

§2.3: APPLICATION OF BOST'S THEOREM TO SUBGROUPS OF ALGEBRAIC GROUPS
(NOTES FOR THE CLASS OF FARB-KISIN)

DAVE MORRIS

Theorem (Bost's Theorem).

- $X =$ (smooth, connected) algebraic variety over number field K ,
- $\mathcal{F} =$ involutive subbundle of tangent bundle T_X that is def'd/K,
- $L =$ leaf of the corresponding foliation (s.t. L has Liouville property)

If $\mathcal{F} \bmod \mathfrak{p}$ is stable under \mathfrak{p} th power, for a.e. prime \mathfrak{p} of \mathcal{O}_K ,
then L is an algebraic subvariety of X (defined over K).

Let G be an algebraic group over a number field K , i.e.,

- G is a group,
- G is an algebraic variety / K , and
- the group operations $G \times G \xrightarrow{\times} G$ and $G \xrightarrow{\text{inverse}} G$ are regular functions
(in local coordinates, they are polynomials — or rational functions).

(Algebraic geometer's version of a Lie group or topological group.)

Remark.

- $G(\mathbb{C})$ is a complex Lie group.
- If $K \subset \mathbb{R}$, then $G(\mathbb{R})$ is a real Lie group.
- Will usually assume G is connected (but neglect to say).

Two Main Cases.

- (1) G is a projective variety
 $\Rightarrow G$ commutative
(so called "abelian variety")
- (2) G is an affine variety
 $\Rightarrow G \hookrightarrow \text{GL}_n(\mathbb{C})$ for some n (closed embedding, defined over K)
(called "affine algebraic group" or "linear algebraic group")

General case (which "never" arises) is a combination of these two:

$\exists N \triangleleft G$, N affine and G/N projective.

Example. Some affine groups:

- $\text{SL}_n = \{ X \mid \det X = 1 \}$,
- $\text{Unip} = \begin{bmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{bmatrix} = \left\{ X \mid \begin{array}{l} x_{1,1} = 1, x_{2,2} = 1, x_{3,3} = 1, \\ x_{2,1} = 0, x_{3,1} = 0, x_{3,2} = 0 \end{array} \right\}$,
- $\text{Diag} = \begin{bmatrix} * & & \\ & * & \\ & & * \end{bmatrix} \subset \text{SL}_n$,
- $\text{Borel} = \begin{bmatrix} * & * & * \\ & * & * \\ & & * \end{bmatrix} = \text{Diag} \times \text{Unip}$,
- $\text{SO}_n = \{ X \mid X^t X = \mathbf{I} \}$.
- $\text{GL}_n = \begin{bmatrix} A & & \\ & & \\ & & \frac{1}{\det A} \end{bmatrix} \subset \text{SL}_{n+1}$,

$$\bullet \text{ parabolic } P = \begin{bmatrix} \text{GL}_{n_1} & * & * \\ & \text{GL}_{n_2} & * \\ & & \text{GL}_{n_3} \end{bmatrix} \subset \text{GL}_n.$$

Each of these is a subgroup that is defined by polynomial equations in the matrix entries.

Notation.

$$\begin{aligned} \mathfrak{g} &= \text{Lie algebra of } G \\ &= \{\text{left-invariant vector fields on } G\} & [X, Y] &= XY - YX \\ &\cong T_e G. \end{aligned}$$

E.g.,

- Lie alg of $\text{GL}_n = \mathfrak{gl}_n(\mathbb{C}) = \text{Mat}_{n \times n}(\mathbb{C}) \quad [X, Y] = XY - YX$
- Lie alg of Unip = $\mathfrak{unip} = \begin{bmatrix} 0 & * & * \\ & 0 & * \\ & & 0 \end{bmatrix}$
- Lie alg of $\text{SL}_n = \mathfrak{sl}_n(\mathbb{C}) = \{X \in \text{Mat}_{n \times n}(\mathbb{C}) \mid \text{trace } X = 0\}$

Remark.

- H is a Zariski-closed subgroup of $G \implies \mathfrak{h} \hookrightarrow \mathfrak{g}$ (Lie subalgebra).
- $H_1 = H_2 \iff \mathfrak{h}_1 = \mathfrak{h}_2$. (for H_i connected, $\text{char } K = 0$)
- G defined / $K \implies \mathfrak{g}$ has K -structure (i.e., well-defined K -points $\mathfrak{g}_K \subset \mathfrak{g}$)
(As vector space, $\mathfrak{g} \cong \mathbb{C}^n$, such that \mathfrak{g}_K maps to K^n .)

Recall.

- In Lie theory:

$$\text{connected Lie subgroups of } G \xrightarrow{1-1} \text{Lie subalgebras of } \mathfrak{g}$$

- In theory of algebraic groups:

$$\text{Zariski-closed subgroups of } G \xrightarrow{1-1} \text{Lie subalgebras of } \mathfrak{g}$$

usually *not* onto

Lie subalgebras in the image are *algebraic*

Example. Let $G = \mathbb{C}^\times \times \mathbb{C}^\times = \begin{bmatrix} * & \\ & * \end{bmatrix} \subset \text{GL}_2$. Then $\mathfrak{g} = \begin{bmatrix} * & \\ & * \end{bmatrix} \subset \text{Mat}_{2 \times 2}(\mathbb{C}) \cong \mathbb{C}^2$.

The algebraic subalgebras of \mathfrak{g} are precisely those that are defined over \mathbb{Q} .

Proof. Suppose $\mathfrak{h} = \{(z, \alpha z) \mid z \in \mathbb{C}\}$, and \mathfrak{h} is the Lie algebra of some Zariski-closed $H \subset G$.

Say $H = \{(e^{2\pi i z}, e^{2\pi i \alpha z}) \mid z \in \mathbb{C}\}$, for some $\alpha \in \mathbb{C}$.

Since H is algebraic, the projection to the first factor of G must be finite-to-one.

Thus, there is some $n \in \mathbb{Z}$, such that $e^{2\pi i \alpha n} = 1$. So $\alpha \in \mathbb{Q}$. □

Corollary (Bost). Let \mathfrak{h} be a Lie subalgebra of \mathfrak{g} (defined/ K).

\mathfrak{h} is the Lie algebra of some Zariski-closed $H \subset G$ (def'd/ K)

\iff " $\mathfrak{h}_{\mathcal{O}_K} \bmod \mathfrak{p}$ " is closed under p th powers, for a.e. prime \mathfrak{p} of \mathcal{O}_K .

Application (Kronecker's Theorem). $\alpha \in K$ is rational $\iff \alpha \bmod \mathfrak{p} \in \mathbb{F}_p$, for a.e. prime \mathfrak{p} of \mathcal{O}_K .

Proof. (\Leftarrow) Let $G = \mathbb{C}^\times \times \mathbb{C}^\times$, and $\mathfrak{h} = \{(z, \alpha z) \mid z \in \mathbb{C}\} \subset \mathfrak{g}$.

By assumption, $\alpha \bmod \mathfrak{p} \in \mathbb{F}_p$, for a.e. prime \mathfrak{p} of \mathcal{O}_K ; so $\alpha^p \equiv \alpha \pmod{\mathfrak{p}}$.

Thus, for any $z \in \mathcal{O}_K$, we have

$$(z, \alpha z)^p = (z^p, (\alpha z)^p) = (z^p, \alpha^p z^p) \equiv (z^p, \alpha z^p) \in \mathfrak{h}_{\mathcal{O}_K} \pmod{\mathfrak{p}}.$$

So Bost's Corollary implies \mathfrak{h} is algebraic. □

Proof of the corollary.

(\Rightarrow) $\mathfrak{h} \subset \mathfrak{g}$ is a vector space of left-invariant vector fields on G ; it defines a subbundle of TG .

At each point, the distribution is tangent to a coset of H , the Lie subgroup of G associated to \mathfrak{h} .

The exponential map $\mathbb{C}^m \cong \mathfrak{h} \rightarrow H \subset G$ is holomorphic, and is biholomorphic in a neighborhood of 0.

Since \mathbb{C}^m has the Liouville property, this implies that H also has the Liouville property.

So Bost's Theorem implies that the leaf H is Zariski closed (and defined over K). \square

BOST'S COROLLARY IN THE CASE OF LINEAR GROUPS

Remark. Since $G \hookrightarrow \mathrm{GL}_n(\mathbb{C})$, we may assume $G = \mathrm{GL}_n(\mathbb{C})$.

Then $\mathfrak{h} \subset \mathfrak{gl}_n(\mathbb{C}) \cong \mathrm{Mat}_{n \times n}(\mathbb{C})$ (with $[X, Y] = XY - YX$). And $\mathfrak{h}_K = \mathfrak{h} \cap \mathrm{Mat}_{n \times n}(K)$.

Lemma. *The p th power operation on $\mathfrak{h}_{\mathcal{O}_K} \bmod \mathfrak{p}$ coincides with raising a matrix to the p th power.*

Proof. Let $Y \in (\mathfrak{h}_K \bmod \mathfrak{p}) \subset \mathrm{Mat}_{n \times n}(k)$ and $f \in \overline{k}[H]$ (where k is the residue field $\mathcal{O}_K/\mathfrak{p}$).

We have

$$(df)_{\mathbf{I}}(Y) = \left. \frac{\partial}{\partial t} f(\mathbf{I} + tY) \right|_{t=0}.$$

Letting \hat{Y} be the left-invariant vector field with $\hat{Y}_{\mathbf{I}} = Y$, we have

$$(\hat{Y}f)(A) = (\hat{Y}(L_A f))(\mathbf{I}) = (d(L_A f))_{\mathbf{I}}(Y) = \left. \frac{\partial}{\partial t} (L_A f)(\mathbf{I} + tY) \right|_{t=0} = \left. \frac{\partial}{\partial t} f(A(\mathbf{I} + tY)) \right|_{t=0}.$$

Thus,

$$(\hat{Y}^p f)(\mathbf{I}) = \left. \frac{\partial^p}{\partial t_1 \partial t_2 \cdots \partial t_p} f(\mathbf{I}(\mathbf{I} + t_1 Y)(\mathbf{I} + t_2 Y) \cdots (\mathbf{I} + t_p Y)) \right|_{t_1, t_2, \dots, t_p=0}.$$

Since \hat{Y}^p is a derivation, we know $(\hat{Y}^p f)(\mathbf{I})$ depends only on the linear part of f . Therefore

$$\begin{aligned} (\hat{Y}^p f)(\mathbf{I}) &= \left. \frac{\partial^p}{\partial t_1 \partial t_2 \cdots \partial t_p} (df)_{\mathbf{I}}(\mathbf{I}(\mathbf{I} + t_1 Y)(\mathbf{I} + t_2 Y) \cdots (\mathbf{I} + t_p Y)) \right|_{t_1, t_2, \dots, t_p=0} \\ &= \text{coefficient of } t_1 t_2 \cdots t_p \text{ in } (df)_{\mathbf{I}}((\mathbf{I} + t_1 Y)(\mathbf{I} + t_2 Y) \cdots (\mathbf{I} + t_p Y)) \\ &= df_{\mathbf{I}}(Y^p) \\ &= (\widehat{Y^p} f)(\mathbf{I}). \end{aligned} \quad \square$$

So we have a concrete understanding of what it means to say that $\mathfrak{h} \bmod \mathfrak{p}$ is closed under p th powers. We would also like a better understanding of the condition that \mathfrak{h} is the Lie algebra of a Zariski-closed group (that is defined over K).

First, let us note that there is no issue about H being defined over K ; the only question is whether H is Zariski closed:

Proposition. *Let \mathfrak{h} be the Lie algebra of a connected, Zariski-closed subgroup H of $\mathrm{GL}_n(\mathbb{C})$. The following are equivalent:*

- (1) H is defined over K .
- (2) \mathfrak{h} is defined over K .

Remark. Let V be a vector subspace V of \mathbb{C}^n . The following are equivalent:

- (1) V is defined over K .
- (2) V is defined by polynomial equations with coefficients in K .
- (3) V is defined by linear equations with coefficients in K .
- (4) V is spanned by vectors in K^n .
- (5) $V \cap K^n$ is dense in V .
- (6) V is stable under $\mathrm{Gal}(\mathbb{C}/K)$.

Furthermore, a connected, Zariski-closed subgroup H of $\mathrm{GL}_n(\mathbb{C})$ is defined over K iff H_K is Zariski dense in H .

Given a Lie subalgebra \mathfrak{h} of $\mathfrak{gl}_n(\mathbb{C})$, Lie theory provides us with a corresponding closed, connected subgroup H of $\mathrm{GL}_n(\mathbb{C})$. In general, H may not be Zariski closed, but there are only two obstructions to this.

Recall (Levi decomposition). From the theory of Lie groups, $H = L \dot{\times} R$, where

- L is semisimple (= almost-direct product of simple groups) (a *Levi subgroup*), and

- R is a solvable, normal subgroup (the *radical*).

Equivalently, $\mathfrak{h} = \mathfrak{l} \ltimes \mathfrak{r}$, with \mathfrak{l} semisimple and \mathfrak{r} solvable.

Example. Parabolic =
$$\begin{bmatrix} \mathrm{GL}_{n_1} & * & * \\ & \mathrm{GL}_{n_2} & * \\ & & \mathrm{GL}_{n_3} \end{bmatrix} = \begin{bmatrix} \mathrm{SL}_{n_1} & & \\ & \mathrm{SL}_{n_2} & \\ & & \mathrm{SL}_{n_3} \end{bmatrix} \dot{\times} \begin{bmatrix} \lambda_1 \mathbf{I}_{n_1 \times n_1} & * & * \\ & \lambda_2 \mathbf{I}_{n_2 \times n_2} & * \\ & & \lambda_3 \mathbf{I}_{n_3 \times n_3} \end{bmatrix}.$$

Remark. If H is Zariski closed, then L and R are Zariski closed.

Recall (Lie-Kolchin Theorem). R is conjugate to a group of upper-triangular matrices.

That is, we may assume

$$R \subset \begin{bmatrix} * & * & * & * \\ & * & * & * \\ & & * & * \\ & & & * \end{bmatrix} = \mathrm{Diag} \times \mathrm{Unip}.$$

Thus, $\mathfrak{r} \subset \delta\mathrm{diag} \times \mathrm{unip}$.

For algebraic groups, the Levi decomposition can be refined, by decomposing R :

Theorem. Suppose R is a connected, Zariski-closed subgroup of $\mathrm{Diag} \times \mathrm{Unip}$.

Then $R = T \times (R \cap \mathrm{Unip})$, where T is conjugate to a subgroup of Diag (i.e., T is a torus).

Example. In the above parabolic, $R = \begin{bmatrix} \lambda_1 \mathbf{I}_{n_1 \times n_1} & & \\ & \lambda_2 \mathbf{I}_{n_2 \times n_2} & \\ & & \lambda_3 \mathbf{I}_{n_3 \times n_3} \end{bmatrix} \times \begin{bmatrix} \mathbf{I}_{n_1 \times n_1} & * & * \\ & \mathbf{I}_{n_2 \times n_2} & * \\ & & \mathbf{I}_{n_3 \times n_3} \end{bmatrix}.$

Now, here are the two obstructions:

Corollary. \mathfrak{h} is algebraic iff, after replacing it by an appropriate conjugate, we have

- (1) $\mathfrak{r} = (\mathfrak{r} \cap \delta\mathrm{diag}) \times (\mathfrak{r} \cap \mathrm{unip})$, and
- (2) $\mathfrak{r} \cap \delta\mathrm{diag}$ is a \mathbb{Q} -subspace of $\delta\mathrm{diag}$.

Remark. The second obstruction amounts to the well-known fact that any connected, Zariski-closed subgroup of Diag can be defined by a system of equations of the form

$$x_{1,1}^{\ell_1} x_{2,2}^{\ell_2} \cdots x_{n,n}^{\ell_n} = 1,$$

where $\ell_1, \ell_2, \dots, \ell_n \in \mathbb{Z}$. (The case $n = 2$ was proved in an example above.)

The first obstruction can be restated as the fact that Zariski-closed subgroups contain the Jordan components of their elements.

Lemma (Jordan decomposition).

- (1) Any $x \in \mathrm{Mat}_{n \times n}(\mathbb{C})$ can be written uniquely in the form $x = x_s + x_n$, where x_s is semisimple (i.e., diagonalizable), x_n is nilpotent (i.e., $(x_n)^k = 0$ for some $k \in \mathbb{N}$), and $x_s x_n = x_n x_s$.
- (2) Any $x \in \mathrm{GL}_n(\mathbb{C})$ can be written uniquely in the form $x = x_s x_u$, where x_s is semisimple (i.e., diagonalizable), x_u is unipotent (i.e., $(x_u - \mathbf{I})^k = 0$ for some $k \in \mathbb{N}$; i.e., the only eigenvalue of x_u is 1), and $x_s x_u = x_u x_s$. (Namely, let $x_u = \mathbf{I} + (x_s)^{-1} x_n$.)

Theorem. Assume H is Zariski closed.

- (1) For all $h \in H$, we have $h_s, h_u \in H$.
- (2) For all $x \in \mathfrak{h}$, we have $x_s, x_n \in \mathfrak{h}$.

So Bost's Theorem in the case of linear algebraic groups can be stated as:

Proposition. Let \mathfrak{h}_K be a Lie subalgebra of $\mathfrak{gl}_n(K)$.

If $\mathfrak{h}_{\mathcal{O}_K} \bmod \mathfrak{p}$ is closed under p th powers, for a.e. prime \mathfrak{p} of \mathcal{O}_K , then

- (1) \mathfrak{h}_K contains the Jordan components of each of its elements, and
- (2) if, in addition, $\mathfrak{h}_K \subset \delta\mathrm{diag}$, then \mathfrak{h}_K is a \mathbb{Q} -subspace of $\delta\mathrm{diag}$.

Remark. The second part is a generalization of Kronecker's Theorem discussed above.

Exercise. Prove this proposition from scratch, without using Bost's Theorem.

AN APPLICATION OF BOST'S THEOREM TO ELLIPTIC CURVES

Bost's theorem has a nice application to elliptic curves that are defined over \mathbb{Q} . (An abelian variety that is one-dimensional is called an *elliptic curve*.) It is a special case of the Faltings Isogeny Theorem, which is a general result for all abelian varieties over number fields.

Throughout this section, E_1 and E_2 are elliptic curves over \mathbb{Q} ; E_1 and E_2 are elliptic curves over \mathbb{F}_p .

Definition. E_1 is isogenous to E_2 if there is a finite homomorphism from E_1 to E_2 .

Corollary. E_1 is isogenous to $E_2 \iff \#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$ for a.e. p .

Idea of proof. (\Rightarrow) Well known (and can be obtained from our proof of the other direction).

(\Leftarrow) Let \mathfrak{h} be a one-dimensional subspace of $\mathfrak{e}_1 \oplus \mathfrak{e}_2$ (not $\mathfrak{e}_1 \oplus \{0\}$ or $\{0\} \oplus \mathfrak{e}_2$).

It suffices to show that \mathfrak{h} is algebraic, for then $H \subset E_1 \times E_2$ is isogenous to both E_1 and E_2 , via the projection maps (and isogeny is an equivalence relation for curves).

Thus, we wish to show $\mathfrak{h} \bmod p$ is closed under p th powers, for a.e. p .

Since E_i is one-dimensional, $\exists \lambda_i \in \mathbb{F}_p$, $D^p = \lambda_i D$ for all $D \in \mathfrak{e}_i \bmod p$.

We wish to show $\lambda_1 = \lambda_2$, for then the p th power map is a scalar on $(\mathfrak{e}_1 \oplus \mathfrak{e}_2) \bmod p$, so every subspace is invariant.

Because $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$, this is immediate from the following proposition. \square

Proposition. $\lambda_i \equiv 1 - \#E_i(\mathbb{F}_p) \pmod{p}$.

Proof. Let $E^* = \text{Jac}(E)$ be the dual of E .

Now the tangent space of E^* (infinitesimal deformations of the trivial line bundle) can be identified with $H^1(E, \mathcal{O}_E)$.

Thus, the Lie algebra of E can be identified with $H^1(E, \mathcal{O}_E)$ (since E is isomorphic to E^* , via $x \mapsto \mathcal{L}([x] - [0])$).

The Frobenius acts on E , so it induces an action on $H^1(E, \mathcal{O}_E) \cong \mathfrak{e}$.

Let us assume this can be identified with the p th power map on \mathfrak{e} .

The eigenvalue λ of Frobenius on $H^1(E, \mathcal{O}_E)$ is called the *Hasse invariant* of E .

It enters into a Lefschetz Trace Formula for the number of fixed points of F :

$$\#E(\mathbb{F}_p) = \# \text{ fixed points of } F \text{ on } E = \sum_{k=0}^2 (-1)^k (\text{trace on } H_{\text{dR}}^k(E)) \equiv 1 - \lambda + p.$$

So $\lambda \equiv 1 - \#E(\mathbb{F}_p) \pmod{p}$, as desired. \square

APPENDIX A. BASIC FACTS ON ALGEBRAIC LIE SUBALGEBRAS OF LINEAR GROUPS

Proposition. Every Lie subalgebra of \mathfrak{unip} is algebraic.

Proposition. Every semisimple Lie subalgebra of $\mathfrak{gl}_n(\mathbb{C})$ is algebraic.

Proposition. If H is a Zariski-closed, and $\varphi: H \rightarrow \text{GL}(V)$ is a regular homomorphism, then $\varphi(H)$ is Zariski closed.

Proposition. If A and B are Zariski-closed subgroups of $\text{GL}_n(\mathbb{C})$, and AB is a subgroup, then AB is Zariski closed.

Corollary. \mathfrak{h} is algebraic iff $\text{rad } \mathfrak{h}$ is algebraic.

Corollary. If \mathfrak{h} is any Lie subalgebra of $\mathfrak{gl}_n(\mathbb{C})$, then $[\mathfrak{h}, \mathfrak{h}]$ is algebraic.

REFERENCES

J.-B. Bost: Algebraic leaves of algebraic foliations over number fields. Publ. Math. Inst. Hautes Études Sci. No. 93 (2001), 161–221. (Section 2.3)

G. P. Hochschild: Basic theory of algebraic groups and Lie algebras. Graduate Texts in Mathematics, 75. Springer-Verlag, New York-Berlin, 1981. ISBN: 0-387-90541-3