CHARACTER VARIETIES OVER PRIME FIELDS AND REPRESENTATION RIGIDITY

BRUNO KLINGLER

1. Results

A finitely generated group Γ is said to be *n-rigid* (where n denotes a positive integer) if Γ has only finitely many conjugacy classes of complex irreducible representations $\rho : \Gamma \longrightarrow \mathbf{GL}_r(\mathbb{C})$, $1 \leq r \leq n$, and *rigid* if it is n-rigid for every positive integer n. Many "natural" groups are rigid; in particular arithmetic groups of higher rank like $\mathbf{SL}_n(\mathbb{Z})$, $n \geq 2$, are even superrigid [14], i.e. their complex proalgebraic completion is finite dimensional.

It has long been observed that the rigidity of Γ is linked to the properties of its finite quotients:

- the set $\mathrm{Rep}_n(\Gamma)(\mathbb{C})$ of complex representations of degree at most n of Γ contains the ones *with finite image*, that is the continuous representations of degree at most n of the profinite completion $\hat{\Gamma}$ of Γ. Hence a necessary condition for Γ to be n-rigid is that $\hat{\Gamma}$ is n-rigid (where we extend the definition of rigidity to topologically finitely generated topological groups by considering only *continuous* representations).

- this link has long been studied in the case where Γ is an arithmetic group. Let $\mathbf{G}$ be a connected semisimple linear algebraic group defined over $\mathbb{Q}$ and $\Gamma \subset \mathbf{G}(\mathbb{Q})$ be an arithmetic group (i.e. commensurable with $\mathbf{G}(\mathbb{Z})$). In this case the problem of classifying the representations of Γ with finite image is known as the congruence subgroup problem [3]. One says that the arithmetic group Γ has the congruence subgroup property (abbreviated CSP) if any subgroup of finite index of Γ contains a subgroup of the form $\ker(\mathbf{G}(\mathbb{Z}) \longrightarrow \mathbf{G}(\mathbb{Z}/N\mathbb{Z}))$. It is well known that the (generalized) CSP holds for "most" families of higher rank arithmetic lattices (we refer to the excellent recent survey [21] and the references therein). It was observed by Bass-Milnor-Serre and Raghunathan that the CSP implies superrigidity (cf. [3, section 16] and [22, section 7]).

1.1. Our first result clarifies the link between rigidity and finite quotients for an arbitrary finitely generated group Γ: the rigidity of Γ is equivalent to a boundedness property of the representation theory of Γ over *prime* fields.

Theorem 1.1. *Let Γ be a finitely generated group and n a positive integer. The following two conditions are equivalent:*

(i) *the group Γ is n-rigid.*

(ii) *there exists a positive integer c_n such that for any prime p the number of $\mathbf{GL}_r(\mathbb{F}_p)$-conjugacy classes of absolutely irreducible representations $\rho : \Gamma \longrightarrow \mathbf{GL}_r(\mathbb{F}_p)$, $1 \leq r \leq n$, is bounded above by c_n (where $\mathbb{F}_p$ denotes the finite field with p elements).*

The main ingredient in the proof of theorem 1.1 is the modular interpretation *over the integers* of (an interesting variant of) the character variety of Γ provided by Nakamoto [16].

1.2. Considering finite simple quotients of a group is often more convenient than dealing with its absolutely irreducible representations over a finite field. We obtain a criterium for a finitely generated group Γ to be rigid in terms of its finite simple quotients of Lie type (we refer to the appendix B for our conventions concerning finite simple groups of Lie type):

Theorem 1.2. *Let Γ be a finitely generated group. Suppose that:*

(i) *Γ has property (FAb) (meaning that any finite index subgroup of Γ has finite abelianization).*

(ii) *for every $n \in \mathbb{Z}^{>0}$ there exists a constant $c_n \in \mathbb{Z}^{>0}$ such that the following holds.*
Let $J(n) \in \mathbb{Z}^{>0}$ be any integer as provided by theorem 3.1. For any normal subgroup Γ' of Γ of index $[\Gamma : \Gamma'] \leq J(n)$, for every prime p and every finite simple subgroup of Lie type $G \subset \mathbf{GL}(n, \mathbb{F}_p)$ of characteristic p acting semisimply on $\mathbb{F}_p^n$, the number of G-conjugacy classes of surjective *morphisms $\rho : \Gamma' \twoheadrightarrow G$ is bounded above by c_n.*

Then Γ is rigid.

Theorem 1.2 follows from theorem 1.1 as follows. The classical Jordan lemma, which states that for every $n \in \mathbb{Z}^{>0}$ there exists $J(n) \in \mathbb{Z}^{>0}$ such that any finite subgroup $\Gamma \subset \mathbf{GL}_n(\mathbb{C})$ admits an abelian normal subgroup Γ_1 of index at most $J(n)$, implies that condition (i) in theorem 1.2 is equivalent to the profinite completion $\hat{\Gamma}$ being rigid (cf. [2, prop.2 (1)]). In particular condition (i) is necessary for Γ being rigid. We use the generalization of Jordan's lemma to fields of positive characteristic (obtained by Nori [17, paragraph 3], Gabber [9, theor. 12.4.1] and Larsen-Pink [12, theor. 0.2]) to prove that conditions (i) and (ii) in theorem 1.2 imply that Γ satisfies property (ii) of theorem 1.1 for any positive integer n, hence is rigid by theorem 1.1. It is not clear to me whether or not condition (ii) in theorem 1.2 is necessary for Γ being rigid.

1.3. Next we use theorem 1.2 and strong approximation (cf. [27] and [18]) to generalize to finitely generated linear groups the statement that for arithmetic groups "CSP implies rigidity".

Let us first recall the definition of the CSP for S-arithmetic groups and the result of Bass-Milnor-Serre and Raghunathan. We will use the following notations. Let k be a global field (i.e. either a number field or the function field of an algebraic curve over a finite field). We let V denote the set of all places of k and V_f (resp. V_∞) the subset of non-Archimedean (resp. Archimedean) places. As usual for $v \in V$ we let k_v denote the corresponding completion. If $v \in V_f$ we moreover denote by $\mathcal{O}_{k_v}$ the ring of integers of k_v. For any finite set S of V we let $\mathbb{A}_k^S$ denote the ring of adèles of k outside of S. Let S be a finite subset of V containing V_∞ and denote by $\mathcal{O}_S$ the ring of S-integers $\mathcal{O}_S = \{x \in k \mid v(x) \geq 0 \text{ for all } v \notin S\}$.

Let $\mathbf{G}$ be an algebraic k-group. We fix a k-embedding $\mathbf{G} \overset{\iota}{\hookrightarrow} \mathbf{GL}_n$ and define the group of S-integral points $\Gamma := \mathbf{G}(\mathcal{O}_S)$ to be $\mathbf{G}(k) \cap \mathbf{GL}_n(\mathcal{O}_S)$. The congruence kernel of Γ is defined as the kernel $C^S(\mathbf{G}) := \ker(\widehat{\mathbf{G}(k)} \longrightarrow \mathbf{G}(\mathbb{A}_k^S))$, where $\widehat{\mathbf{G}(k)}$ denotes the completion of $\mathbf{G}(k)$ with respect to the topology defined by the family of all normal subgroups of finite index of Γ. One says that Γ has the (generalized) CSP if $C^S(\mathbf{G})$ is finite. In [3, section 16] and [22, section 7] it is proven that when $\mathbf{G}$ is semi-simple, simply connected, and satisfy strong approximation, if the group Γ has the CSP then Γ is superrigid. We prove:

Theorem 1.3. *Consider finitely many connected simply connected absolutely simple linear algebraic groups $\mathbf{G}_i$ over global fields k_i, $1 \leq i \leq m$, and a finitely generated subgroup $\Gamma \subset \prod_{i=1}^m \mathbf{G}_i(k_i)$ whose image in each factor is Zariski-dense. For each $1 \leq i \leq m$ let $S_{i,\Gamma}$ denote the (finite) set of places v of k_i for which either v is Archimedean or the image of Γ in $\mathbf{G}_i(k_{i,v})$ does not lie in a compact subgroup. Define the congruence kernel $C(\Gamma)$ as the kernel of the natural map $\hat{\Gamma} \longrightarrow \prod_{i=1}^m \mathbf{G}_i(\mathbb{A}_{k_i}^{S_{i,\Gamma}})$, where $\hat{\Gamma}$ denotes the profinite completion of Γ.*

If Γ has property (FAb) and $C(\Gamma)$ is prosolvable then Γ is rigid.

Remarks 1.4.

(a) In the S-arithmetic case considered by Bass-Milnor-Serre and Raghunathan, theorem 1.3 shows that "CSP implies rigidity". Indeed suppose for simplicity that $\mathbf{G}$ is a connected simply connected absolutely simple group over the global field k and let $\Gamma = \mathbf{G}(\mathcal{O}_S)$. We consider theorem 1.3 for $m = 1$, the set $S_{1,\Gamma}$ is equal to S and one easily shows that $C(\Gamma)$ is equal to $C^S(\mathbf{G})$. Under our assumptions it is known that the congruence kernel $C^S(\mathbf{G})$ is finite if and only if it is central in $\widehat{\mathbf{G}(k)}$ (cf. [21, theor.2]). In particular if $C^S(\mathbf{G})$ is finite it is abelian hence solvable (and clearly Γ has property (FAb)). Hence theorem 1.3 apply and "CSP implies rigidity".

(b) the assumptions of theorem 1.3 are much weaker than those of Bass-Milnor-Serre and Raghunathan: it applies to any finitely generated Zariski-dense subgroup of $\mathbf{G}(k)$ rather than to S-arithmetic subgroups.

(c) Theorem 1.3 should be useful in the context of Platonov's conjecture [19, p.437], which states that a linear rigid group is of arithmetic type. Bass and Lubotzky [1] found counterexamples to Platonov's conjecture (even superrigid ones). Theorem 1.3 might be helpful for finding more counterexamples.

The criterion provided by theorem 1.3 looks theoretically satisfactory. However I am not aware of any general strategy for proving the prosolvability of $C(\Gamma)$ in this situation: already in the arithmetic case this is a hard problem (cf. [21, section 5]). We refer to appendix C for remarks concerning $C(\Gamma)$.

1.4. **Acknowledgments.** I thank E. Breuillard for explaining me [12], Y. de Cornulier for answering my naive questions, and J.P. Serre for his comments.

2. Rigidity and representations over finite fields: proof of theorem 1.1

2.1. **Notations and definitions.** We follow the notations of [16]. Each commutative ring is unital. Morphisms of commutative rings map 1 to 1. If R is a commutative ring and $\mathfrak{p}$ is a prime ideal of R we denote by $k(\mathfrak{p})$ its residue field $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ and by $\overline{k(\mathfrak{p})}$ an algebraic closure of $k(\mathfrak{p})$. For a group Γ we denote by e the unit of Γ. For a scheme Z we denote by h_Z the functor $\mathrm{Hom}(\cdot, Z)$ from the category $\mathcal{S}ch$ of schemes to the category $\mathcal{S}ets$ of sets.

Definition 2.1. *Let Γ be a group and R a commutative ring. A map $\rho : \Gamma \longrightarrow \mathbf{GL}_n(R)$ is called a* representation *if ρ is a group homomorphism. Such a representation is* absolutely irreducible *if for each prime ideal $\mathfrak{p} \in \mathrm{Spec}\, R$ the induced representation $\rho_\mathfrak{p} : \Gamma \xrightarrow{\rho} \mathbf{GL}_n(R) \longrightarrow \mathbf{GL}_n(\overline{k(\mathfrak{p})})$ is irreducible. We abbreviate "absolutely irreducible representation" by "a.i.r".*

Definition 2.2. *Two representations $\rho, \rho' : \Gamma \longrightarrow \mathbf{GL}_n(R)$ are said* equivalent *(denoted $\rho \sim \rho'$) if there exists an R-algebra isomorphism $\sigma : M_n(R) \longrightarrow M_n(R)$ such that $\sigma(\rho(\gamma)) = \rho'(\gamma)$ for each $\gamma \in \Gamma$.*

Notice that if ρ is absolutely irreducible and $\rho \sim \rho'$ then ρ' is absolutely irreducible. If R is a field then $\rho \sim \rho'$ if and only if $\rho = P \cdot \rho' \cdot P^{-1}$ for some $P \in \mathbf{GL}_n(R)$ by the Skolem-Noether theorem.

These definitions naturally extend to schemes. A representation of Γ in a scheme X is a group morphism $\rho : \Gamma \longrightarrow \mathbf{GL}_n(H^0(X, \mathcal{O}_X))$. It is absolutely irreducible if for each $x \in X$ the representation $\rho_x : \Gamma \longrightarrow \mathbf{GL}_n(k(x))$ is absolutely irreducible. For two representations ρ and ρ' in a scheme X we say that ρ and ρ' are equivalent if there exists an $\mathcal{O}_X$-algebra isomorphism $\sigma : M_n(\mathcal{O}_X) \longrightarrow M_n(\mathcal{O}_X)$ such that $\sigma(\rho(\gamma)) = \rho'(\gamma)$ for each $\gamma \in \Gamma$.

We denote by $\mathcal{P}$ the set of prime numbers.

Given a finitely generated group Γ we denote by $\hat{\Gamma}$ its profinite completion.

2.2. **Nakamoto's result.** First we explain Nakamoto's result on representation varieties. Let Γ be a group. Let $\mathrm{Rep}_n(\Gamma) : \mathcal{S}ch^{\mathrm{op}} \longrightarrow \mathcal{S}ets$ be the functor parametrizing the representations of degree n of Γ:

$$(1) \qquad \forall\, X \in \mathcal{S}ch, \quad \mathrm{Rep}_n(\Gamma)(X) := \{\rho : \Gamma \longrightarrow \mathbf{GL}_n(H^0(X, \mathcal{O}_X))\, \text{representation}\} \ .$$

One easily shows that this functor is represented by an affine scheme $\mathrm{Rep}_n(\Gamma) = \mathrm{Spec}\, A_n(\Gamma)$. This is proven in [13, prop.1.2 p.3] in the case where Γ is a finitely generated group and one restricts to the category of affine $\mathbb{C}$-schemes. The same proof generalizes to the general case [16, prop.2.3]. If Γ is finitely generated then the scheme $\mathrm{Rep}_n(\Gamma)$ is of finite type over $\mathbb{Z}$, in particular noetherian.

The character variety $\mathrm{Char}_n(\Gamma)$ is defined as the GIT quotient of $\mathrm{Rep}_n(\Gamma)$ under the natural action of the $\mathbb{Z}$-group scheme $\mathbf{PGL}_n$:

$$\begin{aligned} \mathrm{Ad}\ : \quad & \mathrm{Rep}_n(\Gamma) \times \mathbf{PGL}_n \longrightarrow \mathrm{Rep}_n(\Gamma) \\ & (\rho, P) \mapsto P^{-1}\rho P \ . \end{aligned}$$

Hence $\mathrm{Char}_n(\Gamma) = \mathrm{Spec}\,(A_n(\Gamma)^{\mathbf{PGL}_n})$ (cf. [16, def.2.10], we refer the reader to [25] for details about the GIT construction over an arbitrary base). When Γ is finitely generated $\mathrm{Char}_n(\Gamma)$ is a universal categorical quotient of $\mathrm{Rep}_n(\Gamma)$, in particular of finite type over $\mathbb{Z}$ hence noetherian (cf. [15], [25]). However the modular interpretation of $\mathrm{Char}_n(\Gamma)$ seen as a $\mathbb{Z}$-scheme remains mysterious.

Following Nakamoto [16] we rather consider the subfunctor $\mathrm{Rep}_n(\Gamma)_{\mathrm{a.i.r}} : \mathcal{S}ch^{\mathrm{op}} \longrightarrow \mathcal{S}ets$ of $\mathrm{Rep}_n(\Gamma)$ parametrizing absolutely irreducible representations:

$$(2) \qquad \forall\, X \in \mathcal{S}ch, \quad \mathrm{Rep}_n(\Gamma)_{\mathrm{a.i.r}} := \{\rho : \Gamma \longrightarrow \mathbf{GL}_n(H^0(X, \mathcal{O}_X)) \text{ an a.i.r}\} \;\; .$$

It is representable by an open subscheme $\mathrm{Rep}_n(\Gamma)_{\mathrm{a.i.r}}$ of $\mathrm{Rep}_n(\Gamma)_{\mathrm{a.i.r}}$, whose explicit description shows that it is of finite type over $\mathbb{Z}$ when Γ is finitely generated (cf. [16, def.3.4]). Let's define the functor $\mathrm{EqAIR}_n(\Gamma) : \mathcal{S}ch^{\mathrm{op}} \longrightarrow \mathcal{S}ets$ parametrizing *equivalence classes* of absolutely irreducible representations:

$$(3) \qquad \forall\, X \in \mathcal{S}ch, \quad \mathrm{EqAIR}_n(\Gamma)(X) := \{\rho : \Gamma \longrightarrow \mathbf{GL}_n(H^0(X, \mathcal{O}_X)) \text{ an a.i.r}\}/\sim \;\; .$$

The main result of Nakamoto in [16], building on Donkin's work [5], can now be stated as follows:

Theorem 2.3 (Nakamoto)**.** *Let Γ be any group.*

(a) *There exists a coarse moduli scheme $\mathrm{Char}_n(\Gamma)_{\mathrm{a.i.r}}$ over $\mathbb{Z}$ associated to the moduli functor $\mathrm{EqAIR}_n(\Gamma)$. In other words there exist a separated scheme $\mathrm{Char}_n(\Gamma)_{\mathrm{a.i.r}}$ over $\mathbb{Z}$ and a natural transformation*

$$\tau : \mathrm{EqAIR}_n(\Gamma) \longrightarrow h_{\mathrm{Char}_n(\Gamma)_{\mathrm{a.i.r}}}$$

satisfying the following two conditions:

(1) *For any scheme Z the natural transformation τ induces an isomorphism*

$$\tau : \mathrm{Hom}(\mathrm{EqAIR}_n(\Gamma), h_Z) \simeq \mathrm{Hom}(h_{\mathrm{Char}_n(\Gamma)_{\mathrm{a.i.r}}}, h_Z)(\simeq \mathrm{Hom}_{\mathcal{S}ch}(Z, \mathrm{Char}_n(\Gamma)_{\mathrm{a.i.r}})) \;\; .$$

(2) *For any algebraically closed field Ω the morphism*

$$\tau : \mathrm{EqAIR}_n(\Gamma)(\mathrm{Spec}\,\Omega) \longrightarrow \mathrm{Hom}(\mathrm{Spec}\,\Omega, \mathrm{Char}_n(\Gamma)_{\mathrm{a.i.r}})$$

is bijective.

(b) *The natural morphism $\pi : \mathrm{Rep}_n(\Gamma)_{\mathrm{a.i.r}} \longrightarrow \mathrm{Char}_n(\Gamma)_{\mathrm{a.i.r}}$ is a universal geometric quotient by $\mathbf{PGL}_n$. Moreover it is a torsor under $\mathbf{PGL}_n$.*

(c) *When Γ is finitely generated the scheme $\mathrm{Char}_n(\Gamma)_{\mathrm{a.i.r}}$ is of finite type over $\mathbb{Z}$.*

Statement (a) is [16, Theor1.3], statement (b) is [16, cor. 6.8], statement (c) is [16, rem.6.9].

2.3. **A general lemma.**

Lemma 2.4. *Let X be an affine scheme of finite type over $\mathbb{Z}$. Then $X \times_{\operatorname{Spec}\mathbb{Z}} \operatorname{Spec}\mathbb{C}$ is 0-dimensional if and only if there exists a constant c_X such that for any prime number p the inequality $|X(\mathbb{F}_p)| < c_X$ holds.*

Proof. Let X be an affine scheme of finite type over $\mathbb{Z}$. By [6, 1.6.1] the scheme X is of finite presentation. Let n be the dimension of $X \times_{\operatorname{Spec}\mathbb{Z}} \operatorname{Spec}\mathbb{C}$.

Let $f : \operatorname{Spec}\mathbb{Z} \longrightarrow \mathbb{Z}^{>0}$ be the function which associates to a prime p the number $f(p)$ of geometrically irreducible components of $X_{\mathbb{F}_p}$ of dimension n. By [8, 9.7.9] the function f is constructible. In particular there exists $N \in \mathbb{Z}^{>0}$ such that f is constant on $\operatorname{Spec}\mathbb{Z}[1/N]$. Let $l := f(\operatorname{Spec}\mathbb{Z}[1/N]) \in \mathbb{Z}^{>0}$.

It follows from the generic flatness theorem [7, 6.9.1] that, increasing N if necessary, X is flat over $\mathbb{Z}[1/N]$. In particular all fibers $X_{\mathbb{F}_p}$, $p \not| N$, have the same dimension n.

The Lang-Weil estimates [11] (in their affine version) state that there exists $c_X \in \mathbb{Z}^{>0}$ such that for any $p \in \mathcal{P}$, $p \not| N$, the following holds:

$$||X(\mathbb{F}_p)| - l \cdot p^n| < c_X p^{n-\frac{1}{2}} \quad .$$

This imply that $n = 0$ if and only if $|X(\mathbb{F}_p)|$ is uniformly bounded as p ranges through $\mathcal{P}$. $\square$

2.4. **End of the proof of theorem 1.1.** Statement (i) in theorem 1.1 is equivalent to saying that the $\mathbb{C}$-scheme $\operatorname{Char}_r(\Gamma)_{\text{a.i.r}} \times_{\operatorname{Spec}\mathbb{Z}} \operatorname{Spec}\mathbb{C}$ is 0-dimensional, $1 \leq r \leq n$.

As we assume that Γ is a finitely generated group, for any $r \in \mathbb{Z}^{>0}$ the scheme $\operatorname{Char}_r(\Gamma)_{\text{a.i.r}}$ is of finite type over $\mathbb{Z}$ by theorem 2.3(c).

From lemma 2.4 one obtains that statement (i) is equivalent to the uniform boundedness of $|\operatorname{Char}_r(\Gamma)_{\text{a.i.r}})(\mathbb{F}_p)|$, $1 \leq r \leq n$, as p ranges through $\mathcal{P}$.

This is equivalent to statement (ii) by the following lemma:

Lemma 2.5. *The set $\operatorname{Char}_r(\Gamma)_{\text{a.i.r}}(\mathbb{F}_p)$ is in bijection with the set of conjugacy classes of absolutely irreducible representations $\rho : \Gamma \longrightarrow \mathbf{GL}_r(\mathbb{F}_p)$.*

Proof. By theorem 2.3[(a)] the set $\operatorname{Char}_r(\Gamma)_{\text{a.i.r}}(\overline{\mathbb{F}_p})$ is in bijection with the set of conjugacy classes of irreducible representations $\rho : \Gamma \longrightarrow \mathbf{GL}_r(\overline{\mathbb{F}_p})$. Hence the subset $\operatorname{Char}_r(\Gamma)_{\text{a.i.r}}(\mathbb{F}_p)$ of $\operatorname{Char}_r(\Gamma)_{\text{a.i.r}}(\overline{\mathbb{F}_p})$ can be seen as a set of conjugacy classes of certain irreducible representations $\rho : \Gamma \longrightarrow \mathbf{GL}_r(\overline{\mathbb{F}_p})$.

By theorem 2.3[(b)] $\operatorname{Rep}_r(\Gamma)_{\text{a.i.r}}$ is a $\operatorname{Char}_r(\Gamma)_{\text{a.i.r}}$-torsor under $(\mathbf{PGL}_r)_{\mathbb{Z}}$, hence the base-change $(\operatorname{Rep}_r(\Gamma)_{\text{a.i.r}})_{\mathbb{F}_p}$ is a $(\operatorname{Char}_r(\Gamma)_{\text{a.i.r}})_{\mathbb{F}_p}$-torsor under $(\mathbf{PGL}_r)_{\mathbb{F}_p}$. Let $x \in \operatorname{Char}_r(\Gamma)_{\text{a.i.r}}(\mathbb{F}_p)$. The fiber at x of the morphism $\pi_p : (\operatorname{Rep}_r(\Gamma)_{\text{a.i.r}})_{\mathbb{F}_p} \longrightarrow \operatorname{Char}_r(\Gamma)_{\text{a.i.r}}(\mathbb{F}_p)$ is thus an $\mathbb{F}_p$-torsor under $(\mathbf{PGL}_r)_{\mathbb{F}_p}$. By Lang's theorem [10] this torsor is trivial, which exactly means that x lifts to an $\mathbb{F}_p$-point of $(\operatorname{Rep}_r(\Gamma)_{\text{a.i.r}})_{\mathbb{F}_p}$, namely an absolutely irreducible representation $\rho : \Gamma \longrightarrow \mathbf{GL}_r(\mathbb{F}_p)$.

Hence $\mathrm{Char}_r(\Gamma)_{\mathrm{a.i.r}}(\mathbb{F}_p)$ identifies with the set of stable conjugacy classes of absolutely irreducible representations $\rho : \Gamma \longrightarrow \mathbf{GL}_r(\mathbb{F}_p)$.

Notice that if $\rho_1, \rho_2 : \Gamma \longrightarrow \mathbf{GL}_r(\mathbb{F}_p)$ are absolutely irreducible and stably conjugate then they are conjugate. This follows from $\mathrm{Hom}_{\overline{\mathbb{F}_p}[\Gamma]}(\rho_1, \rho_2) = \mathrm{Hom}_{\mathbb{F}_p[\Gamma]}(\rho_1, \rho_2) \otimes_{\mathbb{F}_p} \overline{\mathbb{F}_p}$ and Schur's lemma.

This concludes the proof of theorem 1.1. □

3. Counting finite simple quotients of Lie type: proof of theorem 1.2

The classical Jordan's lemma does not hold in characteristic $p > 0$: for example the group $\mathbf{GL}_n(\overline{\mathbb{F}_p})$ contains arbitrarily large finite subgroups $\mathbf{SL}_n(\mathbb{F}_{p^r})$ which are simple modulo center. However Nori [17, paragraph 3], Gabber [9, theor. 12.4.1] and Larsen-Pink [12, theor. 0.2] provide generalization of this lemma to arbitrary characteristic.

Theorem 3.1. *(Larsen-Pink) For every $n \in \mathbb{Z}^{>0}$ there exists a constant $J(n)$ depending only on n such that any finite subgroup G of $\mathbf{GL}_n$ over any field k possesses normal subgroups $G_3 \subset G_2 \subset G_1 \subset G$ such that:*

(a) $[G : G_1] \leq J(n)$.
(b) *Either $G_1 = G_2$, or $p := \mathrm{char}(k)$ is positive and G_1/G_2 is a product of finite simple groups of Lie type in characteristic p.*
(c) *G_2/G_3 is abelian of order not divisible by* $\mathrm{char}(k)$.
(d) *Either $G_3 = \{1\}$, or $p := \mathrm{char}(k)$ is positive and G_3 is a p-group.*

We refer to appendix B for conventions concerning finite simple groups of Lie type.

Theorem 1.2 is then an immediate corollary of the following more precise:

Theorem 3.2. *Let Γ be a finitely generated group. Consider the following conditions:*

(i) *Γ is rigid.*
(ii) *for every $n \in \mathbb{Z}^{>0}$ there exists a positive integer c_n such that for any prime p the number of $\mathbf{GL}_n(\mathbb{F}_p)$-conjugacy classes of absolutely irreducible representations $\rho : \Gamma \longrightarrow \mathbf{GL}_n(\mathbb{F}_p)$ is bounded above by c_n.*
(iii) *for every $n \in \mathbb{Z}^{>0}$ there exists a positive integer c_n such that for any prime p the number of $\mathbf{GL}_r(\mathbb{F}_p)$-conjugacy classes of irreducible representations $\rho : \Gamma \longrightarrow \mathbf{GL}_n(\mathbb{F}_p)$ is bounded above by c_n.*
(iv) *the following two conditions hold:*
  (a) *Γ has property (FAb).*
  (b) *for every $n \in \mathbb{Z}^{>0}$ there exists a constant $c_n \in \mathbb{Z}^{>0}$ such that the following holds. Let $J(n) \in \mathbb{Z}^{>0}$ be any integer as provided by theorem 3.1. For any normal subgroup Γ' of Γ of index $[\Gamma : \Gamma'] \leq J(n)$, for every prime p and every finite simple subgroup of Lie type $G \subset \mathbf{GL}(n, \mathbb{F}_p)$ of characteristic p acting semisimply on $\mathbb{F}_p^n$, the number of $\mathbf{GL}(n, \mathbb{F}_p)$-conjugacy classes of* surjective *morphisms $\rho : \Gamma' \twoheadrightarrow G$ is bounded above by c_n.*

Then $(iv) \Longrightarrow (iii) \Longrightarrow (ii) \Longleftrightarrow (i)$.

Proof. Theorem 1.1 says that the conditions (i) and (ii) of theorem 3.2 are equivalent.

The implication $(iii) \Longrightarrow (ii)$ is clear.

Hence we only have to show that (iv) implies (iii).

3.0.1. *The case of finite groups.* Notice that any finite group Γ obviously satisfies condition (iv). We first show that (iv) implies (iii) in this particular case:

Lemma 3.3. *Let* Γ *be a finite group. Then* Γ *satisfies condition* (iii) *of theorem 3.2.*

Proof. This follows from the description of irreducible $\mathbb{F}_p$-representations of Γ for p not dividing $m := |G|$.

Let p not dividing m. First, the number of irreducible $\overline{\mathbb{F}_p}$-representations of Γ coïncide with the number of conjugacy classes of Γ. Any such representation is in fact defined over k, where k denotes the smallest finite extension of $\mathbb{F}_p$ containing all m-th roots of unity. Hence irreducible $k\Gamma$-modules are in bijection with conjugacy classes of elements of Γ.

The Galois group $\mathrm{Gal}(k/\mathbb{F}_p)$ is naturally a subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$. Two elements $\gamma, \gamma' \in \Gamma$ are said to be in the same $\mathbb{F}_p$-class if there exists $t \in \mathrm{Gal}(k/\mathbb{F}_p) \subset (\mathbb{Z}/m\mathbb{Z})^*$ such that γ and γ^t are conjugated in Γ. Then the number of irreducible $\mathbb{F}_p\Gamma$-modules is equal to the number of $\mathbb{F}_p$-classes in Γ, which is uniformly bounded by the number of conjugacy classes of Γ. □

3.0.2. *The general case.* We first fix some notations. Let p be a prime. Let $(\rho : \Gamma \longrightarrow \mathbf{GL}(V_\rho), V_\rho \simeq \mathbb{F}_p^n)$ be an irreducible representation. Let $G_\rho := \rho(\Gamma)$ and let

$$\mathbf{GL}(V_\rho) \simeq \mathbf{GL}_n(\mathbb{F}_p) \supset G_\rho \supset G_{1,\rho} \supset G_{2,\rho} \supset G_{3,\rho}$$

be the sequence of normal subgroups of G_ρ provided by theorem 3.1. First notice that any $\mathbb{F}_p$-representation of a p-group fixes a non-zero vector hence $G_{3,\rho}$ fixes a non-zero vector of V_ρ . As $G_{3,\rho}$ is normal in G_ρ and ρ is irreducible this implies that $G_{3,\rho} = 1$. Let $\Gamma_{i,\rho} \subset \Gamma$, $1 \leq i \leq 3$, be the subgroup $\rho^{-1}(G_{i,\rho})$. Hence one has the sequence of normal subgroups

$$\Gamma \supset \Gamma_{1,\rho} \supset \Gamma_{2,\rho} \supset \Gamma_{3,\rho} = \ker \rho \ .$$

The property (c) of theorem 3.1 then implies that the restriction of ρ to $\Gamma_{2,\rho}$ is an abelian character of $\Gamma_{2,\rho}$ of order prime to p.

Assume (iv) and suppose by contradiction that (iii) does not hold. Hence there exists a positive integer n such that the cardinality of the set of conjugacy classes of irreducible representations $\rho : \Gamma \longrightarrow \mathbf{GL}_n(\mathbb{F}_p)$ is unbounded as p ranges through $\mathcal{P}$. For such a representation ρ consider the subgroup $\Gamma_{1,\rho}$ of Γ. By property (a) of theorem 3.1 the index $[\Gamma : \Gamma_{1,\rho}]$ is bounded above by $J(n)$. As Γ is finitely generated it has only a finite number of subgroups of index at most $J(n)$. Hence there exists a normal subgroup $\Gamma' \subset \Gamma$ of index at most $J(n)$ such that the cardinality of the set $C_{n,\Gamma_1=\Gamma'}(\Gamma)(\mathbb{F}_p)$ of conjugacy classes of irreducible representations $\rho : \Gamma \longrightarrow \mathbf{GL}_n(\mathbb{F}_p)$ satisfying moreover $\Gamma_{1,\rho} = \Gamma'$ is unbounded as p ranges through $\mathcal{P}$.

By property (b) in theorem 3.1 one can decompose

$$C_{n,\Gamma_1=\Gamma'}(\Gamma)(\mathbb{F}_p) = C_{n,\Gamma_2=\Gamma'}(\Gamma)(\mathbb{F}_p) \amalg C_{n,\Gamma_2\neq\Gamma'}(\Gamma)(\mathbb{F}_p) \quad ,$$

where $C_{n,\Gamma_2=\Gamma'}(\Gamma)(\mathbb{F}_p)$ denotes the subset of conjugacy classes of representations such that moreover $\Gamma_{2,\rho} = \Gamma_{1,\rho}(= \Gamma')$. For $[\rho] \in C_{n,\Gamma_2=\Gamma'}(\Gamma)(\mathbb{F}_p)$ the representation ρ restricted to $\Gamma' = \Gamma_2$ is an abelian character of Γ'. By assumption the group Γ has property (FAb). Hence $(\Gamma')^{\mathrm{ab}} := \Gamma'/[\Gamma',\Gamma']$ is finite. The subgroup $[\Gamma',\Gamma']$ of Γ is normal of finite index and any $[\rho] \in C_{n,\Gamma_2=\Gamma'}(\Gamma)(\mathbb{F}_p)$, $p \in \mathcal{P}$, factorizes through the finite quotient $G := \Gamma/[\Gamma',\Gamma']$. It follows from lemma 3.3 that the cardinality of $C_{n,\Gamma_2=\Gamma'}(\Gamma)(\mathbb{F}_p)$ is bounded uniformly as p ranges through $\mathcal{P}$.

Hence the cardinality of $C_{n,\Gamma_2\neq\Gamma'}(\Gamma)(\mathbb{F}_p)$ has to be unbounded as p ranges through $\mathcal{P}$. Let $[\rho] \in C_{n,\Gamma_2\neq\Gamma'}(\Gamma)(\mathbb{F}_p)$. As $G_{2,\rho}$ is abelian of order prime to p, the restriction to $\Gamma_{2,\rho}$ of $\rho \otimes_{\mathbb{F}_p} \overline{\mathbb{F}_p}$ decomposes into isotypical components

$$V_\rho \otimes_{\mathbb{F}_p} \overline{\mathbb{F}_p} := \bigoplus_{\chi \in X^*(V_\rho)} V_{\rho,\chi} \quad , \tag{4}$$

where $X^*(V_\rho)$ denotes the set of characters χ of $G_{2,\rho}$ whose isotypical component $V_{\rho,\chi} \subset V_\rho \otimes_{\mathbb{F}_p} \overline{\mathbb{F}_p}$ is non-zero. Notice that $|X^*(V_\rho)| \leq n$. As $G_{2,\rho}$ is normal in G_ρ the group G_ρ acts by permutation on $X^*(V_\rho)$ hence a morphism $\lambda : G_\rho/G_{2,\rho} \longrightarrow S_n$. The group $G_{1,\rho}/G_{2,\rho}$ is a product of finite simple groups of Lie type. The restriction of λ to such a simple factor is necessarily injective or trivial. As there are only finitely many primes p such that there exists a finite simple subgroup of Lie type in characteristic p injecting into S_n, we can assume without loss of generality that λ is trivial on $G_{1,\rho}/G_{2,\rho}$ for every $[\rho] \in C_{n,\Gamma_2\neq\Gamma'}(\Gamma)(\mathbb{F}_p)$ as p ranges through $\mathcal{P}$. This means that the action of $G_{1,\rho}$ stabilizes the isotypical decomposition (4). Equivalently:

$$G_{1,\rho} = G_{2,\rho} \times G_{1,\rho}/G_{2,\rho} \quad ,$$

which implies that the abelian group $G_{2,\rho}$ is a quotient of $\Gamma' = \Gamma_{1,\rho}$. But Γ has property (FAb) hence $(\Gamma')^{\mathrm{ab}}$ is finite. Without loss of generality we can thus assume that the group $G_{2,\rho}$ is constant (we denote by G_2 this group) and all the morphisms $\Gamma' \longrightarrow G_{2,\rho} = G_2$ coïncide as p ranges through $\mathcal{P}$ and $[\rho]$ ranges through $C_{n,\Gamma_2\neq\Gamma'}(\Gamma)(\mathbb{F}_p)$.

Let Γ'' be the kernel of the projection $\Gamma' \longrightarrow G_2$. The restriction $\rho_{|\Gamma''} : \Gamma'' \longrightarrow \mathbf{GL}_n(\mathbb{F}_p)$ has for image the product $G_{1,\rho}/G_2$ of finite simple groups of Lie type of characteristic p in $\mathbf{GL}_n(\mathbb{F}_p)$ for every $[\rho] \in C_{n,\Gamma_2\neq\Gamma'}(\Gamma)(\mathbb{F}_p)$ as p ranges through $\mathcal{P}$. Notice the following two facts:

(i) For every $[\rho] \in C_{n,\Gamma_2\neq\Gamma'}(\Gamma)(\mathbb{F}_p)$, $p \in \mathcal{P}$, the representation $\rho_{\Gamma''}$ is semi-simple: this is not automatic as we work in the defining characteristic but follows from the fact that ρ is irreducible and Γ'' is normal in Γ' which is normal in Γ.

(ii) Given a representation α of degree n of Γ'' there exist at most $[\Gamma : \Gamma''] \cdot n$ irreducible representations ρ of Γ whose restrictions to Γ'' is isomorphic to α (this follows from Frobenius reciprocity $\mathrm{Hom}_{\Gamma''}(\alpha, \rho_{|\Gamma''}) = \mathrm{Hom}_\Gamma(\mathrm{Ind}_{\Gamma''}^{\Gamma}\alpha, \rho)$).

It follows from these two facts that if the cardinality of $C_{n,\Gamma_2\neq\Gamma'}(\Gamma)(\mathbb{F}_p)$ is unbounded as p ranges through $\mathcal{P}$ then the number of $\mathbf{GL}_n(\mathbb{F}_p)$-conjugacy classes of surjections from Γ'' (hence also from Γ') to a finite simple subgroup of Lie type of $\mathbf{GL}_n(\mathbb{F}_p)$ acting semi-simply on $\mathbb{F}_p^n$ is unbounded as p ranges through $\mathcal{P}$. By lemma B.1 it follows a fortiori that one gets a contradiction to the condition (b) of (*iv*).

This finishes the proof of theorem 3.2. $\square$

4. Solvability of the congruence kernel: proof of theorem 1.3

For simplicity we assume $m = 1$ and write $k = k_1$ and $S = S_{1,\Gamma}$. The general case is left to the reader.

It is enough to show that if Γ satisfies the conditions of theorem 1.3 then Γ satisfies property (ii) of theorem 1.2. Let $n \in \mathbb{Z}^{>0}$. Let $J(n) \in \mathbb{Z}^{>0}$ be any integer as provided by theorem 3.1. Let $\Gamma' \subset \Gamma$ be a normal subgroup of index $[\Gamma : \Gamma'] \leq J(n)$. Let p be a prime number and H be a finite simple group of Lie type of characteristic p. Let $\rho : \Gamma' \twoheadrightarrow H$ be a surjective morphism. It extends continuously to a surjective morphism $\rho : \widehat{\Gamma'} \twoheadrightarrow H$.

Consider the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C(\Gamma') & \longrightarrow & \widehat{\Gamma'} & \longrightarrow & \overline{\Gamma'} & \longrightarrow & 1 \\ \| & & \downarrow & & \downarrow & & \downarrow & & \| \\ 1 & \longrightarrow & C(\Gamma) & \longrightarrow & \widehat{\Gamma} & \longrightarrow & \overline{\Gamma} & \longrightarrow & 1 \end{array} \tag{5}$$

where $\overline{\Gamma'}$ (resp. $\overline{\Gamma}$) denotes the closure of Γ' (resp. Γ) in $\mathbf{G}(\mathbb{A}_k^S)$. As Γ' is of finite index in Γ the vertical map $\widehat{\Gamma'} \longrightarrow \hat{\Gamma}$ is injective. Hence the map $C(\Gamma') \longrightarrow C(\Gamma)$ is injective.

By assumption the group $C(\Gamma)$ is prosolvable hence $C(\Gamma')$ is also prosolvable. Thus $\rho(C(\Gamma'))$ is a normal solvable subgroup of the simple non-Abelian group H. Hence $\rho(C(\Gamma'))$ is trivial and ρ factorizes through $\rho : \overline{\Gamma'} \longrightarrow H$.

Under the hypotheses of theorem 1.3 the group Γ' satisfies strong approximation (cf. [27] and [18]): the group $\overline{\Gamma'}$ is a compact open subgroup of $\mathbf{G}(\mathbb{A}_k^S)$. In particular it contains a finite normal index subgroup of the form $U = \prod_{v\in V\setminus S} U_v$, where $U_v \subset \mathbf{G}(\mathcal{O}_{k_v})$ is a compact open subgroup of $\mathbf{G}(\mathcal{O}_{k_v})$, equal to $\mathbf{G}(\mathcal{O}_{k_v})$ for all $v \in V \setminus S'$ where S' is a finite subset of V containing S. As U is normal in $\overline{\Gamma'}$ and H is simple the image $\rho(U)$ is trivial or equal to H.

As Γ contains only finitely many subgroups Γ' of index at most n the following lemma implies that Γ satisfies property (ii) of theorem 1.2:

Lemma 4.1. *Let $\mathbf{G}$ be a connected simply connected absolutely simple linear algebraic group over a global field k. Let S be a finite subset of V and $U := \prod_{v\in V\setminus S} U_l$ be a compact open subgroup of $\mathbf{G}(\mathbb{A}_k^S)$. There exists a constant c such that for any finite simple group H of Lie type the number of H-conjugacy classes of surjections $\rho : U \twoheadrightarrow H$ is bounded above by c.*

Proof. For $v \in V\setminus S$ the group U_v is normal in U hence its image $\rho(U_v)$ is normal in $H = \rho(\overline{\Gamma})$. As H is simple $\rho(U_v)$ is trivial or equal to H. For $v \in V \setminus S'$ one has $U_v = \mathbf{G}(\mathcal{O}_{k_v})$ hence U_v admits a unique non-abelian simple quotient F_v (usually $F_v = \mathbf{G}^{\mathrm{ad}}(\mathcal{O}_{k_v}/\mathfrak{m}_{k_v})$). Hence we are reduced to count the number of H-conjugacy classes of surjections $\prod_{v\in V\setminus S'} F_v \longrightarrow H$. Given H there exists at most one v such that $F_v \simeq H$. Hence the result. □

Appendix A. Rigidity and finite index subgroups

The following lemma seems to be well-known, we provide a proof for completeness.

Lemma A.1. *Let Γ be a finitely generated group. The following conditions are equivalent:*

(i) *Γ is rigid.*

(ii) *there exists a subgroup Γ' of Γ of finite index which is rigid.*

(iii) *every subgroup of Γ of finite index is rigid.*

Proof. We use the results of [2] and follow its notations. In particular $A(\Gamma)$ denotes the complex proalgebraic completion of Γ; for all $n \in \mathbb{Z}^{>0}$ the group $A_n(\Gamma)$ is the quotient of $A(\Gamma)$ by the normal subgroup $K_n(\Gamma)$ intersection of kernels of all algebraic representations of $A(\Gamma)$ of degree at most n. By [2, theor.2.] the group Γ is rigid if and only if for all $n \in \mathbb{Z}^{>0}$ the proalgebraic group $A_n(\Gamma)$ is finite dimensional.

Let Γ' be a subgroup of Γ of finite index r. By [2, prop.1] the natural morphism $A(\Gamma') \longrightarrow A(\Gamma)$ is an injection and the natural map $q : \Gamma/\Gamma' \longrightarrow A(\Gamma)/A(\Gamma')$ is an isomorphism. Hence $A(\Gamma')$ is a proalgebraic subgroup of $A(\Gamma)$ of index r. By [2, cor.1] the map $A(\Gamma')^0 \longrightarrow A(\Gamma)^0$ is an isomorphism.

Let $n \in \mathbb{Z}^{>0}$. Any representation $\rho : A(\Gamma) \longrightarrow \mathbf{GL}_n(\mathbb{C})$ defines by restriction a representation $\mathrm{Res}_{A(\Gamma)}^{A(\Gamma')}\rho : A(\Gamma') \longrightarrow \mathbf{GL}_n(\mathbb{C})$. As $A(\Gamma') \hookrightarrow A(\Gamma)$ this implies that $K_n(\Gamma) \supset K_n(\Gamma')$ hence

$$A_n(\Gamma') \twoheadrightarrow A_n(\Gamma)\ . \tag{6}$$

On the other hand let $\rho : A(\Gamma') \longrightarrow \mathbf{GL}_n(\mathbb{C})$ be an n-dimensional representation of $A(\Gamma')$. The kernel of the induced algebraic representation $\mathrm{Ind}_{A(\Gamma')}^{A(\Gamma)}\rho : A(\Gamma) \longrightarrow \mathbf{GL}_{nr}(\mathbb{C})$ contains the kernel of ρ. This shows that $K_n(\Gamma')$ contains $K_{nr}(\Gamma)$. Hence $A_n(\Gamma')^0 = A(\Gamma')^0/K_n(\Gamma')^0$ is a quotient of $A(\Gamma')^0/K_{nr}(\Gamma)^0 = A(\Gamma)^0/K_{nr}(\Gamma)^0 = A_{nr}(\Gamma)^0$:

$$A_{nr}(\Gamma)^0 \twoheadrightarrow A_n(\Gamma')^0\ . \tag{7}$$

If Γ' is rigid then for any $n \in \mathbb{Z}^{>0}$ the proalgebraic group $A_n(\Gamma')$ is finite dimensional. By (6) its quotient $A_n(\Gamma)$ is finite dimensional. Hence Γ is rigid.

Conversely if Γ is rigid then for all $n \in \mathbb{Z}^{>0}$ the proalgebraic group $A_{nr}(\Gamma)^0$ is finite dimensional. By (7) its quotient $A_n(\Gamma')^0$ is finite dimensional, hence also $A_n(\Gamma')$. This shows that Γ' is rigid.

□

Appendix B. Finite groups of Lie type

We follow the conventions of [12, p.1120]. A finite group of Lie type in characteristic p is a finite group of fixed points $\mathbf{G}(\overline{\mathbb{F}_p})^F$, where:

(1) $\mathbf{G}$ is a connected simple adjoint linear algebraic group over $\overline{\mathbb{F}_p}$; we denote by Φ its root system.
(2) $F : \mathbf{G} \longrightarrow \mathbf{G}$ is a Frobenius maps (also called a Steinberg map), i.e. there exists some positive integer n such that F^n is a standard Frobenius map defining a form $\mathbf{G}_0$ of $\mathbf{G}$ over $\mathbb{F}_q$, $q = p^r$.

Lemma B.1. *Let n be a positive integer. The number of $\mathbf{GL}_n(\mathbb{F}_p)$-conjugacy classes of finite simple subgroups G of Lie type of characteristic p of $\mathbf{GL}_n(\mathbb{F}_p)$ acting semi-simply on $\mathbb{F}_p^n$ is uniformly bounded as p ranges through $\mathcal{P}$.*

Proof. It is enough to show that for each $n \in \mathbb{Z}^{>0}$ the number of $\mathbf{GL}_n(\mathbb{F}_p)$-conjugacy classes of finite simple subgroups of Lie type $G = \mathbf{G}(\overline{\mathbb{F}_p})^F$ of characteristic p of $\mathbf{GL}_n(\mathbb{F}_p)$ acting irreducibly on $\mathbb{F}_p^n$ is uniformly bounded as p ranges through $\mathcal{P}$.

Let $G = \mathbf{G}(\overline{\mathbb{F}_p})^F$ be a finite simple group of Lie type and $\rho : G \longrightarrow \mathbf{GL}_n(\mathbb{F}_p)$ an irreducible representation. As the extension $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$ is separable the representation $\rho \otimes_{\mathbb{F}_p} \overline{\mathbb{F}_p} : G \longrightarrow \mathbf{GL}_n(\overline{\mathbb{F}_p})$ is semisimple ([4, theor.7.5]):

$$\rho \otimes_{\mathbb{F}_p} \overline{\mathbb{F}_p} = \bigoplus_{i=1}^{i_\rho} \rho_i \quad , \tag{8}$$

where $1 \leq i_\rho \leq n$, $1 \leq r_{\rho_i} \leq n$ and each $\rho_i : G \longrightarrow \mathbf{GL}_{r_{\rho_i}}(\overline{\mathbb{F}_p})$ is a simple $\overline{\mathbb{F}_p}$-representation of G of degree $r_{\rho_i} \leq n$.

First notice that the number of simple groups of Lie type of characteristic p admitting a faithful irreducible representation over $\overline{\mathbb{F}_p}$ of degree at most n is bounded uniformly as p ranges through p. Hence by (8) we are reduced to showing to showing that the number of isomorphism classes of irreducible representations over $\mathbb{F}_p$ of degree at most n of a simple group of Lie type G of characteristic p is bounded independently of p. Because of the decomposition (8) it is enough to show that the number of isomorphism classes of irreducible representations over $\overline{\mathbb{F}_p}$ of degree at most n of a simple group of Lie type G of characteristic p is bounded independently of p.

By a theorem of Steinberg [26, theor. 1.3] any irreducible $\overline{\mathbb{F}_p}$-representation of G is the restriction to G of an algebraic irreducible representation of $\mathbf{G}$. Hence we have to show that the number of isomorphism classes of algebraic irreducible representations over $\overline{\mathbb{F}_p}$ of degree at most n of a connected simple adjoint linear algebraic group $\mathbf{G}$ over $\overline{\mathbb{F}_p}$ is bounded independently of p.

Such a representation is parametrized by a highest weight of $\mathbf{G}$. The dimension of such a highest weight representation is given by Weyl's character formula, which is independent of p. The result follows. □

Appendix C. On the structure of the congruence kernel $C(\Gamma)$ when it is central in $\hat{\Gamma}$

We follow the notations of section 5 and the discussion in [21, p.6].

Consider the short exact sequence of groups

$$1 \longrightarrow C(\Gamma) \longrightarrow \hat{\Gamma} \longrightarrow \overline{\Gamma} \longrightarrow 1 \quad . \tag{9}$$

Let $I = \mathbb{R}/\mathbb{Z}$. The Hochschild-Serre spectral sequence for continuous cohomology with coefficients in I yields from (9) the following exact sequence:

$$H^1_{\mathrm{ct}}(\overline{\Gamma}) \xrightarrow{\varphi} H^1_{\mathrm{ct}}(\hat{\Gamma}) \longrightarrow H^1_{\mathrm{ct}}(C(\Gamma))^{\overline{\Gamma}} \xrightarrow{\psi} H^2_{\mathrm{ct}}(\overline{\Gamma}) \quad . \tag{10}$$

Notice that the short exact sequence (9) splits over Γ. Hence

$$1 \longrightarrow \mathrm{Coker}\varphi \longrightarrow H^1_{\mathrm{ct}}(\hat{\Gamma})) \longrightarrow H^1_{\mathrm{ct}}(C(\Gamma))^{\overline{\Gamma}} \longrightarrow M(\Gamma) := \ker(H^2_{\mathrm{ct}}(\overline{\Gamma}) \longrightarrow H^2(\Gamma)) \quad . \tag{11}$$

From now on we assume that $C(\Gamma)$ is central in $\hat{\Gamma}$. In this case the group

$$H^1_{\mathrm{ct}}(C(\Gamma))^{\overline{\Gamma}} = \mathrm{Hom}_{\mathrm{ct}}(C(\Gamma), I)^{\overline{\Gamma}} = \mathrm{Hom}_{\mathrm{ct}}(C(\Gamma)/[C(\Gamma), \hat{\Gamma}], I) \tag{12}$$

is the Pontrjagin dual $PD(C(\Gamma)) := \mathrm{Hom}_{\mathrm{ct}}(C(\Gamma), I)$ of the compact abelian group $C(\Gamma)$. Hence we obtain

(13)
$$1 \longrightarrow \mathrm{Coker}(H^1_{\mathrm{ct}}(\overline{\Gamma}) \longrightarrow H^1_{\mathrm{ct}}(\hat{\Gamma})) \longrightarrow PD(C(\Gamma)) \longrightarrow M(\Gamma) := \ker(H^2_{\mathrm{ct}}(\overline{\Gamma}) \longrightarrow H^2(\Gamma)) \quad .$$

The short exact sequence (13) describes the structure of $C(\Gamma)$ in case it is central in $\hat{\Gamma}$. When Γ is S-arithmetic then one can show that $C(\Gamma)$ is central, and the cokernel on the left and the (metaplectic) kernel on the right are both finite.

References

[1] Bass H., Lubotzky A., Nonarithmetic superrigid groups: counterexamples to Platonov's conjecture, *Annals of Math.* **151** (2000), 1151-1173 3

[2] Bass H., Lubotzky A., Magid A., Mozes S., The proalgebraic completion of rigid groups, *Geom. Dedicata* **95** (2002), 19-58 2, 11

[3] Bass H., Milnor J., Serre J.P., Solution of the congruence subgroup problem for SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$, *Publ.IHES* **33** (1967), 59-137 1, 3

[4] Curtis C.W., Reiner I., Methods of representation theory, Vol.1, Wiley and Sons (1981) 12

[5] Donkin S., Invariants of several matrices, *Invent. Math.* **110** (1992) 389-401 5

[6] Grothendieck A., EGA IV_1, *Publ.IHES* **20** (1964) 6

[7] Grothendieck A., EGA IV_2, *Publ.IHES* **24** (1965) 6

[8] Grothendieck A., EGA IV_3, *Publ.IHES* **28** (1966), 59-137 6

[9] Katz N.M., Gauss sums, Kloosterman sums and monodromy groups, *Annals of Math. Studies* **116**, Princeton University Press (1988). 2, 7

[10] Lang S., Algebraic groups over finite fields, *Amer. J. Math.* **78** (1956), 555-563 6

[11] Lang S., Weil A., Number of points of varieties over finite fields, *Amer. J. Math* **76** (1954), 819-827 6

[12] Larsen M., Pink R., Finite subgroups of algebraic groups, *JAMS* **24**, 4, (2011), 1105-1158 2, 3, 7, 11

[13] Lubotzky A., Magid A., Varieties of representations of finitely generated groups, *Mem. Amer. Math. Soc.* **58** (1985), no.336 4

[14] Margulis G.A, Discrete subgroups of semisimple Lie groups, *Ergebnisse der Mathematik und ihrer Grengebiete* 17, Springer-Verlag, (1991) 1

[15] Mumford D., Fogarty J., Kirwan F., Geometric Invariant Theory, third edition, Springer Verlag (1994) 5

[16] Nakamoto K., Representation varieties and character varieties, *Publ. RIMS* **36** (2000), 159-189 2, 4, 5

[17] Nori M.V., On subgroups of $\mathbf{GL}_n(\mathbb{F}_p)$, *Invent. Math.* **88** (1987), 257-275 2, 7

[18] Pink R., Strong approximation for Zariski-dense subgroups over arbitrary global fields, *Comment. Math. Helv.* **75** (2000), 608-643 2, 10

[19] Platonov V.P., Rapinchuk A.S., ALgebraic groups and number theory, *Pure and applied Math.* **139**, Academic Press (1994) 3

[20] Platonov V.P., Rapinchuk A.S., Abstract properties of S-arithmetic groups and the congruence problem, *Russian Acad. Sci. Izv. Math.* **40** (1993)

[21] Prasad G., Rapinchuk A.S., Developments on the congruence subgroup problem after the work of Bass, Milnor and Serre, In "Collected papers of John Milnor", vol. V, AMS (2010), 307-325. 1, 3, 12

[22] Raghunathan M.S., On the congruence subgroup problem, *Publ.IHES* **46** (1976) 107-161 1, 3

[23] Shalom Y., Bounded generation and Kazhdan's property (T), *Publ.IHES* **90** (1999), 145-168

[24] Shalom Y., The algebraization of Kazhdan's property (T), International Congress of Mathematicians vol. II, p.1283-1310 (2006)

[25] Seshadri C.S., Geometric reductivity over arbitrary base, *Adv. Math.* **26** (1977), 225-274 5

[26] Steinberg R., Representations of algebraic groups, *Nagoya Math. J.* **22** (1963), 33-56 12

[27] Weisfeiler B., Strong approximation for Zariski-dense subgroups of semi-simple algebraic groups, *Annals of Math.* **120** (1984), 271-315 2, 10

Bruno Klingler
email: klingler@math.jussieu.fr
Institut de Mathématiques de Jussieu, Paris, France et Institut Universitaire de France