GROWTH IN GROUPS III: ESCAPE

NICK GILL

The main result of this series of lectures is that *generating sets in simple groups of Lie type grow*; this was Thm. 1 of the previous lecture (we shall call it *the Main Theorem* in this lecture).

The main goal of the current lecture is to complete the first step towards proving the Main Theorem. In the notation of the previous lecture our aim is to prove (P1):

Proposition 0.1 (P1)**.** *Let G be a finite group of Lie type of rank r; let K be a finite field. Let $A \subset G(K)$ be a set such that $\langle A \rangle = G(K)$. Then there exists $k \ll_r 1$ such that A_k contains a regular element.*

In fact we shall prove some much stronger results than this. The methods that we develop will underpin the proofs of (P2) and (P3). Material for this lecture is based heavily on [Hel].

1. Background on Varieties

The proof of the Main Theorem uses the crucial fact that a finite group of Lie type is the set of points of an algebraic group. To understand how this works we need to establish some notation from algebraic geometry.

We work inside affine space $\mathbb{A}^n$. An (affine) *variety* V is given by a finite set of polynomial equations $F(x_1, x_2, \dots, x_n) = 0$ in n variables with coefficients in a field. If the coefficients all lie in a field K, we say that V is *defined over* K, or simply write V/K. If L is another field – containing, contained in, or equal to K – then we write $V(L)$ for the set of *L-valued points of* V, i.e., the set of solutions in L^n to our set of equations. (The notation that we describe cropped already in the previous lecture.)

A *subvariety* $W \subset V$ is a variety that can be defined by a set of equations that contains a set of equations defining V. By a *proper subvariety* $W \subsetneq V$ we mean simply a subvariety with $W \neq V$. Clearly, if two varieties V, W defined over K satisfy $W \subset V$, then $W(L) \subset V(L)$ for every extension L of K.

We can define maps between affine varieties; such a map is called *regular* if it is given by polynomials.

1.1. Degree and dimension.

The *dimension* $\dim(X)$ of an irreducible variety X is the length k of the longest chain $\{x\} = X_0 \subset X_1 \subset \cdots \subset X_k = X$ of irreducible subvarieties of X; this corresponds to the intuitive notion of dimension. If the irreducible components of a variety V all have the same dimension, we say V is *pure dimensional*, and define the dimension $\dim(V)$ of V to be that of any of its irreducible components. (An *irreducible component* of a variety V is an irreducible subvariety of V not contained in any other irreducible subvariety of V.)

The *degree* $\deg(V)$ of a pure-dimensional variety V of dimension r in n-dimensional affine or projective space is its number of intersection points with a generic linear variety of dimension $n-r$. (Here *generic* means *outside a variety of positive codimention.*)

It remains to see how to define the dimension and the degree of a variety V when V is not irreducible. We simply define $\dim V$ to be the dimension of the irreducible subvariety of V of largest dimension. As for the degree, it will be best to see it as a vector: we define the *degree* $\overrightarrow{\deg}(V)$ of an arbitrary variety V to be

$$(d_0, d_1, \dots, d_k, 0, 0, 0, \dots),$$

where $k = \dim(V)$ and d_j is the degree of the union of the irreducible components of V of dimension j.

We will need the following important fact: if a variety V is defined by equations

$$\begin{aligned} F_1(x_1, x_2, \dots, x_n) &= 0 \\ F_2(x_1, x_2, \dots, x_n) &= 0 \\ &\dots\dots \\ F_k(x_1, x_2, \dots, x_n) &= 0, \end{aligned}$$

then $\overrightarrow{\deg}(V) \ll_{n,\deg(F_1),\deg(F_2),\dots,\deg(F_n)} 1$ [Hel, p. 12].

If a regular map $\phi : V \mapsto W$ between two varieties $V \subset \mathbb{A}^m$, $W \subset \mathbb{A}^n$ is defined by polynomials $\phi_1, \phi_2, \dots, \phi_n$ on the variables $x_1, x_2, \dots, x_m$, we define $\deg_{\text{pol}}(\phi)$ to be $\max_j \deg(\phi_j)$. (If several representations of ϕ by polynomials $\phi_1, \phi_2, \dots, \phi_n$ are possible, we choose – for the purposes of defining $\deg_{\text{pol}}$ – the one that gives us the least value of $\deg_{\text{pol}}$.) What we have just seen amounts to stating that, if a subvariety V' of V is given by $\phi(x) = y$ for some $y \in W(\overline{K})$, then $\overrightarrow{\deg}(V')$ can be bounded in terms of $\deg_{\text{pol}}(\phi)$ and n (where $W \subset \mathbb{A}^n$).

1.1.1. *Abuse of language.* Given a variety V defined over a field K, and a subvariety $W/\overline{K}$ defined over the algebraic completion $\overline{K}$ of K, we will write $W(K)$ for $W(\overline{K}) \cap V(K)$. (We will even speak of the points of W over K, meaning $W(K) := W(\overline{K}) \cap V(K)$.)

1.1.2. *Independence.* Let $V_1, V_2, \dots, V_k$ be linear subspaces of an affine space $\mathbb{A}^n$; let them be defined over a field K. We say that $V_1, V_2, \dots, V_k$ are *linearly independent* if there is no choice of points $v_1 \in V_1(\overline{K})$, $v_2 \in V_2(\overline{K})$, $\dots$, $v_k \in V_k(\overline{K})$, not all of them 0, such that $v_1 + v_2 + \dots + v_k = 0$.

1.2. **Algebraic groups.** An (affine) *algebraic group* defined over a field K is an affine variety G/K with a group law such that the multiplication map $\mu : G \times G \mapsto G$ and the inverse map $\iota : G \to G$ are regular and defined over K. Thus, strictly speaking, an algebraic group G is not a group; rather, its set of points $G(L)$ will be a group for every field L containing K. The set of points $G(L)$ for L contained in K may also be a group, if it is closed under the group operation.

I will assume a basic knowledge of semisimple linear algebraic groups, especially facts about Jordan decomposition and tori. See, for instance, [Bor91, Hum97, Spr09]. For now we recall some definitions.

Let V be a vector space over K. An element $g \in GL(V)$ is *semi-simple* if there exists a basis for V consisting of eigenvectors for g. An element g in $GL(V)$ is *unipotent* if $(g-I)^n = 0$ for some integer $n \geq 1$. Relevant facts:

- Take $g \in GL(V)$. There exist unique elements $g_s, g_u \in GL(V)$ such that $g = g_s g_u = g_u g s$ and g_s is semi-simple, g_u is unipotent. This is the *Jordan decomposition* in GL
- A linear algebraic group G defined over $\overline{K}$ is a subgroup of GL_n for some n. Then for every $g \in G(K)$, the elements g_s and g_u are also in $G(K)$.

Now suppose that G is a *simple* linear algebraic group; in other words all normal subgroups of G lie in $Z(G)$. A *torus* of G is a subgroup T of G that is isomorphic to $\underbrace{GL_1 \times \cdot \times GL_1}_{n}$ for some n. We can think of G as a subgroup of GL_n; then for an appropriate choice of basis, the elements of T are all diagonal matrices.

A *maximal torus* in G is a torus that is not properly contained in any other torus. All maximal tori of G have the same dimension, r, which number defines the *rank* of the group G. Relevant facts:

- Any element of T is semi-simple; conversely, any semi-simple element lies in (at least one) maximal torus.
- The centralizer of a semi-simple element always contains a maximal torus. (This follows from the previous fact, and the fact that tori are abelian.)

A *regular* semi-simple element is an element g for which $C_G(g) = T$ for some maximal torus T. In SL_n (or GL_n), the regular elements are precisely those with distinct eigenvalues.

Finally, note that if T_1 and T_2 are distinct maximal tori in G, then $T_1(\overline{K})$ and $T_2(\overline{K})$ are conjugate in $G(\overline{K})$. What is more the $N_{G(\overline{K})}(T_1(\overline{K}))/T_1(\overline{K}) \cong W$, where W is the *Weyl group* of G. The group W is a finite group; i.e. $|W| \ll_r 1$. When $G = SL_n$, we have $W \cong S_n$.

2. Escape from subvarieties

We start by giving a background result; this is Bezout's result which describes how degree is affected when we consider the intersection of varieties.

Lemma 2.1 (Bezout's theorem, generalised)**.** [Dan94, p. 251] *Let $X_1, X_2, \ldots, X_k$ be pure-dimensional varieties in $\mathbb{P}^n$, and let $Z_1, Z_2, \ldots, Z_l$ be the irreducible components of the intersection $X_1 \cap X_2 \cap \cdots \cap X_k$. Then*

$$\sum_{j=1}^{l} \deg(Z_j) \leq \prod_{i=1}^{k} \deg(X_i),$$

where $X_1, X_2, \ldots, X_k$ are the irreducible components of X_j.

The next result first appeared in [Hel]; it was based on work in [EMO05].

Proposition 2.2. *Let G be a group. Consider a linear representation of G on a vector space $\mathbb{A}^n(K)$ over a field K. Let V be an affine subvariety of $\mathbb{A}^n$.*

Let A be a subset of G; let $\mathscr{O}$ be an $\langle A\rangle$-orbit in $\mathbb{A}^n(K)$ not contained in V. Then there are constants $\eta > 0$ and m depending only on $\overrightarrow{deg}(V)$ such that, for every $x \in \mathscr{O}$, there are at least $\max(1, \eta|A|)$ elements $g \in A_m$ such that $gx \notin V$.

This may be phrased as follows: one can escape from V by the action of the elements of A.

Proof. Let us begin by showing that there are elements $g_1, \dots, g_l \in A_r$ such that, for every $x \in \mathscr{O}$, at least one of the $g_i \cdot x$'s is not in V. (Here l and r are bounded in terms of $\overrightarrow{\deg} V$ alone.) We will proceed by descent (that is, induction) on $\overrightarrow{\deg} V$, paying special attention to the number s_V of irreducible components of V of maximal dimension $\dim V$. (Notice that s_V is bounded in terms of $\overrightarrow{\deg} V$: in fact, $s_V \leq (\overrightarrow{\deg} V)_{\dim V}$.)

We shall always pass from V to a variety V' with either (a) $\dim V' < \dim V$ or (b) $\dim V' = \dim V$ and $s_{V'} < s_V$. Moreover, $\overrightarrow{\deg} V'$ will be bounded in terms of $\overrightarrow{\deg} V$ alone. We will iterate until we arrive at a variety V' of dimension 0 with $s_{V'} = 0$, i.e., an empty variety. It is clear that this process terminates in a number of steps bounded in terms of $\overrightarrow{\deg} V$ alone.

Let V_+ be the union of all irreducible components of V of maximal dimension (i.e., dimension $\dim V$). If V_+ and $\mathscr{O}$ are disjoint, we set $V' = V \setminus V_+$ and are done. Suppose otherwise. Since $\mathscr{O}$ is not contained in V_+, we can find $x_0 \in V_+ \cap \mathscr{O}$, $g \in A \cup A^{-1}$ such that $gx_0 \notin V_+$, i.e., $x_0 \notin g^{-1}V_+$. Hence the set of components of maximal dimension $\dim V$ in V is not the same as the set of components of maximal dimension $\dim g^{-1}V = \dim V$ in $g^{-1}V$. It follows that $V' = g^{-1}V \cap V$ does not contain V_+, and thus has fewer components of dimension $\dim V$ than V has.

We have thus passed from V to V', where either (a) $\dim V' < \dim V$ or (b) $\dim V' = \dim V$ and $s'_V < s_V$. Bezout's theorem assures us that $\overrightarrow{\deg} V'$ is bounded in terms of $\overrightarrow{\deg} V$ alone. By the inductive hypothesis, we already know that there are $g'_1, \dots, g'_{l'} \in A_{r'}$ such that, for every $x \in \mathscr{O}$, at least one of the $g'_i \cdot x$'s is not in V'. (Here l' and r' are bounded in terms of $\overrightarrow{\deg} V'$ alone.) Since at least one of the $g'_i \cdot x$'s is not in $V' = g^{-1}V \cap V$, either one of the $g'_i \cdot x$'s is not in V or one of the $g'_i \cdot x$'s is not in $g^{-1}V$, i.e., one of the $gg'_i \cdot x$'s is not in V. Set

$$g_1 = g'_1,\ g_2 = g'_2,\ \dots,\ g_{l'} = g'_{l'}$$
$$g_{l'+1} = gg'_1,\ g_{l'+2} = gg'_2,\ \dots,\ g_{2l'} = gg'_{l'}, \qquad l = 2l'.$$

(As can be seen, $g_i \in A_r$, where $r = r' + 1$.) We conclude that, for every $x \in \mathscr{O}$, at least one of the $g_i \cdot x$'s is not in V.

The rest is easy: for each $x \in \mathscr{O}$ and each $g \in A$, at least one of the elements $g_i g \cdot x$, $1 \leq i \leq l$ ($g_i \in A_r$) will not be in V. Each possible $g_i g$ can occur for at most l different elements $g \in A$; thus, there are at least $\min(1, |A|/l)$ elements $h = g_i g$ of A_{r+1} such that $hx \notin V$. □

2.1. **A proof of (P1).** First observe that, given a set of generators, we can avoid a subvariety in an algebraic group by escape from subvarieties.

Lemma 2.3. *Let $G \subset \mathrm{GL}_n$ be an algebraic group defined over a field K. Let V be a subvariety of G such that $V(K)$ is a proper subset of $G(K)$. Let $A \subset G(K)$ be a set of generators of $G(K)$.*

Then

$$|A_k \cap (G(K) \setminus V(K))| \gg_{\overrightarrow{deg}(V)} |A|,$$

where $k \ll_{\overrightarrow{deg}(V)} 1$.

Proof. By escape from subvarieties (Prop. 2.2) with A and V as given, $x = 1$, and G and $\mathscr{O}$ both equal to $G(K)$. (We are implicitly using the fact that G is contained in an affine space, viz., $\mathbb{A}^{n^2}$.) □

Let W be the set of elements in G that are not regular semi-simple. Prop. 0.1 follows immediately from Lem. 2.3 and the following easy lemma.

Lemma 2.4. *The set W is an affine algebraic variety of positive codimension in G and degree $\ll_r 1$.*

Proof. We prove this result only for $G = SL_n$; it is easy enough to prove the result in general. An element of SL_n is regular semisimple if and only if its eigenvalues are distinct. Let W be the variety of all $g \in G$ whose characteristic polynomials have multiple roots, i.e., define W by $\mathrm{Disc}(\det(\lambda I - g)) = 0$.

Clearly the defining polynomial of W has degree $\ll_r 1$, and so the degree of W is $\ll_r 1$. Next observe that $G = SL_n$ is an irreducible affine variety (it is defined by a single polynomial); since we can easily find points in $G(\overline{K}) \setminus W(\overline{K})$ we conclude that W has positive codimension in G. □

2.2. **Non-singularity and almost-injectivity.** If a map f is injective, then, for every finite subset E of the domain, $|f(E)| = |E|$. If f is such that the preimage $f^{-1}(\{x\})$ of every point x consists of at most k points, then $|f(E)| \geq \frac{1}{k}|E|$. This simple fact lies at the root of several of our arguments.

First, let us see how non-singularity gives us "almost injectivity". (A regular map $f : X \mapsto Y$ is said to be *non-singular* at a point $x = x_0$ if its derivative $Df|_{x=x_0}$ at $x = x_0$ is a non-singular linear map from $(TX)_{x=x_0}$ to $(TY)_{y=f(x_0)}$.)

Lemma 2.5. *Let $X \subset \mathbb{A}^{m_1}$ and $Y \subset \mathbb{A}^{m_2}$ be affine varieties defined over a field K. Let $f : X \to Y$ be a regular map. Let V be a subvariety of X such that the derivative $Df|_{x=x_0}$ of f at $x = x_0$ is a nonsingular linear map for all x_0 on X outside V.*

Let $S \subset X(\overline{K}) \setminus V(\overline{K})$. Then

$$|f(S)| \gg_{\overrightarrow{deg}(X), \deg_{\mathrm{pol}}(f)} |S|.$$

Proof. It will be enough to show that the intersection of $X(\overline{K}) \setminus V(\overline{K})$ with the preimage $Z = f^{-1}(y_0)$ of any point y_0 on Y consists of a number of irreducible zero-dimensional varieties (that is, points) bounded in terms of $\deg(V)$ and the degree of the polynomials defining f. Now Z is the intersection $X \cap \bigcap_j X_j$, where X_j, $1 \leq j \leq n$, is the variety in $\mathbb{A}^m$ defined by by $(f(x))_j = (y_0)_j$, where we denote by y_j the jth coordinate of an element y of $\mathbb{A}^n$. Thus, by Bezout's theorem (Lem. 2.1), the degree $\overrightarrow{\deg}(Z)$ of Z is

$\ll_{\overrightarrow{\deg}(X),\overrightarrow{\deg}(X_1),\dots,\overrightarrow{\deg}(X_n)} 1$. The degree $\overrightarrow{\deg}(X_j)$ of the hypersurface X_j is bounded in terms of the degree of the polynomial $(f(x))_j$, and so

$$\overrightarrow{\deg}(Z) \ll_{\overrightarrow{\deg}(X),\deg((f(x))_1),\dots,\deg((f(x))_n)} 1.$$

Thus, it remains only to show that any point x_0 on Z not lying on V lies on a component of Z of dimension 0.

Suppose it were not so. Then there would be a direction $\vec{v} \neq 0$ such that

$$Df|_{x=x_0}(\vec{v}) = 0;$$

any direction $\vec{v} \neq 0$ on the tangent space to Z at $x = x_0$ would do. Then $Df_{x=x_0}$ would have to be singular. However, this would mean that x_0 would have to lie on V. Contradiction. □

Corollary 2.6. *Let $G \subset \mathrm{GL}_n$ be an algebraic group and $Y \subset \mathbb{A}^m$ an affine variety, both defined over a field K. Let $f : G \to Y$ be a regular map. Let V be a subvariety of G such that $V(K)$ is a proper subset of $G(K)$. Assume that the derivative $Df|_x$ of f at x is a nonsingular linear map for all x on G outside V.*

Let $E \subset G(K)$ be a set of generators of $G(K)$. Then

$$|f(E_k \cap (G(K) \setminus V(K)))| \gg_{\overrightarrow{deg}(G),\overrightarrow{deg}(V),\deg_{\mathrm{pol}}(f)} |E|,$$

where $k \ll_{\overrightarrow{deg}(V)} 1$.

Proof. Immediate from Lemma 2.3 and Lemma 2.5 – the latter with $m_1 = n^2$, $m_2 = m$ and $S = E_k \cap (G(K) \setminus V(K))$. □

Next we show how to weaken one of the assumptions of Lemma 2.3.

Lemma 2.7. [Hel, Lem. 4.6] *Let $G \subset \mathrm{GL}_n$ be a simple irreducible simple algebraic group defined over a field K. Let $V/\overline{K}$ be a proper subvariety of G. Then*

$$V(K) \subsetneq G(K)$$

provided that $|K|$ is larger than a constant depending only on n, $\overrightarrow{deg}(V)$ and $\overrightarrow{deg}(G).s$

2.3. **Sticking subgroups in generic directions.** We finish with with two beautiful results that can be proved with the use of a whole load of algebraic geometry (for which we do not have time). These results will be central to our proofs of (P3) and (P4).

Recall that every algebraic group G/K acts on its Lie algebra (i.e., its tangent space $\mathfrak{g}$ at the origin) by conjugation; the *adjoint map* $\mathrm{Ad}_g : \mathfrak{g} \to \mathfrak{g}$ is the action of an element $g \in G(\overline{K})$. Recall as well the definition of *linear independence* of subspaces given in §1.1.2.

Proposition 2.8. [Hel, Prop. 4.12] *Let $G \subset \mathrm{GL}_n$ be an irreducible algebraic group defined over a field K; let $H_0/\overline{K}$, $H_1/\overline{K}$,..., $H_\ell/\overline{K}$ be algebraic subgroups thereof. Assume either that K is perfect or that G is reductive. Write $\mathfrak{g}$ for the Lie algebra of G, and $\mathfrak{h}_\mathrm{j}$ for the Lie algebra of H_j, $0 \leq j \leq \ell$. Assume there are $g_0, g_1, \dots, g_\ell \in G(\overline{K})$ such that*

$$\mathrm{Ad}_{g_0}(\mathfrak{h}_0), \mathrm{Ad}_{g_1}(\mathfrak{h}_1), \dots, \mathrm{Ad}_{g_\ell}(\mathfrak{h}_\ell) \tag{2.1}$$

are linearly independent.

Let $A \subset G(K)$ be a set of generators of $G(K)$. Then there are $g_0, g_1, \dots, g_\ell \in A_k$, $k \ll_n 1$, such that

$$|g_0 E_0 g_0^{-1} \cdot g_1 E_1 g_1^{-1} \cdot \dots \cdot g_\ell E_\ell g_\ell^{-1}| \gg_{n,\deg(H_0),\deg(H_1),\dots,\deg(H_\ell)} |E_0||E_1| \cdots |E_\ell|$$

for any non-empty subsets $E_j \subset H_j(K)$, $0 \le j \le \ell$.

Proposition 2.9. [Hel, Prop. 4.13] *Let $G \subset \mathrm{GL}_n$ be an algebraic group defined over a field K; write $\mathfrak{g}$ for its Lie algebra. Let $\mathfrak{h}$ be a subspace of $\mathfrak{g}$. Suppose that there are elements $\vec{g}_1, \vec{g}_2, \dots, \vec{g}_\ell$ of $\mathfrak{g}(\overline{K})$ such that the spaces*

$$\mathfrak{h}, [\vec{g}_1, \mathfrak{h}], [\vec{g}_2, \mathfrak{h}], \dots, [\vec{g}_\ell, \mathfrak{h}] \tag{2.2}$$

are linearly independent and of dimension $\dim(\mathfrak{h})$. Suppose that the characteristic $\mathrm{char}(K)$ of K is either 0 or greater than k, where $k = \dim(\mathfrak{h})$.

Then there is a proper subvariety X of G^ℓ such that, for all $(g_1, g_2, \dots, g_\ell) \in G^\ell(\overline{K})$ not on X, the spaces

$$\mathfrak{h}, \mathrm{Ad}_{g_1}(\mathfrak{h}), \mathrm{Ad}_{g_2}(\mathfrak{h}), \dots, \mathrm{Ad}_{g_\ell}(\mathfrak{h})$$

are linearly independent and of dimension $\dim(\mathfrak{h})$. Moreover, $\overrightarrow{deg}(X) \ll_n 1$.

References

[Bor91] Armand Borel, *Linear algebraic groups*, second ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991.

[Dan94] V. I. Danilov, *Algebraic varieties and schemes*, Algebraic geometry, I, Encyclopaedia Math. Sci., vol. 23, Springer, Berlin, 1994, pp. 167–297.

[EMO05] Alex Eskin, Shahar Mozes, and Hee Oh, *On uniform exponential growth for linear groups*, Invent. Math. **160** (2005), no. 1, 1–30.

[Hel] H.A. Helfgott, *Growth and generation in $SL_3(\mathbb{Z}/p\mathbb{Z})$*, J. Eur. Math. Soc. (JEMS), To appear.

[Hel08] H. A. Helfgott, *Growth and generation in* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, Ann. of Math. (2) **167** (2008), no. 2, 601–623.

[Hum97] John F. Humphreys, *A course in group theory*, Oxford Science Publications, Oxford University Press, 1997.

[Spr09] T. A. Springer, *Linear algebraic groups*, second ed., Modern Birkhäuser Classics, Birkhäuser Boston Inc., Boston, MA, 2009.