and $e' \equiv^0_a e$ but $e' \neq e$, then $\delta(a/ee') = 0$.

Lemma (Trivial bound)

Assume such a e' exists (i.e. $e \notin \mathrm{dcl}(a)$).
Then $\delta(a/e) \leq \frac{1}{2}\delta(a)$.

Proof.

Take $e' \equiv_a e$ with $e' \neq e$ and $\delta(e'/ab) = \delta(e'/a)$.
Then $0 = \delta(a/ee') = \delta(aee') - \delta(ee') = 2\delta(ab) - \delta(a) - \delta(ee') \geq 2\delta(a/e) - \delta(a)$. $\square$

Lemma (Szemerédi-Trotter bound due to Elekes-Szabó)

Assume $\delta(e) > \frac{1}{2}\delta(a) > 0$.
Then $\delta(a/e) < \frac{1}{2}\delta(a)$.

Hrushovski: Szemerédi-Trotter bounds correspond to modularity.

Modularity

Recall

- A **geometry** is a pregeometry with $\mathrm{cl}(\emptyset) = \emptyset$ and $\mathrm{cl}(\{x\}) = \{x\}$.
- The geometry of a pregeometry $(P; \mathrm{cl})$ is $(\{\mathrm{cl}(x) : x \in P\}; \mathrm{cl})$.

Definition

- A geometry (P, cl) is **modular** if for $a, b \in P$ and $C \subseteq P$, if $a \in \mathrm{cl}(bC) \setminus \mathrm{cl}(C)$ then there exists $c \in \mathrm{cl}(C)$ such that $a \in \mathrm{cl}(bc)$.
- Say $a, b \in P$ are **non-orthogonal** if $a \in \mathrm{cl}(bC) \setminus \mathrm{cl}(C)$ for some $C \subseteq P$.

Fact (Veblen-Young co-ordinatisation theorem)

The modular geometries of dimension ≥ 4 in which every two points are non-orthogonal are precisely the projective geometries $\mathbb{P}_F(V)$ of vector spaces of dimension ≥ 4 over division rings.

Linearity

Lemma

Suppose $P \subseteq \mathbb{K}^{<\omega}$ *is coherent,* $a_1, a_2, b_1, \ldots, b_n \in P$*, and:*

- $d^0(a_1) = k = d^0(a_2)$;
- $a_1 \in \mathrm{acl}^0(a_2\overline{b}) \setminus \mathrm{acl}^0(\overline{b})$ *and* $a_1 \notin \mathrm{acl}^0(a_2)$.

Let $e := \mathrm{Cb}^{\mathrm{ACF}}(\overline{a}/\mathbb{C}(\overline{b}))$*. Then* $d^0(e) = k$*.*
Moreover, e is cgp, so $\{e\}$ *is coherent.*

Linearity

Lemma

Suppose $P \subseteq \mathbb{K}^{<\omega}$ is coherent, $a_1, a_2, b_1, \ldots, b_n \in P$, and:

- $d^0(a_1) = k = d^0(a_2)$;
- $a_1 \in \mathrm{acl}^0(a_2\overline{b}) \setminus \mathrm{acl}^0(\overline{b})$ *and* $a_1 \notin \mathrm{acl}^0(a_2)$.

Let $e := \mathrm{Cb}^{\mathrm{ACF}}(\overline{a}/\mathbb{C}(\overline{b}))$. *Then* $d^0(e) = k$.
Moreover, e is cgp, so $\{e\}$ is coherent.

Proof.

By cgp and canonicity, if $e' \equiv e$ and $e' \equiv^0_a e$ but $e' \neq e$, then $\delta(\overline{a}/ee') = 0$.
But $\delta(\overline{a}/e) \geq \delta(\overline{a}/\overline{b}) = d^0(\overline{a}/\overline{b}) = \frac{1}{2}d^0(\overline{a}) = \frac{1}{2}\delta(\overline{a})$.
So by the Szemerédi-Trotter bounds, we have $\delta(e) \leq \frac{1}{2}\delta(\overline{a})$.
Now $e \in \mathrm{acl}^0(\overline{b})$ and $\overline{b}$ is coherent, and it follows that $d^0(e) \leq \delta(e)$.
So $d^0(e) \leq \delta(e) \leq \frac{1}{2}\delta(\overline{a}) = k$.
…

□

Linearity

Lemma

Suppose $P \subseteq \mathbb{K}^{<\omega}$ is coherent, $a_1, a_2, b_1, \ldots, b_n \in P$, and:

- $d^0(a_1) = k = d^0(a_2)$;
- $a_1 \in \mathrm{acl}^0(a_2\overline{b}) \setminus \mathrm{acl}^0(\overline{b})$ *and* $a_1 \notin \mathrm{acl}^0(a_2)$.

Let $e := \mathrm{Cb}^{\mathrm{ACF}}(\overline{a}/\mathbb{C}(\overline{b}))$. *Then* $d^0(e) = k$.
Moreover, e is cgp, so $\{e\}$ *is coherent.*

Proof.

...

It remains to show that e is cgp.
Suppose $B \subseteq \mathbb{K}^{<\omega}$ and $e \not\downarrow^0 B$; we show $\delta(e/B) = 0$.
Let $\overline{a}' = a'_1 a'_2$ such that $\overline{a}' \equiv_e \overline{a}$ and $\overline{a}' \downarrow^{\delta}_{e} B$. So $e \in \mathrm{acl}^0(\overline{a}')$. Then $\overline{a}' \not\downarrow^0 B$. So since $\overline{a}'$ is coherent, $\delta(\overline{a}'/B) \leq \delta(a'_i) = k$.
Meanwhile, $\delta(\overline{a}'/e) = \delta(\overline{a}') - \delta(e) = d^0(\overline{a}') - d^0(e) = k$. So $\delta(e/B) = \delta(\overline{a}'/B) - \delta(\overline{a}'/eB) = \delta(\overline{a}'/B) - \delta(\overline{a}'/e) \leq k - k = 0$.

□

Modularity of coherence

Definition

For $P \subseteq \mathbb{K}^{<\omega}$, $\mathrm{ccl}(P) := \{x \in \mathrm{acl}^0(P) : \{x\} \text{ is coherent}\}$.

Lemma

If P is coherent, so is $\mathrm{ccl}(P)$.

Proposition

Suppose $P = \mathrm{ccl}(P)$ is coherent.
Then the geometry of $(P; \mathrm{acl}^0)$ is modular.

Projective subgeometries in ACF

Define $\mathbb{P}(\mathbb{K}) := \{\text{acl}^0(x) : x \in \mathbb{K}\}$.

Example

Suppose G is a 1-dimensional complex algebraic group and
$F \leq \mathbb{Q} \otimes_{\mathbb{Z}} \text{End}(G)$ is a subfield.
$G(\mathbb{K})/G(\mathbb{C})$ is naturally an F-vector space.
Let $B \subseteq G(\mathbb{K})$ be a set of independent generics, and set
$V := \langle B/G(\mathbb{C}) \rangle_F$.
Define $\eta : \mathbb{P}_F(V) \to \mathbb{P}(\mathbb{K})$ by $\eta(\langle x/G(\mathbb{C}) \rangle_F) := \text{acl}^0(x)$.
Then η embeds $\mathbb{P}_F(V)$ as a subgeometry of $\mathbb{P}(\mathbb{K})$.

Theorem (Evans-Hrushovski 1991)

Any projective subgeometry of $\mathbb{P}(\mathbb{K})$ of dimension at least 3 arises in this way.

Projective geometries fully embedded in $\mathrm{ACF}^{\mathrm{eq}}$

Define $\mathbb{P}(\mathbb{K}^{<\omega}) := \{\mathrm{acl}^0(x) : x \in \mathbb{K}^{<\omega}\}$.

Definition

$\eta : \mathbb{P}_F(V) \to \mathbb{P}(\mathbb{K}^{<\omega})$ is a ***k*-dimensional full embedding** if for all $\overline{b} \in \mathbb{P}_F(V)^{<\omega}$, we have $d^0(\eta(\overline{b})) = k \cdot \dim_{\mathbb{P}_F(V)}(\overline{b})$.

Example

If G is a complex abelian algebraic group, $F \leq \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(G)$ a division subring, $B \subseteq G(\mathbb{K})$ independent generics, and $V := \langle B/G(\mathbb{C})\rangle_F$. Then $\eta(\langle x/G(\mathbb{C})\rangle_F) := \mathrm{acl}^0(x)$ is a $\dim(G)$-dimensional full embedding.

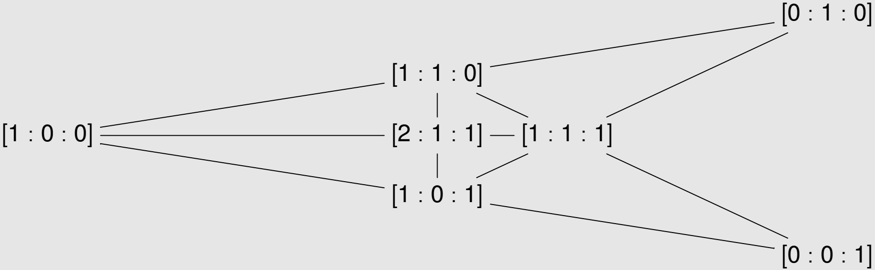
Theorem ("Higher Evans-Hrushovski")

Suppose V is a vector space of dimension at least 3 over a division ring F, and $\eta : \mathbb{P}_F(V) \to \mathbb{P}(\mathbb{K}^{<\omega})$ is a k-dimensional full embedding. Then there are G and embeddings $F \leq \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(G)$ and $V \leq G(\mathbb{K})/G(\mathbb{C})$ such that η is as in the example.

Projective geometries fully embedded in $\mathrm{ACF}^{\mathrm{eq}}$

Proof idea.

Abelian group configuration yields G.



Version due to Faure of the fundamental theorem of projective geometry (semilinearity of projective morphisms) yields embeddings $F \hookrightarrow \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(G)$ and $V \hookrightarrow G(\mathbb{K})/G(\mathbb{C})$. □

Elekes-Szabó consequences

Definition

Say a finite subset X of a variety W is **τ-cgp** if for any proper subvariety $W' \subsetneq W$ of complexity $\leq \tau$, we have $|X \cap W'| < |X|^{\frac{1}{\tau}}$.

Definition

If $V \subseteq \prod_i W_i$ are irreducible complex algebraic varieties, with $\dim(W_i) = m$ and $\dim(V) = dm$, say V **admits a powersaving** if for some τ and $\epsilon > 0$ there is a bound

$$\left| \prod_i X_i \cap V \right| \leq O(N^{d-\epsilon})$$

for τ-cgp $X_i \subseteq W_i$ with $|X_i| \leq N$.

Lemma

V admits no powersaving iff exists coherent generic $\overline{a} \in V(\mathbb{K})$.

Elekes-Szabó consequences

Definition

$H \leq G^n$ is a **special subgroup** if G is a commutative algebraic group and $H = \ker(A)^o$ for some $A \in \mathrm{Mat}(F \cap \mathrm{End}(G))$ for some division subalgebra $F \leq \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(G)$.

Theorem

$V \subseteq \prod_i W_i$ admits no powersaving iff it is in co-ordinatewise algebraic correspondence with a product of special subgroups.

Proof.

$\Longrightarrow$: Take coherent generic; apply modularity of coherence and "higher Evans-Hrushovski".
$\Leftarrow$: see below. $\square$

Sharpness

Fact (Amitsur-Kaplansky)

Any division subring $F \subseteq \mathrm{Mat}_n(\mathbb{C})$ *has finite dimension over its centre.*

Corollary

Any finitely generated subring of a division subring $F \subseteq \mathrm{End}^0(G)$ *is contained in a finitely generated subring* $\mathcal{O} \subseteq F$ *which is* ***constrainedly filtered****: there are finite* $\mathcal{O}_n \subseteq \mathcal{O}$ *such that*

(CF0) $\mathcal{O}_n \subseteq \mathcal{O}_{n+1}; \bigcup_{n\in\mathbb{N}} \mathcal{O}_n = \mathcal{O}$

(CF1) $\exists k.\ \forall n.\ \mathcal{O}_n + \mathcal{O}_n \subseteq \mathcal{O}_{n+k};$

(CF2) $\forall a \in \mathcal{O}.\ \exists k.\ \forall n.\ a\mathcal{O}_n \subseteq \mathcal{O}_{n+k};$

(CF3) $\forall \epsilon > 0.\ \frac{|\mathcal{O}_{n+1}|}{|\mathcal{O}_n|} \leq O(|\mathcal{O}_n|^\epsilon).$

(e.g. $\mathbb{Z} = \bigcup_n [-2^n, 2^n]$ is constrainedly filtered.)
Let "$X_k := \prod_{s\to\mathcal{U}} (\sum_{i=1}^{s} \mathcal{O}_{s-k}\gamma_i)$" with $\gamma_i \in G$ generic independent.
Then $X := \bigcap_k X_k$ is an $\mathcal{O}$-submodule and $\delta(X) = \delta(X_0)$ and X is cgp.
So any special subgroup defined using $\mathcal{O}$ admits no powersaving.

Application: Generalised sum-product phenomenon

Corollary

Let $(G_1, +_1)$ and $(G_2, +_2)$ be one-dimensional non-isogenous connected complex algebraic groups, and for $i = 1, 2$ let $f_i : G_i(\mathbb{C}) \to \mathbb{C}$ be a rational map. Then there are $\epsilon, c > 0$ such that if $A \subset \mathbb{C}$ is a finite set lying in the range of each f_i, then setting $A_i = f_i^{-1}(A) \subseteq G_i(\mathbb{C})$ we have

$$\max(|A_1 +_1 A_1|, |A_2 +_2 A_2|) \geq c|A|^{1+\epsilon}.$$

Proof.

Else, considering $\{(x, y, f_1^{-1}(x) +_1 f_1^{-1}(y), f_2^{-1}(x) +_2 f_2^{-1}(y)) : x, y \in \mathbb{C}\}$, get group $(G; +)$ such that Γ_{+_i} is in co-ordinatewise correspondence with Γ_+, $i = 1, 2$.

But then (by Ziegler) G_i is isogenous to G. □

Similarly in higher dimension, with a cgp assumption.

Application: Intersections of varieties with approximate subgroups

Theorem

$\Gamma \leq G(\mathbb{K})$ a $\emptyset$-$\bigwedge$-definable subgroup of a 1-dimensional algebraic group G, with $\delta(\Gamma) = \dim(G)$.
Then any coherent tuple $\overline{\gamma} \in \Gamma^n$ is generic in a coset of an algebraic subgroup of G^n.

Similarly in higher dimension, with a cgp assumption.

Corollary

Let G be a commutative complex algebraic group. Suppose V is a subvariety of G^n which is not a coset of a subgroup. Then there are $N, \epsilon, \eta > 0$ depending only on G and the complexity of V such that if $A \subseteq G$ is a finite subset such that $A - A$ is τ-cgp and $|A + A| \leq |A|^{1+\epsilon}$ and $|A| \geq N$, then $|A^n \cap V| < |A|^{\frac{\dim(V)}{\dim(G)} - \eta}$.

Diophantine connection

Example

$G = E$ complex elliptic curve.
$E[\infty] := \bigcup_m E[m]$ torsion subgroup.
Suppose $V \subseteq E^n$ is an irreducible closed complex subvariety such that $V(\mathbb{C}) \cap E[\infty]$ is Zariski dense in V. Let $d := \dim(V)$.
By Manin-Mumford, V is a coset of an algebraic subgroup. Hence for any $\epsilon > 0$, for arbitrarily large $r \in \mathbb{N}$,

$$|V(\mathbb{C}) \cap E[r!]^n| \geq |E[r!]|^{d-\epsilon}.$$

Suppose conversely that we only know this consequence of Manin-Mumford on the asymptotics of the number of torsion points in V. Then V has a coherent generic non-standard torsion point, and so by above theorem V is a coset.
Similarly for Mordell-Lang.

Relaxing general position

Remark

$V :=$ graph of $(a_1, b_1) * (a_2, b_2) = (a_1 + a_2 + b_1^2 b_2^2, b_1 + b_2)$,
$X_i := \{-N^4, \ldots, N^4\} \times \{-N, \ldots, N\} \subseteq \mathbb{C}^2 =: W_i$.
Then $|X_i^3 \cap V| \geq \Omega(|X_i|^2)$, but not in coarse general position, and V is not in co-ordinatewise correspondence with the graph of a group operation.

Thanks

Thanks

(Bonus slides follow)

Elekes-Szabó consequences; detailed statement

Definition

$a \in W(\mathbb{K})$ is **dcgp** if $a \in X \subseteq W(\mathbb{K})$ for some $\emptyset$-definable cgp X.

Theorem

Given $V \subseteq \prod_i W_i$, TFAE

(a) *V admits no powersaving.*

(b) *Exists coherent generic $\overline{a} \in V(\mathbb{K})$ with a_i dcgp in W_i.*

(c) *Exists coherent generic $\overline{a} \in V(\mathbb{K})$.*

(d) *V is in co-ordinatewise algebraic correspondence with a product of special subgroups.*

Proof.

$(a) \Leftrightarrow (b)$: ultraproducts.
$(b) \implies (c)$: clear.
$(c) \implies (d)$: modularity of coherence + "higher Evans-Hrushovski".
$(d) \implies (b)$: see below. □

Example

- $G := (\mathbb{C}^\times)^4$.
- $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(G) \cong \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{Mat}_4(\mathbb{Z}) \cong \mathrm{Mat}_4(\mathbb{Q})$.
- $\mathcal{H}_{\mathbb{Q}} = (\mathbb{Q}[i,j,k] : i^2 = j^2 = k^2 = -1;\ ij = k;\ jk = i;\ ki = j)$ embeds in $\mathrm{Mat}_4(\mathbb{Q})$ via the left multiplication representation.
- $\mathcal{H}_{\mathbb{Z}} = \mathbb{Z}[i,j,k] \subseteq \mathcal{H}_{\mathbb{Q}}$ acts on G by endomorphisms:

$$\begin{aligned} n \cdot (a,b,c,d) &= (a^n, b^n, c^n, d^n); \\ i \cdot (a,b,c,d) &= (b^{-1}, a, d^{-1}, c); \\ j \cdot (a,b,c,d) &= (c^{-1}, d, a, b^{-1}); \\ k \cdot (a,b,c,d) &= (d^{-1}, c^{-1}, b, a). \end{aligned}$$

- Then

$$\begin{aligned} V := &\{(x, y, z_1, z_2, z_3) \in G^5 \\ &: z_1 = x + y,\ z_2 = x + i \cdot y,\ z_3 = x + j \cdot y\} \end{aligned}$$

  is a special subgroup of G^5.

Example (continued)

- $V := \{(x, y, z_1, z_2, z_3) \in G^5 : z_1 = x + y,\ z_2 = x + i \cdot y,\ z_3 = x + j \cdot y\}$ is a special subgroup of G^5.
- "Approximate $\mathcal{H}_{\mathbb{Z}}$-submodules" witness that V admits no powersaving:
- $H_N := \{n + mi + pj + qk : n, m, j, k \in [-N, N]\} \subseteq \mathcal{H}_{\mathbb{Z}}$
- $g \in G$ generic
- $X_N := H_N \cdot g = \{h \cdot g : h \in H_N\} \subseteq \mathcal{H}_{\mathbb{Z}} \cdot g \subseteq G$.
- Then (by uniform Mordell-Lang), for $W \subsetneq G$ proper closed of complexity $\leq \tau$, $|W \cap \mathcal{H}_{\mathbb{Z}} g| \leq O_\tau(1)$.
- So $\forall \tau.\ \forall N >> 0.$ X_N is τ-cgp in G.
- But $i \cdot X_N = X_N = j \cdot X_N$, so $|X_N^5 \cap V| \geq \Omega(|X_N|^2)$.