Exponential generation and largeness for compact
p-adic Lie groups

Michael Larsen

msp

Exponential generation and largeness for compact p-adic Lie groups

Michael Larsen

Given a fixed integer n, we consider closed subgroups $\mathcal{G}$ of $\mathrm{GL}_n(\mathbb{Z}_p)$, where p is sufficiently large in terms of n. Assuming that the identity component of the Zariski closure G of $\mathcal{G}$ in $\mathrm{GL}_{n,\mathbb{Q}_p}$ does not admit any nontrivial torus as quotient group, we give a condition on the (mod p) reduction of $\mathcal{G}$ which guarantees that $\mathcal{G}$ is of bounded index in $\mathrm{GL}_n(\mathbb{Z}_p) \cap G(\mathbb{Q}_p)$.

Nori [1987] considered a special class of subgroups of $\mathrm{GL}_n(\mathbb{F}_p)$, namely groups which are generated by elements of order p or, as we shall say, *p-generated groups*. He showed that if p is sufficiently large in terms of n, there is a correspondence between p-generated groups and a certain class of connected algebraic groups which he called *exponentially generated*. In particular, every p-generated group Γ is a subgroup of $G(\mathbb{F}_p)$ for the corresponding algebraic group G, and $[G(\mathbb{F}_p) : \Gamma]$ is bounded by a constant depending only on n. The p-generated groups are admittedly rather special, but on the other hand, every finite subgroup $\Gamma \subset \mathrm{GL}_n(\mathbb{F}_p)$ contains a p-generated normal subgroup, Γ^+, of prime-to-p index, which shows that every Γ can be related to a connected algebraic group in a weak sense. This construction can serve in some measure as a substitute for the (identity component of the) Zariski closure in the setting of finite linear groups, where the actual identity component of the Zariski closure of Γ is always trivial.

In this paper we consider closed subgroups $\mathcal{G}$ of the compact p-adic Lie group $\mathrm{GL}_n(\mathbb{Z}_p)$. In this setting, of course, Zariski closure behaves well, so we do not need a substitute. Nevertheless, it turns out that there is an interesting class of groups $\mathcal{G}$ for which we can prove a bounded index result analogous to that of Nori: see Theorem 7. We intend to give an application of this result to geometric monodromy of nonsingular projective varieties over function fields in finite characteristic.

Throughout the paper, n will denote a positive integer and F a field. If F is of characteristic $p > 0$, we assume $p \geq n$, so $i!$ is nonzero for $i < n$. As every

nilpotent element $x \in M_n(F)$ satisfies $x^n = 0$, the truncated exponential function

$$\exp(x) := \sum_{i=0}^{n-1} \frac{x^i}{i!}$$

satisfies $\exp(x + y) = \exp(x)\exp(y)$ for every pair x, y of commuting nilpotent matrices. Moreover $\exp(x) - 1$ is nilpotent, so $\exp(x)$ is unipotent. Conversely, if u is unipotent, $1 - u$ is nilpotent, so

$$\log(u) := -\sum_{i=1}^{n-1} \frac{(1-u)^i}{i}$$

is nilpotent, and log and exp set up mutually inverse bijections between the unipotent and nilpotent $n \times n$ matrices over F. In the positive characteristic case, every unipotent element $u \neq 1$ is of order p, and conversely, every element of order p is unipotent (because this is true for every Jordan block of order $\leq p$).

For every nilpotent element $x \in M_n(F)$, there exists a morphism of algebraic groups $\phi_x \colon \mathbb{A}^1 \to \mathrm{GL}_n$ defined by

$$\phi_x(t) := \exp(tx).$$

If $x \neq 0$, this morphism is injective, and its image is isomorphic to $\mathbb{A}^1$. If N is a set of nilpotent elements of $M_n(F)$, let G_N denote the subgroup of GL_n generated by $\phi_x(\mathbb{A}^1)$ for all $x \in N$, i.e., the intersection of all algebraic subgroups of GL_n which contain

$$\bigcup_{x \in N} \phi_x(\mathbb{A}^1).$$

Following Nori we say that an algebraic subgroup of GL_n over a field F is *exponentially generated* if it is of the form G_N for some $N \subset M_n(F)$.

Proposition 1. *Over a perfect field, every exponentially generated group is the extension of a semisimple group by a unipotent group.*

Proof. It is clear that every quotient group of an exponentially generated group G must be generated by subgroups isomorphic to the additive group. In particular exponentially generated groups must be connected, and every reductive exponentially generated group must be semisimple since no nontrivial torus is generated by additive groups. As long as F is perfect, the (geometric) unipotent radical N is actually defined over F, so G is an extension of the semisimple group G/N by the unipotent group N. $\square$

In general, the converse of Proposition 1 is not true. For example, if $F = \mathbb{R}$, GL_n contains F-anisotropic connected semisimple subgroups which have no nontrivial unipotent elements. If F is of positive characteristic, even if it is algebraically

closed, the image of SL_2 under the 4-dimensional representation which is the direct sum of the standard representation and its Frobenius twist fails to be exponentially generated. In characteristic zero, we have a precise criterion for exponential generation.

Proposition 2. *Let F be a field of characteristic zero. An algebraic subgroup G of GL_n defined over F is exponentially generated if and only if it has no nontrivial finite, toric, or anisotropic quotient group.*

Proof. As there is no nontrivial homomorphism from an additive group to a finite, toric, or anisotropic group, one direction is clear. For the other, let U denote a unipotent F-subgroup of G. Thus U has a composition series

$$U = U_0 \supset U_1 \supset \cdots \supset U_s = \{e\},$$

with each U_i/U_{i+1} isomorphic to the additive group. By Steinberg's theorem [1965], $H^1(F, U_i) = 0$ for all i, so for each $1 \le i \le s$ we have a short exact sequence

$$0 \to U_i(F) \to U_{i-1}(F) \to F \to 0,$$

and there exists $u_{i-1} \in U_{i-1}(F) \setminus U_i(F)$. As F is of characteristic zero,

$$\langle u_i \rangle \subset U_{i-1}(F) \cap \phi_{\log(u_i)}(F)$$

is isomorphic to $\mathbb{Z}$, so $\phi_{\log(u_i)}(\mathbb{A}^1) \cap U_{i-1}$ has dimension 1, which means $\phi_{\log(u_i)}(\mathbb{A}^1) \subset U_{i-1}$. It follows that

$$\phi_{\log(u_i)}(\mathbb{A}^1)U_i = U_{i-1}.$$

Thus, by descending induction,

$$U = \prod_{i=1}^{s} \phi_{\log(u_{i-1})}(\mathbb{A}^1).$$

Let H denote the quotient of $G = G^\circ$ by its unipotent radical N. As H is isotropic, the set $\mathcal{P}$ of its proper parabolic F-subgroups is nonempty. For each $P \in \mathcal{P}$, let U_P denote the inverse image in G of the unipotent radical of P. Thus each U_P is a unipotent F-subgroup of G containing N. Each is therefore exponentially generated. Let $K \subset G$ be the (exponentially generated group) generated by all U_P. Thus K is normalized by the inverse image of $H(F)$ in G. By a theorem of [Chevalley 1954], $H(F)$ is Zariski-dense in H, so K is normal in G. Thus G/K is isomorphic to a quotient $H/(K/N)$, which is isotropic. It follows that $\mathcal{P}$ contains a proper parabolic F-subgroup not contained in K/N, contrary to assumption. Thus $K = G$, and G is exponentially generated. $\qquad\square$

We say that a Lie algebra is *nilpotently generated* if it is spanned by its nilpotent elements. By [Nori 1987, Theorem A], if F is of characteristic zero or characteristic p sufficiently large in terms of n, the log and exp maps give mutually inverse bijections, described more explicitly below, between exponentially generated F-subgroups of GL_n and nilpotently generated F-subalgebras of the Lie algebra $M_n = \mathfrak{gl}_n$.

The following proposition allows us to put all exponentially generated subgroups (as well, possibly, as other subvarieties of GL_n) into a family over a base of finite type. It is convenient to work projectively, by embedding GL_n into $\mathbb{P}^{n^2}$. For any scheme Z and any closed subvariety K of $\mathrm{GL}_{n,Z}$, we denote by $\bar{K}$ the closed subset $Z \cup (\mathbb{P}_Z^{n^2} \setminus \mathrm{GL}_{n,Z})$ endowed with its reduced induced scheme structure.

Proposition 3. *For every positive integer n there exists an integer N and a finite set S of polynomials such that for every field F over $\mathbb{Z}[1/N]$ and every exponentially generated subgroup $G_F \subset \mathrm{GL}_{n,F}$, the Hilbert polynomial of $\bar{G}_F$ belongs to S.*

Proof. We prove that there exists a positive integer N and a morphism $Y' \to X'$ of schemes of finite type over $\mathbb{Z}$ such that for all F whose characteristic does not divide N and all exponentially generated $G_F \subset \mathrm{GL}_{n,F}$, there exists $x' \in X'(F)$ with $Y'_{x'} = \bar{G}_F$. By [Grothendieck 1961, §2], the set of Hilbert polynomials for the $\bar{G}_F$ is therefore finite.

We begin by trying to parametrize nilpotently generated Lie algebras. The set of k-tuples of nilpotent $n \times n$ matrices which span a Lie subalgebra of $n \times n$ matrices is constructible because Lie algebra closure can be expressed as the existence of a set of k^3 structure constants for the Lie bracket. Let $N_n/\mathbb{Z}$ denote the scheme of nilpotent $n \times n$ matrices and $W \subset N_n^{n^2}$ the constructible set of ordered n^2-tuples of nilpotent matrices spanning a Lie algebra. Replacing W with the disjoint union X of the strata of a suitable stratification, we get a scheme indexing n^2-tuples of nilpotent matrices which span nilpotent Lie algebras. Thus, for every field F of characteristic zero or characteristic p sufficiently large and every nilpotently generated Lie algebra $L \subset \mathfrak{gl}_n$ over F, there exists $x \in X(F)$ which indexes a spanning set of L.

We choose N sufficiently divisible that outside of characteristics dividing N, there is a bijection between exponentially generated subgroups G of GL_n and nilpotently generated Lie subalgebras L of $\mathfrak{gl}_n$, given by the mutually inverse maps sending G to its Lie algebra and L to the group generated by $\phi_x(\mathbb{A}^1)$ for all nilpotent $x \in L$. In particular, $\phi_{x_i}(\mathbb{A}^1)$ generates G whenever $x_1, \ldots, x_{n^2}$ is a nilpotent spanning set of L. From the scheme X indexing all possible n^2-tuples, we would like to obtain a scheme of finite type over $\mathbb{Z}[1/N]$ indexing all $\bar{G}_F$, where G_F ranges over exponentially generated groups and F ranges over fields over $\mathbb{Z}[1/N]$.

Recall (from [Borel 1991, Proposition 2.2], for example) that if $V \subset G \subset \mathrm{GL}_n$ is any connected generating subvariety of an algebraic group G, the image of V^{n^2} under the multiplication map is dense in G, and the image of V^{2n^2} is exactly G. This implies

$$\left(\phi_{x_1}(\mathbb{A}^1) \ldots \phi_{x_{n^2}}(\mathbb{A}^1) \right)^{2n^2} \twoheadrightarrow G.$$

Let $Y := \mathbb{P}_X^{n^2}$ and

$$Z := (\mathbb{P}_X^{n^2} \setminus \mathrm{GL}_{n,X}) \coprod (X \times \mathbb{A}^{2n^4}).$$

We define $\xi \colon Z \to Y$ by extending the obvious inclusion map on the first component of Z by

$$\xi \left((x_1, \ldots, x_{n^2}), (t_{1,1}, \ldots, t_{n^2, 2n^2}) \right) := \left((x_1, \ldots, x_{n^2}), \prod_{j=1}^{2n^2} \prod_{i=1}^{n^2} \phi_{x_i}(t_{i,j}) \right).$$

For each F and each $x \in X(F)$, the image of the map of fibers $Z_x \to Y_x = \mathbb{P}_F^{n^2}$ is the union of $\mathbb{P}_F^{n^2} \setminus \mathrm{GL}_{n,F}$ and the exponential subgroup of $\mathrm{GL}_{n,F}$ in correspondence with the nilpotently generated Lie subalgebra of $\mathfrak{gl}_n(F)$ associated to x. The following lemma now implies the proposition. $\square$

Lemma 4. *Let m be a positive integer, X a scheme of finite type over $\mathbb{Z}$, Y a closed subscheme of $\mathbb{P}_X^m$, and $\xi \colon Z \to Y$ a morphism of finite type such that $\xi(Z_x)$ is a closed subset of Y_x for all $x \in X$. There exists $N \in \mathbb{N}$, a morphism $\psi \colon X' \to X$, and a closed subscheme $Y' \subset \mathbb{P}_{X'}^m$ such that for every field F over $\mathbb{Z}[1/N]$ and every $x \in X(F)$, there exists $x' \in X_x'(F)$ such that $Y_{x'}' = \xi(Z_x)^{\mathrm{red}}$.*

Proof. We use Noetherian induction on X. If the image of $Z \to X$ has Zariski closure $C \subsetneq X$, we can replace X and Y by C and Y_C respectively. We therefore assume without loss of generality that $Z \to X$ has dense image. Replacing Z by Z^{red}, without loss of generality we may assume Z is reduced. We choose N divisible by every prime which is the characteristic of a generic point of X.

Let η denote a generic point of X. As any localization of a reduced ring is reduced, Z_η is reduced. Either η lies over a prime p dividing N or η is of characteristic zero. In the former case, let U_1 denote any neighborhood of η which lies over $\mathrm{Spec}\, \mathbb{F}_p$. In the latter case, Z_η is geometrically reduced [Grothendieck 1965, Proposition 4.6.1 on p. 68], so Z_x is geometrically reduced for all x in some neighborhood U_1 of η [Grothendieck 1966, Theorem 9.7.7(iii) on p. 79]. Let W denote the Zariski closure of $\overline{\xi(Z)} \setminus \xi(Z)$ in Y, endowed with its reduced induced scheme structure. As $\xi(Z_\eta)$ is closed in Y_η, the η-fibers of $\xi(Z)$ and $\overline{\xi(Z)}$ are the same, so W_η is empty. Let U_2 denote a neighborhood of η which does not meet the image of $W \to X$. Finally, let $U = U_1 \cap U_2$, $X_1 = X \setminus U$, $Y_1 = Y \times_X X_1$, and $Z_1 = Z \times_X X_1$.

By the induction hypothesis, if N is sufficiently divisible, the lemma holds for X_1, Y_1, and Z_1. Let X_1', Y_1', and ψ_1 be chosen suitably. Let $X' = U \coprod X_1'$ and $Y' = W_U \coprod Y_1'$, and let ψ denote the extension of ψ_1 which is given on W_U by the composition of the obvious maps $W_U \to Y \to \mathbb{P}_X^m \to X$. If $x \in X(F)$ belongs to $X_1(F)$, we are done already. If not, it belongs to $U(F)$. Let x' denote the image of $x \in U(F)$ under the inclusion $U \to X'$. As $U \subset U_2$, at the set level, the fiber $Y_{x'}'$ coincides with $\xi(Z_x)$. As $U \subset U_1$, if F is a $\mathbb{Z}[1/N]$-algebra, then $Y_{x'}'$ is reduced. $\quad\square$

We now specialize to the case $F = \mathbb{F}_p$, where $p \geq n$. If Γ is a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$, we write Γ^+ for the subgroup of Γ generated by all elements of order p. Let $N(\Gamma) = N(\Gamma^+)$ denote the set $\{\log u \mid u^p = 1, u \in \Gamma\}$, and let $G := G_{N(\Gamma)}$. Then $\Gamma^+ \subset G(\mathbb{F}_p)$.

Definition 5. If Γ is a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ we define the *Nori dimension*, Ndim Γ, to be $\dim G_{N(\Gamma)}$. Likewise if $\mathcal{G}$ is a subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$ its Nori dimension, Ndim $\mathcal{G}$, is the Nori dimension of its reduction $(\bmod\ p)$.

Lemma 6. *Let $p \geq 2n$, let x be a nilpotent $n \times n$ matrix over $\mathbb{F}_p$, and let $A \in \mathrm{GL}_n(\mathbb{Z}_p)$ be a p-adic lift of $\exp(x)$. For all positive integers k,*

$$A^{p^k} \equiv 1 + p^k M \pmod{p^{k+1}},$$

where M reduces $(\bmod\ p)$ to x.

Proof. It suffices to prove the lemma when $k = 1$. Without loss of generality, we may assume that M is nilpotent, so $M^p = 0$. Let $N = \exp(M) - 1$. As N reduces $(\bmod\ p)$ to the nilpotent element $\exp(x) - 1$, N^n is divisible by p in $M_n(\mathbb{Z}_p)$, and we can write A as $1 + N + pB$ for some $B \in M_n(\mathbb{Z}_p)$. Expanding,

$$A^p = (1 + N + pB)^p = \sum_{m=0}^{p} \binom{p}{m}(N + pB)^m$$

$$\equiv \sum_{m=0}^{p} \binom{p}{m}\left(N^m + p \sum_{i+j=m-1} N^i B N^j\right)$$

$$\equiv \sum_{m=0}^{p} \binom{p}{m} N^m = (1 + N)^p = \exp(pM) \equiv 1 + pM \pmod{p^2}. \quad\square$$

Theorem 7. *For every positive integer n there exist constants A_n, B_n, and C_n such that if $p > A_n$ is prime, $\mathcal{G}$ is a closed subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$, and G is the Zariski closure of $\mathcal{G}$ in $\mathrm{GL}_{n,\mathbb{Q}_p}$, then Ndim $\mathcal{G} \leq \dim G$. If Ndim $\mathcal{G} = \dim G$, then:*

(1) *$\mathcal{G}$ is an open subgroup of $G(\mathbb{Q}_p)$.*

(2) *G/G° is of prime-to-p order and has a normal abelian subgroup of index $\leq B_n$.*

(3) *If*, *in addition*, *the radical of G° is unipotent*, *then*

$$[G(\mathbb{Q}_p) \cap GL_n(\mathbb{Z}_p) : \mathcal{G}] \leq C_n.$$

Proof. We fix $A_n \geq 2n$ large enough for Proposition 3 to apply.

Let $\mathcal{H} = G(\mathbb{Q}_p) \cap GL_n(\mathbb{Z}_p)$. Let $F_m\mathcal{H}$ denote the subgroup of $\mathcal{H}$ consisting of elements congruent to 1 (mod p^m). We identify $F_m\mathcal{H}/F_{m+1}\mathcal{H}$ with a subspace of M_n over the field $\mathbb{F}_p$. As

$$(1 + p^m A)^p \equiv 1 + p^{m+1}A \quad (\text{mod } p^{m+2}),$$

we have that

$$F_m\mathcal{H}/F_{m+1}\mathcal{H} \subset F_{m+1}\mathcal{H}/F_{m+2}\mathcal{H}$$

for all $m \geq 1$. It follows that

$$\dim F_m\mathcal{H}/F_{m+1}\mathcal{H} \leq \dim G$$

for all $m \geq 1$. Indeed, otherwise, the quotient $\mathcal{H}/F_m\mathcal{H}$ would grow at least as fast as $cp^{m(1+\dim G)}$, which is impossible [Serre 1981, Theorem 8].

As $\mathcal{G} \subset \mathcal{H}$, we have

$$F_m\mathcal{G}/F_{m+1}\mathcal{G} \subset F_m\mathcal{H}/F_{m+1}\mathcal{H}.$$

By the preceding lemma the dimension of $F_m\mathcal{G}/F_{m+1}\mathcal{G}$ is at least the dimension of the vector space spanned by the logarithms of elements of order p in the (mod p) reduction of $\mathcal{G}$. By the correspondence between exponentially generated groups and nilpotently generated Lie algebras this dimension is the Nori dimension of $\mathcal{G}$. In summary, for all $m \geq 1$,

$$\text{Ndim } \mathcal{G} \leq F_m\mathcal{G}/F_{m+1}\mathcal{G} \leq F_m\mathcal{H}/F_{m+1}\mathcal{H} \leq \dim G.$$

This proves the first claim of the theorem.

If the Nori dimension of $\mathcal{G}$ equals $\dim G$, we have further that

$$\dim F_m\mathcal{G}/F_{m+1}\mathcal{G} = \dim F_m\mathcal{H}/F_{m+1}\mathcal{H},$$

for all $m \geq 1$. As $\mathcal{G}$ and $\mathcal{H}$ are closed subgroups of $GL_n(\mathbb{Z}_p)$, this implies $F_1\mathcal{G} = F_1\mathcal{H}$, which implies (1).

If G is any closed subgroup of GL_n, there exists a finite central extension of G/G° which can be realized as a subgroup of $G(\mathbb{Q}_p)$. (See, e.g., the proof of [Khare et al. 2008, Proposition 6.2].) Jordan's theorem implies the existence of a normal abelian subgroup of bounded index.

For $n < p - 1$, $GL_n(\mathbb{Q}_p)$ has no element of order p, since the p-th cyclotomic polynomial is irreducible over $\mathbb{Q}_p$. On the other hand, every extension of a group containing an element of order p again has an element of order p. This gives (2).

For (3), we note first that since $\mathcal{G}$ meets every component of G, it suffices to prove that

$$\mathcal{G}^\circ := \mathcal{G} \cap G^\circ(\mathbb{Q}_p)$$

is of bounded index in $G^\circ(\mathbb{Q}_p) \cap \mathrm{GL}_n(\mathbb{Z}_p)$. As $[\mathcal{G} : \mathcal{G}^\circ]$ is prime to p, the (mod p) reduction of $\mathcal{G}^\circ$ is of prime-to-p index in that of $\mathcal{G}$. It follows that $\mathrm{Ndim}\,\mathcal{G}^\circ = \mathrm{Ndim}\,\mathcal{G}$. Replacing $\mathcal{G}$ with $\mathcal{G}^\circ$ if necessary, we may assume without loss of generality that G is connected.

Let F denote any finite extension of $\mathbb{Q}_p$ over which G has no nontrivial anisotropic quotient. We may take F to be totally ramified over $\mathbb{Q}_p$ since the anisotropic simple groups over $\mathbb{Q}_p$ are all central quotients of groups of the form $\mathrm{SL}_1(D)$, where D is a division algebra over $\mathbb{Q}_p$ [Kneser 1965], and every degree n division algebra over $\mathbb{Q}_p$ splits over $\mathbb{Q}_p(p^{1/n})$. We denote by $\mathcal{O}$ the ring of elements of nonnegative valuation in F. Thus, the residue field of $\mathcal{O}$ is $\mathbb{F}_p$. By Proposition 2, G_F is exponentially generated.

Let $\bar{G}_F$ denote $G_F \cup (\mathbb{P}_F^{n^2} \setminus \mathrm{GL}_{n,F})$, regarded as a reduced subscheme of $\mathbb{P}_F^{n^2}$ and $\bar{G}_\mathcal{O}$ denote the schematic closure of $\bar{G}_F \subset \mathbb{P}_\mathcal{O}^{n^2}$ in $\mathbb{P}_\mathcal{O}^{n^2}$, i.e., the unique $\mathcal{O}$-flat closed subscheme of $\mathbb{P}_\mathcal{O}^{n^2}$ having generic fiber $\bar{G}_F$ [Grothendieck 1965, Proposition 2.8.5 on p. 35]. Thus, $\mathcal{H} \subset \bar{G}_\mathcal{O}(\mathcal{O})$.

Let X denote the union of Hilbert schemes of the polynomials in S over $\mathbb{Z}[1/N]$, where N and S are given by Proposition 3. Let Y be the universal closed subscheme of $\mathbb{P}_X^{n^2}$ with Hilbert polynomials in S. If A_n is sufficiently large, for every $p > A_n$, every p-adic field F, and every exponentially generated $G_F \subset \mathrm{GL}_{n,F}$, there exists an F-point $x \in X(F)$ such that $G_F = Y_x \cap \mathrm{GL}_{n,F}$. By the valuative criterion of properness, x extends to a morphism $\mathrm{Spec}\,\mathcal{O} \to X$, where $\mathcal{O}$ is the ring of integers in F. Pulling back Y by this morphism, we obtain an $\mathcal{O}$-flat subscheme of $\mathrm{GL}_{n,\mathcal{O}}$ whose generic point is $\bar{G}_F$. This must be isomorphic to $\bar{G}_\mathcal{O}$ by uniqueness of flat extension over $\mathcal{O}$. Let $G_\mathcal{O}$ denote the intersection of $\bar{G}_\mathcal{O}$ with $\mathrm{GL}_{n,\mathcal{O}} \subset \mathbb{P}_\mathcal{O}^{n^2}$. Thus $G_\mathcal{O}$ is flat over $\mathcal{O}$ and the generic fiber of $G_\mathcal{O}$ is $\bar{G}_F \cap \mathrm{GL}_{n,F} = G_F$. The fiber $G_{\mathbb{F}_p}$ has no more irreducible components than the fiber $\bar{G}_{\mathbb{F}_p}$, which can be regarded as a fiber of $Y \to X$. By the local constructibility of the function giving the number of irreducible components of geometric fibers [Grothendieck 1966, Corollary 9.7.9 on p. 82] and Noetherian induction, this gives an upper bound d_n on $G_{\mathbb{F}_p}/G_{\mathbb{F}_p}^\circ$ independent of G and $p > A_n$.

By the flatness of $G_\mathcal{O}$, the special fiber $G_{\mathbb{F}_p}$ has dimension equal to that of G_F, which is $\mathrm{Ndim}\,\mathcal{G}$. We claim that the number of $\mathbb{F}_p$-points of a connected d-dimensional algebraic group over $\mathbb{F}_p$ is at least $(p-1)^d$ and at most $(p+1)^d$. This is obvious for additive groups (where the number of points is p^d) and tori (where the number of points is $Q(p)$, Q being the characteristic polynomial of Frobenius on the character group), and it is well-known in the semisimple case. It

follows in the general case from the structure theory of connected linear algebraic groups. The upper bound implies

$$G_{\mathbb{F}_p}(\mathbb{F}_p) \leq |G_{\mathbb{F}_p}/G^\circ_{\mathbb{F}_p}|(p+1)^{\mathrm{Ndim}\,\mathcal{G}} \leq d_n(3/2)^{n^2} p^{\mathrm{Ndim}\,\mathcal{G}}.$$

The kernel $F_1 G_{\mathbb{O}}(\mathbb{O})$ of the reduction map

$$G_{\mathbb{O}}(\mathbb{O}) \to G_{\mathbb{O}}(\mathbb{F}_p) = G_{\mathbb{F}_p}(\mathbb{F}_p)$$

consists of elements of $F_1\,\mathrm{GL}_n(\mathbb{O})$, i.e., elements of $\mathrm{GL}_n(\mathbb{O})$ congruent to 1 modulo the maximal ideal of $\mathbb{O}$. Thus,

$$\mathcal{H} \cap F_1 G_{\mathbb{O}}(\mathbb{O}) \subset \mathrm{GL}_n(\mathbb{Z}_p) \cap F_1\,\mathrm{GL}_n(\mathbb{O}) = F_1\,\mathrm{GL}_n(\mathbb{Z}_p).$$

It follows that

$$|\mathcal{H}/F_1\mathcal{H}| \leq d_n(3/2)^{n^2} p^{\mathrm{Ndim}\,\mathcal{G}}.$$

On the other hand, by Nori's theorem [1987], $(\mathcal{G}/F_1\mathcal{G})^+$ is of bounded index e_n in $G_{N(\mathcal{G}/F_1\mathcal{G})}(\mathbb{F}_p)$. The lower bound for points on a connected group implies

$$|\mathcal{G}/F_1\mathcal{G}| \geq |(\mathcal{G}/F_1\mathcal{G})^+| \geq e_n^{-1}(p-1)^{\mathrm{Ndim}\,\mathcal{G}} \geq e_n^{-1} 2^{-n^2} p^{\mathrm{Ndim}\,\mathcal{G}}.$$

Combining these estimates, we obtain

$$\frac{|\mathcal{H}/F_1\mathcal{H}|}{|\mathcal{G}/F_1\mathcal{G}|} \leq 3^{n^2} d_n e_n.$$

As $F_1\mathcal{G} = F_1\mathcal{H}$, setting $C_n = 3^{n^2} d_n e_n$, we obtain (3). $\qquad\square$

References

[Borel 1991] A. Borel, *Linear algebraic groups*, 2nd ed., Graduate Texts in Mathematics **126**, Springer, New York, 1991. MR 92d:20001 Zbl 0726.20030

[Chevalley 1954] C. Chevalley, "On algebraic group varieties", *J. Math. Soc. Japan* **6** (1954), 303–324. MR 16,672g Zbl 0057.26301

[Grothendieck 1961] A. Grothendieck, "Techniques de construction et théorèmes d'existence en géométrie algébrique, IV: les schémas de Hilbert", in *Séminaire Bourbaki,* 1960/61, fasc. 3, exposé 221, Secrétariat mathématique, Paris, 1961. Reprinted W. A. Benjamin, Amsterdam, 1966, and Soc. Mat. de France, Paris, 1995, pp. 249–276.

[Grothendieck 1965] A. Grothendieck, "Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, II", *Inst. Hautes Études Sci. Publ. Math.* **24** (1965), 1–231. MR 33 #7330 Zbl 0135.39701

[Grothendieck 1966] A. Grothendieck, "Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, III", *Inst. Hautes Études Sci. Publ. Math.* **28** (1966), 1–255. MR 36 #178 Zbl 0144.19904

[Khare et al. 2008] C. Khare, M. Larsen, and G. Savin, "Functoriality and the inverse Galois problem", *Compos. Math.* **144**:3 (2008), 541–564. MR 2009m:11076 Zbl 1194.11062

[Kneser 1965] M. Kneser, "Galois-Kohomologie halbeinfacher algebraischer Gruppen über p-adischen Körpern, II", *Math. Z.* **89** (1965), 250–272. MR 32 #5658 Zbl 0143.04702

[Nori 1987] M. V. Nori, "On subgroups of $GL_n(\mathbf{F}_p)$", *Invent. Math.* **88**:2 (1987), 257–275. MR88d: 20068 Zbl 0632.20030

[Serre 1981] J.-P. Serre, "Quelques applications du théorème de densité de Chebotarev", *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 123–201. MR 83k:12011 Zbl 0496.12011

[Steinberg 1965] R. Steinberg, "Regular elements of semisimple algebraic groups", *Inst. Hautes Études Sci. Publ. Math.* **25** (1965), 49–80. MR 31 #4788 Zbl 0136.30002

mjlarsen@indiana.edu   *Department of Mathematics, Rawles Hall, Indiana University, Bloomington, IN 47405-5701, United States*
http://mlarsen.math.indiana.edu/~larsen/

Algebra & Number Theory

www.jant.org

Copyright ©2010 by Mathematical Sciences Publishers

Algebra & Number Theory