FINITENESS THEOREMS FOR DIMENSIONS OF IRREDUCIBLE λ-ADIC REPRESENTATIONS

by

Yuri G. Zarhin

Max–Planck–Institut
für Mathematik
Gottfried–Claren–Straße 26
D–5300 Bonn 3

Federal Republic of Germany

The USSR Academy of Sciences
Research Computing Center
Pushchino, Moscow Region
142292, USSR

USSR

MPI/89– 17

FINITENESS THEOREMS FOR DIMENSIONS OF IRREDUCIBLE λ–ADIC REPRESENTATIONS

Yuri G. Zarhin

In this paper absolutely irreducible integral λ–adic representations of the Galois groups of number fields are studied . We assume that the representations satisfy the "Weil – Riemann conjecture" with weight n and prove that their dimension is bounded above by a constant, depending only on n and the rank of the corresponding λ–adic Lie algebras . As an application we obtain that the dimension of an Abelian variety is bounded above by the rank of its endomorphism ring times a certain constant, depending only on the semisimple rank of the corresponding ℓ–adic Lie algebra .

I am deeply grateful to Yu. I. Manin , J. – P. Serre and P. Deligne for useful discussions. This paper was written during my stay in Bonn and I am very happy to be able to thank the Max–Planck–Institut für Mathematik for the hospitality.

0. Preliminaries .

Let K be a number field of finite degree over the field $\mathbf{Q}$ of rational numbers, $K(\mathrm{a})$ the algebraic closure of K and $\mathrm{G}(K) := \mathrm{Gal}(K(\mathrm{a})/K)$ the Galois group of K . If $K' \subset K(\mathrm{a})$ is a finite algebraic extension of K, then its Galois group $\mathrm{G}(K') =$ $= \mathrm{Gal}(K(\mathrm{a})/K')$ is an open subgroup of finite index in $\mathrm{G}(K)$.

Let E be a number field of finite degree over $\mathbf{Q}$ and let $\mathfrak{O} = \mathfrak{O}_{\mathrm{E}}$ be the ring of integers of E . Let λ be a non–zero prime ideal in $\mathfrak{O}$ and $l = l(\lambda)$ be the characteristic of the finite residue field $\mathfrak{O}/\lambda$. We let E_λ be the completion of E in λ and regard E_λ as a finite algebraic extension of the field $\mathbf{Q}_l$ of l–adic numbers.

0.1. **λ–adic representations.** Recall (Serre [6]) that a λ–adic representation of $G(K)$ is a continuous homomorphism

$$\rho\colon G(K) \to \mathrm{Aut}(V)$$

where V is a finite–dimensional vector space over E_λ. The dimension of ρ is the dimension $\dim(V)$ of the corresponding representation space V. The kernel $\mathrm{Ker}(\rho)$ is a closed invariant subgroup of $G(K)$. We write $K(\rho)$ for the subfield of all $\mathrm{Ker}(\rho)$–invariants in $K(a)$. Clearly, $K(\rho)$ is (possibly infinite) Galois extension of K.

To each K' corresponds the λ–adic representation

$$\rho'\colon G(K') \to \mathrm{Aut}(V)$$

which is the restriction of ρ to $G(K')$. Clearly, $\mathrm{Ker}(\rho') = \mathrm{Ker}(\rho) \cap G(K')$ and $K'(\rho')$ is the compositum $K'\,K(\rho)$ of K' and $K(\rho)$.

Since the group $\mathrm{Aut}(V)$ of all E_λ–linear automorphisms of V lies in the group $\mathrm{Aut}_{\mathbf{Q}_l}(V)$ of all $\mathbf{Q}_l$–linear automorphisms of V, it is clear that ρ also may be regarded as l–adic representation

$$\rho\colon G(K) \to \mathrm{Aut}_{\mathbf{Q}_l}(V)$$

of dimension $\dim_{\mathbf{Q}_l} V = [E_\lambda : \mathbf{Q}_l] \dim(V)$.

Recall that ρ is called absolutely irreducible if it is irreducible and the centralizer

$\mathrm{End}_{G(K)}V = E_\lambda$.

Definition. ρ *is called infinitisemally absolutely irreducible if it is absolutely irreducible and for all finite algebraic extensions* K' *of* K *the* λ*–adic representations* ρ' *of* $G(K')$ *are also absolutely irreducible.*

In order to justify this definition we need the notion of l–adic Lie algebra attached to λ–adic representation .

0.2. l–adic Lie groups and Lie algebras. Since $G(K)$ is a compact group, its image $\mathrm{Im}(\rho)$ is a closed compact subgroup of $\mathrm{Aut}(V)$.(Clearly, the compact group $\mathrm{Im}(\rho)$ is isomorphic to the profinite Galois group $\mathrm{Gal}(K(\rho)/K)$.) This implies that $\mathrm{Im}(\rho)$ is a compact Q_l–Lie subgroup of $\mathrm{Aut}(V)$ but not necessarily E_λ–Lie subgroup . We may define its Lie algebra $\mathrm{Lie}(\mathrm{Im}(\rho))$ which is a Q_l–Lie subalgebra of $\mathrm{End}(V)$ but *not necessarily* E_λ–Lie subalgebra . Clearly, $\mathrm{Im}(\rho')$ is an open subgroup of finite index in $\mathrm{Im}(\rho)$ and , therefore , $\mathrm{Lie}(\mathrm{Im}(\rho)) = \mathrm{Lie}(\mathrm{Im}(\rho'))$ for all finite algebraic extensions K' of K .

Now, one may easily check that ρ infinitisemally absolutely irreducible if and only if the natural representation of $\mathrm{Lie}(\mathrm{Im}(\rho))$ in V is "absolutely irreducible", i. e., there is no non–trivial $\mathrm{Lie}(\mathrm{Im}(\rho))$–invariant E_λ–vector subspaces in V and the centralizer of $\mathrm{Lie}(\mathrm{Im}(\rho))$ in $\mathrm{End}(V)$ coincides with E_λ .

Further, ρ always assumed to be infinitisemally absolutely irreducible . In this case one may check that $\mathrm{Lie}(\mathrm{Im}(\rho))$ is a reductive Q_l–Lie algebra and its center is a Q_l–vector subspace of $E_\lambda\,\mathrm{id}$. Here $\mathrm{id}\colon V \to V$ is the identity map. Indeed, let B be a non–zero $\mathrm{Lie}(\mathrm{Im}(\rho))$–invariant Q_l–vector subspace of V such that the natural representation of $\mathrm{Lie}(\mathrm{Im}(\rho))$ in B is irreducible . Clearly,

$$V = \Sigma\, eB \quad (e \in E_\lambda) .$$

and the simple $\mathrm{Lie}(\mathrm{Im}(\rho))$–module eB is isomorphic to B for all $e \in E_\lambda \setminus \{0\}$. This implies that the representation of $\mathrm{Lie}(\mathrm{Im}(\rho))$ in the $\mathbf{Q}_l$–vector space V is isomorphic to the quotient of the direct sum of $[E_\lambda : \mathbf{Q}_l]$ copies of the simple $\mathrm{Lie}(\mathrm{Im}(\rho))$–module B . This implies , in turn , that the $\mathbf{Q}_l$–vector space V is also isotype representation of $\mathrm{Lie}(\mathrm{Im}(\rho))$. In particular, it is semisimple and , therefore , $\mathrm{Lie}(\mathrm{Im}(\rho))$ is reductive .

Since it is more convenient to work with E_λ–Lie algebras, let us define $E_\lambda\, \mathrm{Lie}(\mathrm{Im}(\rho))$ as the E_λ–Lie subalgebra of $\mathrm{End}(V)$ spanned by $\mathrm{Lie}(\mathrm{Im}(\rho))$. Clearly, the natural representation of $E_\lambda\, \mathrm{Lie}(\mathrm{Im}(\rho))$ in V is faithful and absolutely irreducible . In particular, $E_\lambda\, \mathrm{Lie}(\mathrm{Im}(\rho))$ is a reductive E_λ–Lie algebra . Let us split $E_\lambda\, \mathrm{Lie}(\mathrm{Im}(\rho))$ into the direct sum

$$E_\lambda\, \mathrm{Lie}(\mathrm{Im}(\rho)) = \mathfrak{c} \oplus \mathfrak{g}_\rho$$

of its center $\mathfrak{c}$ and a semisimple E_λ–Lie algebra $\mathfrak{g}_\rho$. The absolute irreducibility implies that either $\mathfrak{c} = \{0\}$ or $\mathfrak{c} = E_\lambda\, \mathrm{id}$. In both cases the natural representation of $\mathfrak{g}_\rho$ in V is absolutely irreducible . In addition , $E_\lambda\, \mathrm{Lie}(\mathrm{Im}(\rho))$ is an algebraic E_λ–Lie subalgebra of $\mathrm{End}(V)$.

0.3. Ranks of semisimple Lie algebras . Let r be the rank of the semisimple E_λ–Lie algebra $\mathfrak{g}_\rho$. Clearly, r does not exceed the rank r' of the semisimple part of the reductive $\mathbf{Q}_l$–Lie algebra $\mathrm{Lie}(\mathrm{Im}(\rho))$. Notice, that if $r = 0$, then $\mathfrak{g}_\rho = \{0\}$ and the absolute irreducibility of the $\mathfrak{g}_\rho$–module V implies that

$\dim(V) = 1$. Further, we will assume that $\mathfrak{g}_\rho \neq \{0\}$, i. e., $r > 0$. The aim of this paper is to give upper bounds for $\dim(V)$ in terms of r for certain class of λ–adic representations described in the next subsection.

0.4. Integral λ–adic representations of weight n . Let us fix a positive integer n .

Definition. λ–adic representation ρ is called E–integral of weight n if for all but finitely many places v of K the following conditions hold:

a) ρ is unramified at v ;

b) let $\mathrm{Fr}_v \in \mathrm{Im}(\rho)$ be a Frobenius element attached to v (defined up to conjugacy [6,5]) and let

$P_v(t) = \det(1 - t\,\mathrm{Fr}_v^{-1}, V)$ be its characteristic poynomial.

Then all the coefficients of P_v lie in E and even in $\mathfrak{O}$.

c) (the Weil – Riemann conjecture). All (complex) reciprocal roots of P_v and their conjugate over $\mathbf{Q}$ have absolute value $q(v)^{n/2}$ where $q(v)$ is the number of elements of the residue field $k(v)$ at v .

Clearly, if ρ is E–integral of weight n , then ρ' are also E–integral of weight n for all finite algebraic extensions K' of K .

Remark. The Weil – Riemann conjecture easily implies that $\mathrm{Lie}(\mathrm{Im}(\rho))$ is not semisimple, i. e. $E_\lambda \mathrm{Lie}(\mathrm{Im}(\rho)) = E_\lambda \mathrm{id} \oplus \mathfrak{g}_\rho$ .Indeed , the determinant $\det(\mathrm{Fr}_v^{-1}, V)$ of Fr_v^{-1} is an algebraic integer $\in E_\lambda^*$, which is not a root of 1 , since its (any) archimedean absolute value is equal to $q(v)^{n \dim(V)/2} \neq 1$. Notice that $\det(\mathrm{Fr}_v^{-1}, V)$ is a λ–adic unit , because the image of the determinant map $\mathrm{Im}(\rho) \to E_\lambda^*$ oughts to be a compact subgroup . On the other hand, the logarithm map

$\log\colon \mathrm{Im}(\rho) \to \mathrm{Lie}(\mathrm{Im}(\rho))$

for the compact l–adic Lie group $\mathrm{Im}(\rho)$ is also defined [1] . One may easily check that

$\mathrm{tr}\,(\log u) = \log\,(\det(u\,,\,\mathrm{V})\,) \in \mathrm{E}_\lambda$ for all $u \in \mathrm{Im}(\rho) \subset \mathrm{Aut}(\mathrm{V})$.

Here $\mathrm{tr}\colon \mathrm{End}(\mathrm{V}) \to \in \mathrm{E}_\lambda$ is the trace map . Now, if we put

$\mathrm{fr}_{\mathrm{v}} = \log\,(\mathrm{Fr}_{\mathrm{v}}^{-1}) = -\log(\mathrm{Fr}_{\mathrm{v}})$, then

$\mathrm{tr}(\mathrm{fr}_{\mathrm{v}}) = \log\,(\det(\mathrm{Fr}_{\mathrm{v}}^{-1}, \mathrm{V}) \neq 0$,

i. e. $\mathrm{Lie}(\mathrm{Im}(\rho))$ contains an operator with non–zero trace .(Henniart [4] even proved that $\mathrm{Lie}(\mathrm{Im}(\rho))$ contains scalar operators $\mathbf{Q}_l\,\mathrm{id}$.)

Our main result is the following assertion .

0.5. **Main theorem** . *There exists an absolute constant* $D = D(r,n)$, *depending only on* n *and* r, *enjoying the following properties*:

Let $\rho\colon \mathrm{G}(K) \to \mathrm{Aut}(\mathrm{V})$ *be infinitisemally absolutely irreducible* E–*integral* λ–*adic representation of weight* n . *If the rank of the semisimple* E_λ–*Lie algebra* $\mathfrak{g}_\rho$ *is equal to* r *then* $\dim(\mathrm{V}) < D(r,n)$.

Remark . For $r = 0$ one may put $D(0,n) = 1$ (see Sect. 0.3).

Corollary of Theorem 0.5. *Let* $\rho\colon \mathrm{G}(K) \to \mathrm{Aut}(\mathrm{V})$ *be infinitisemally absolutely irreducible* E–*integral* λ–*adic representation of weight* n . *Let* r' *be the rank of the semisimple part of the reductive* $\mathbf{Q}_l$–*Lie algebra* $\mathrm{Lie}(\mathrm{Im}(\rho))$. *Then* $\dim(\mathrm{V}) < \max\,\{D(j,n)\,,\, 0 \leq j \leq r'\,\}$.

Indeed, one has only to recall that $r \leq r'$ (Sect. 0.3) and apply Theorem 0.5.

0.6. **Remark** . Let C be the algebraic closure of E_λ (= algebraic closure of. $\mathbf{Q}_l$)). Let us put

$W := V \otimes_{E_\lambda} C$, $\mathfrak{g} := \mathfrak{g}_\rho \otimes_{E_\lambda} C \subset \mathrm{End}_C W$

and consider the simple module W over the semisimle C–Lie algebra $\mathfrak{g}$ of rank r. In order to prove Theorem 0.5 it suffices to prove that there exists a positive constant D', depending only on r and n, and such that the highest weight of the simple $\mathfrak{g}$–module W is a sum of no more than D' fundamental weights. Let us split $\mathfrak{g}$ into the direct sum

$$\mathfrak{g} = \oplus\, \mathfrak{g}_i \ (1 \le i \le s)$$

of simple C–Lie algebras $\mathfrak{g}_i$. Clearly, $s \le r$ and the rank of each $\mathfrak{g}_i$ does not exceed r. Then one may decompose W into the tensor product $W = \otimes\, W_i$ of simple $\mathfrak{g}_i$–modules $W_i\,(1 \le i \le s)$.

So, in order to prove Theorem 0.5 it suffices to prove that there exists a positive constant D'', depending only on n and r, and such that for all i the highest weight of the simple $\mathfrak{g}_i$–module W_i is a sum of no more than D'' fundamental weights.

0.7. Key lemma. *Let*

$f \in E_\lambda \mathrm{Lie}(\mathrm{Im}(\rho)) = E_\lambda \mathrm{id} \oplus \mathfrak{g}_\rho \subset \mathrm{End}(V)$

be a regular element of the reductive E_λ*–Lie algebra* $E_\lambda\mathrm{Lie}(\mathrm{Im}(\rho))$. *Since* $\mathrm{End}(V) \subset \mathrm{End}_C(W)$, *one may view* f *as a* C*–linear operator in* W. *Let* $\mathrm{spec}(f) \subset C$ *be the set of all eigen values of* $f: W \to W$. *Let* $Q(f)$ *be the* Q*–vector subspace of* C, *spanned by* $\mathrm{spec}(f)$. *Let us assume that there exists a finite set* A *of rational numbers and a finite set* M *of* Q*–linear maps* $\theta: Q(f) \to Q$, *enjoying the following properties:*

1) $\theta(\mathrm{spec}(f)) \subset A$ *for all* $\theta \subset M$;

2) *the map* $Q(f) \to Q^M$, $a \to \{\theta(a)\}_{\theta \in M}$ *is an embedding.*

Then for all i *(with* $1 \le i \le s$*) the highest weight of the simple* $\mathfrak{g}_i$*–module* W_i *is a sum of no more than* $[\mathrm{card}(A)-1]$ *fundamental weights.*

Here card(A) *is the number of elements of* A .

We will prove Key Lemma in Section 2 .

So, in order to prove Theorem 0.5 it suffices to prove the existence of such f, A and M with A , depending *only* on r and n .

1. Proof of Main theorem.

Our proof consists of the following steps..

Step 1. Replacing ,if necesary , K by its suitable finite algebraic extension K' and ρ by ρ', we may and will assume that K enjoys the following properties:

1) K is a Galois extension of $\mathbf{Q}$;

2) K contains a subfield, isomorphic to E .

Let us fix a prime number p and a place v of K, enjoying the following properties:

3) p is unramified in K , v lies above p and the residue field $k(\mathrm{v})$ at v coincides with the finite prime field $\mathbf{Z}/p\mathbf{Z}$.;

4) ρ is unramified at v and the characteristic polynomial $\mathrm{P_v(t)}$ of the corresponding Frobenius element $\mathrm{Fr_v}$ lies in $1 + \mathrm{t}\,\mathcal{O}[\mathrm{t}]$ and satisfies the Weil–Riemann conjecture with weight n ;

5) all the eigen values of $\mathrm{Fr_v}^{-1}$ are congruent to 1 modulo ℓ^2 and the ℓ-adic logarithm $\mathrm{fr_v} := \log(\mathrm{Fr_v}^{-1}) = -\log(\mathrm{Fr_v})$ is a regular element of the reductive $\mathbf{Q}_\ell$-Lie algebra Lie(Im(ρ)) (use Chebotarev density theorem).

The regularity condition implies that $\mathrm{fr_v}$ is a semisimple endomorphism of the $\mathbf{Q}_\ell$-vector space V and, therefore, is a semisimple endomorphism of the E_λ–vector space V . Clearly, $\mathrm{fr_v}$ is also regular in the reductive reductive E_λ–Lie algebra $\mathrm{Lie}(\mathrm{Im}(\rho)) \otimes_{\mathbf{Q}_l} E_\lambda$. Since $E_\lambda \mathrm{Lie}(\mathrm{Im}(\rho))$ is isomorphic to the quotient of $\mathrm{Lie}(\mathrm{Im}(\rho)) \otimes_{\mathbf{Q}_l} E_\lambda$, fr_v is also regular in $E_\lambda \mathrm{Lie}(\mathrm{Im}(\rho))$.

Step 2 . Let us fix an embedding of E in K . Now we may and will assume that E is a subfield of K . Since K is a Galois extension of Q, the condition 3 of Step 1 implies that p splits completely in K . Since E is a subfield of K , p also splits completely in E .

Recall that C is the algebraic closure of E_λ . Let L be the subfield of C obtained by adjunction to E of the set R of all eigenvalues of $\mathrm{Fr}_{v'}^{-1}$. Clearly, it is a finite Galois extension of E and all elements of R are algebraic integers . For each embedding of L into the field C of complex numbers all elements of R have absolute value $p^{n/2}$. Let us denote by Γ the multiplicative subgroup of L^* generated by R . Since all elements of R are congruent to 1 modulo l^2, Γ does not contain roots of 1 different from 1. So, Γ is a finitely generated free abelian group . I claim that the rank $\mathrm{rk}(\Gamma)$ of Γ does not exceed $r+1$. Indeed, the l–adic logarithm maps R into the set $\mathrm{spec}(\mathrm{fr}_v)$ of all eigen values of the C–linear operator $\mathrm{fr}_v: W \to W$, and , therefore, defines an isomorphism between Γ and the additive subgroup $\mathbf{Z}(\mathrm{fr}_v)$ of C , generated by $\mathrm{spec}(\mathrm{fr}_v)$. Let me recall that fr_v is a semisimple element of $E_\lambda \mathrm{id} \oplus \mathfrak{g}_\rho \subset C\,\mathrm{id}_W \oplus \mathfrak{g}$ where $\mathrm{id}_W: W \to W$ is the identity map and $\mathfrak{g}$ is the semisimple $C-$Lie subalgebra of $\mathrm{End}(W)$, having the rank r . Now, E. Cartan theory of modules with highest weight [2] easily implies that the additive subgroup, generated by all eigen values of each operator from $\mathfrak{g}$, has the rank $\leq r$. Since fr_v is the sum of a scalar operator and an operator from $\mathfrak{g}$, the rank of $\mathbf{Z}(\mathrm{fr}_v)$ does not exceed $r+1$.

Notice,that the Galois group Gal(L/E) acts naturally on Γ . This action defines an embedding

$$\mathrm{Gal}(L/E) \to \mathrm{Aut}(\Gamma) \approx \mathrm{GL}(\mathrm{rk}(\Gamma),\mathbf{Z}) \subset \mathrm{GL}(r+1, \mathbf{Z}) .$$

Since Gal(L/E) is finite, it is isomorphic to a finite subgroup of GL(r+1,Z). Applying a theorem of Jordan we obtain that there exists a positive constant $D_1 = D_1(r)$, depending only on r, such that the order of Gal(L/E) divides D_1 , i. e. the extension degree [L:E] divides D_1 .

Step 3 . Let $\mathfrak{O}_L$ be the ring of integers in L . Conditions 3 and 4 of Step 1 imply that all elements α of R are algebraic integers in L and for each embedding of L into **C** we have

$$\alpha'\alpha = p^n .$$

Here α' is the complex–conjugate of α and, of course, also, an algebraic integer . This implies that if p' is a prime ideal in $\mathfrak{O}_L$, not lying above p, then α is a p'–adic unit for all $\alpha \in R$. Notice, that $\alpha' = p^n/\alpha$ lies in L and even in $\mathfrak{O}_L$.

Let S be the set of prime ideals in $\mathfrak{O}_L$, lying above p . For each p from S let

$$\mathrm{ord}_{\mathfrak{p}} : L^* \to \mathbf{Q}$$

be the discrete valuation of L attached to p and normalized by the condition

$$\mathrm{ord}_{\mathfrak{p}}(p) = 1 .$$

Recall that p completely splits in E . This implies that

$$\mathrm{ord}_{\mathfrak{p}}(E^*) = \mathrm{ord}_{\mathfrak{p}}(\mathbf{Q}^*) = \mathbf{Z} ,$$

$$n = \mathrm{ord}_{\mathfrak{p}}(p^n) = \mathrm{ord}_{\mathfrak{p}}(\alpha) + \mathrm{ord}_{\mathfrak{p}}(\alpha') \text{ for all } \alpha \in R .$$

Since α , α' are algebraic integers, the rational numbers $\mathrm{ord}_{\mathfrak{p}}(\alpha)$, $\mathrm{ord}_{\mathfrak{p}}(\alpha')$ are non–negative, and, therefore,

$0 \leq \mathrm{ord}_{\mathrm{p}}(\alpha) \leq n$ for all $\alpha \in R$.

Since [L:Q] divides D_1,

$\mathrm{ord}_{\mathrm{p}}(\mathrm{L}^*) \subset (1/D_1)\, \mathrm{ord}_{\mathrm{p}}(\mathrm{E}^*) = (1/D_1)\, \mathbf{Z}$.

Let us put $A := \{c \in \mathbf{Q}, 0 \leq c \leq n, D_1\, c \in \mathbf{Z}\}$. Clearly, A is a finite set of rational numbers, consisting of $(D_1 n + 1)$ elements and depending only on n and r. We have

$\mathrm{ord}_{\mathrm{p}}(\alpha) \in A$ for all $\alpha \in R$, $\mathrm{p} \in S$.

Let ord: $\Gamma \to \mathbf{Q}^S$ be the homomorphism defined by the formula

$\mathrm{ord}(\gamma) = \{\mathrm{ord}_{\mathrm{p}}(\gamma)\}_{\mathrm{p} \in S}$.

Clearly, $\mathrm{ord}(R) \subset A^S \subset \mathbf{Q}^S$.

I claim that ord is an embedding. Indeed, if $\mathrm{ord}(\gamma) = 0$ for some $\gamma \in \Gamma$ then γ is an unit in L. The Weil – Riemann conjecture implies the equality of all archimedean valuations on the elements of Γ. Therefore, the product formula implies that $|\gamma| = 1$ for all archimedean valuations on L. This implies that γ is a root of 1. Since Γ does not contain non–trivial roots of 1, $\gamma = 1$.

One may extend ord by Q–linearity to an embedding

$\Gamma \otimes \mathbf{Q} \to \mathbf{Q}^S$,

which we will also denote by ord.

Step 4. Let $\mathbf{Q}(\mathrm{fr}_{\mathrm{v}})$ be the Q–vector subspace of C, spanned by $\mathrm{spec}(\mathrm{fr}_{\mathrm{v}})$. We have

$\mathrm{spec}(\mathrm{fr}_{\mathrm{v}}) \subset \mathbf{Z}(\mathrm{fr}_{\mathrm{v}}) \subset \mathbf{Q}(\mathrm{fr}_{\mathrm{v}})$.

The l–adic logarithm defines the isomorphism

$\log: \Gamma \to \mathbf{Z}(\mathrm{fr}_{\mathrm{v}})$,

which can be extended by Q–linearity to an isomorphism

$\Gamma \otimes \mathbf{Q} \to \mathbf{Q}(\mathrm{fr}_{\mathrm{v}})$, which we will also denote by log . Clearly, the $\mathbf{Q}$–vector space $\mathrm{Hom}(\mathbf{Q}(\mathrm{fr}_v),\mathbf{Q})$ is generated by maps

$\mathrm{ord}_p \log^{-1} : \mathbf{Q}(\mathrm{fr}_v) \to \Gamma \otimes \mathbf{Q} \to \mathbf{Q} \quad (p \in S)$.

Notice, that

$\mathrm{ord}_p \log^{-1}(\mathrm{spec}(\mathrm{fr}_v)) = \mathrm{ord}_p(R) \subset A$ for all $p \in S$.

Now, I claim that the highest weight of each simple $\mathfrak{g}_i$–module W_i is the sum of no more than $n\,D_1$ fundamental weights. Indeed, one has only to apply Lemma 0.7 to the regular element $f = \mathrm{fr}_v$, the set

$M = \{ \mathrm{ord}_p \log^{-1}(\mathrm{spec}(\mathrm{fr}_v)) : \mathbf{Q}(\mathrm{fr}_v) \to \mathbf{Q} \mid p \in S \}$

of homomorphisms $\mathbf{Q}(\mathrm{fr}_v) \to \mathbf{Q}$ and A .

2. Proof of Key Lemma .

We start the proof with the following remarks. First, we have natural embeddings

$E_\lambda \mathrm{id} \otimes \mathfrak{g}_\rho \subset (E_\lambda \mathrm{id} \otimes \mathfrak{g}_\rho) \otimes_{E_\lambda} C = C\,\mathrm{id}_W \oplus \mathfrak{g} \subset \mathrm{End}_C W$.

Since f is regular in the reductive E_λ–Lie algebra $E_\lambda \mathrm{id} \otimes \mathfrak{g}_\rho$, it remains regular in the reductive C–Lie algebra $C\,\mathrm{id}_W \oplus \mathfrak{g}$. We have

$$f = c\,\mathrm{id} + \Sigma f_i \ \ (1 \le i \le s)$$

with $c \in C$, $f_i \in \mathfrak{g}_i$. Since f is regular, all f_i are non–zero semisimple elements of $\mathfrak{g}_i$. Let $\mathrm{spec}(f_i) \subset C$ be the set of all eigen values of the C–linear operator $f_i\colon W_i \to W_i$ (recall that W_i is the faithful simple $\mathfrak{g}_i$–module) . If $\alpha \in \mathrm{spec}(f_i)$ then we write $\mathrm{mult}_i(\alpha)$ for the multiplicity of the eigen value α of the operator f_i . Clearly ,

$$\Sigma_{\alpha \in \mathrm{spec}(f_i)} \mathrm{mult}_i(\alpha) = \dim(W_i) .$$

Since $\mathfrak{g}_i$ is the (semi)simple subalgebra of $\mathrm{End}(W_i)$, the trace

$$\mathrm{tr}(f_i, W_i) := \Sigma_{\alpha \in \mathrm{spec}(f_i)} \mathrm{mult}_i(\alpha)\, \alpha = 0 .$$

We have

$$\mathrm{spec}(f) = c + \Sigma_i \mathrm{spec}(f_i) =$$
$$= \{ c + \Sigma_i \alpha_i \mid \alpha_i \in \mathrm{spec}(f_i) , 1 \le i \le s \} .$$

Claim . *For all i there exists $c_i \in \mathbf{Q}(f)$ such that*

$\mathrm{spec}(f_i) \subset c_i + \mathrm{spec}(f)$.

In particular, $\mathrm{spec}(f_i) \subset \mathbf{Q}(f)$.

We will prove Claim at the end of this Section .

Proof of Key Lemma (modulo Claim) . We will identify $\mathfrak{g}_i$ with its image in $\mathrm{End}(W_i)$. Let $\mathbf{Q}(f_i)$ be the $\mathbf{Q}$–vector subspace of C spanned by $\mathrm{spec}(f_i)$. Clearly , $\mathbf{Q}(f_i) \subset \mathbf{Q}(f)$. To each homomorphism $\varphi: \mathbf{Q}(f_i) \to C$ corresponds a C–linear operator $f_i^{(\varphi)}: W_i \to W_i$ called a *replica* of f and defined as follows [10].

Each eigen vector $x \in W_i$ of f is also an eigen vector of $f_i^{(\varphi)}$ and $f_i^{(\varphi)}x = \varphi(\alpha)x$ if $fx = \alpha x$ ($\alpha \in \mathrm{spec}(f_i) \subset \mathbf{Q}(f_i)$).

Clearly , the set $\mathrm{spec}(f_i^{(\varphi)})$ of the all eigen values of $f_i^{(\varphi)}$ coincides with $\varphi(\mathrm{spec}(f_i))$.

Since $\mathfrak{g}_i$ is simple , it is an algebraic Lie subalgebra of $\mathrm{End}(W_i)$ and,therefore , contains all the replicas of their elements [10] . This implies that

$$f_i^{(\varphi)} \in \mathfrak{g}_i \subset \mathrm{End}(W_i)$$

for all φ . Clearly , $f_i^{(\varphi)}$ is a semisimple element of $\mathfrak{g}_i$.

Since $\mathbf{Q}(f_i) \subset \mathbf{Q}(f)$, one may attach to each homomorphism $\psi : \mathbf{Q}(f) \to C$ its restriction $\psi': \mathbf{Q}(f_i) \to C$ and consider the corresponding replica

$$f_i^{(\psi')} \in \mathfrak{g}_i \subset \mathrm{End}(W_i)\ .$$

Clearly, $f_i^{(\psi')} \neq 0$ if and only if the restriction of ψ to $\mathbf{Q}(f_i)$ does not vanish identically . We have

$$\mathrm{spec}(f_i^{(\psi')}) = \psi'(\mathrm{spec}(f_i)) = \psi(\mathrm{spec}(f_i)) \subset \psi(c_i + \mathrm{spec}(f)\ ) =$$

$$= \psi(c_i) + \psi(\mathrm{spec}(f)) = \{\psi(c_i) + \psi(\alpha)\ ,\ \alpha \in \mathrm{spec}(f)\ \}$$

Now, let us choose a homomorphism θ: $\mathbf{Q}(f) \to \mathbf{Q} \subset C$ such that $\theta \in M$ and the restriction of θ to $\mathbf{Q}(f_i)$ does not vanish identically . Then

$$f_i^{(\theta')} \in \mathfrak{g}_i \subset \mathrm{End}(W_i)$$

is a non–zero semisimple operator and

$$\mathrm{spec}(f_i^{(\theta')}) \subset \theta(c_i) + \theta(\mathrm{spec}(f)) \subset \theta(c_i) + A\ .$$

In particular, $f_i^{(\theta')}$ has , at most, card(A) different eigen values .

Let me recall that if a linear irreducible simple Lie algebra contains a non–zero semisimple operator with exactly m different eigen values , then the highest weight of the corresponding irreducible representation is the sum of no more than $(m-1)$ fundamental weights ([11] , Th. 2.2) .

Applying this assertion to a non–zero semisimple element $f_i^{(\theta')}$ of linear irreducible simple Lie algebra $\mathfrak{g}_i \subset \mathrm{End}(W_i)$ we obtain that the highest weight of the simple $\mathfrak{g}_i$–module W_i is the sum of no more than [card(A)–1] fundamental weights .QED.

Proof of Claim . First let us assume that $s = 1$, i. e. , $\mathfrak{g} = \mathfrak{g}_1$ is simple and $W = W_1$. Then $f_1 = f - c\,\mathrm{id}_W \in \mathfrak{g}_1$ and

$$c = \mathrm{tr}(f, W)/\dim(W)$$

where $\mathrm{tr}(f, W)$ is the trace of f: $W \to W$. This implies that $c \in \mathbf{Q}(f)$ and

$$\mathrm{spec}(f_1) = (-c) + \mathrm{spec}(f)\ .$$

One has only to put $c_1 = -c$.

Now, let us assume that $s > 1$. For each j let us choose an eigen value $\beta_j \in \mathrm{spec}(f_j)$ $(1 \le j \le s)$. Then for each $\alpha \in \mathrm{spec}(f_i)$

$$c + \alpha + \Sigma_{j \neq i} \beta_j \in \mathrm{spec}(f).$$

So, if we put $c_i = -(c + \Sigma_{j \neq i} \beta_j)$, then $\alpha \in c_i + \mathrm{spec}(f)$, i.e.

$$\mathrm{spec}(f_i) \subset c_i + \mathrm{spec}(f).$$

One has only to check that $c_i \in \mathbf{Q}(f)$. But we may write the following explicit formula (recall that the trace of f_i vanishes and the sum of multiplicities of all eigen values of f_i is equal to $\dim(W_i)$).

$$c_i = -\left(\Sigma_{\alpha \in \mathrm{spec}(f_i)} \mathrm{mult}_i(\alpha)\, (c + \alpha + \Sigma_{j \neq i} \beta_j) \right) / \dim(W_i).$$

This formula implies that c_i is a linear combination of eigen values $c + \alpha + \Sigma_{j \neq i} \beta_j$ of f with rational coefficients, i. e. $c_i \in \mathbf{Q}(f)$. QED.

3. Applications to Abelian varieties.

Let X be an Abelian variety defined over K. Let $\mathrm{T}_l(X)$ be the Tate $\mathbf{Z}_l$–module of X and

$$\mathrm{V}_l(X) = \mathrm{T}_l(X) \otimes_{\mathbf{Z}_l} \mathbf{Q}_l.$$

It is well–known that $\mathrm{V}_l(X)$ is the $\mathbf{Q}_l$–vector space of dimension $2 \dim X$. There is a natural l–adic representation [6 ,5]

$$\rho_l : \mathrm{G}(K) \to \mathrm{Aut}\, \mathrm{V}_l(X).$$

A theorem of Faltings [3] asserts that ρ_l is semisimple and the centralizer of $\mathrm{G}(K)$ in $\mathrm{End}\, \mathrm{V}_l(X)$ coincides with $\mathrm{End}_K X \otimes \mathbf{Q}_l$. Here $\mathrm{End}_K X$ is the ring of all K–endomorphisms of X. This implies that the $\mathbf{Q}_l$–Lie algebra $\mathrm{Lie}(\mathrm{Im}(\rho_l)$ is reductive, its natural representation in $\mathrm{V}_l(X)$ is semisimple and the centralizer of $\mathrm{Lie}(\mathrm{Im}(\rho_l))$ in $\mathrm{End}\, \mathrm{V}_l(X)$ coincides with $\mathrm{End}\, X \otimes \mathbf{Q}_l$ Here $\mathrm{End}\, X$ is the ring of all endomorphisms of X (over $K(\mathrm{a})$). Recall that the ring End X is a free abelian group of finite rank . We write rk(End X) for the rank of End X .

Let us split the reductive $\mathbf{Q}_l$– Lie algebra Lie(Im(ρ_l)) into the direct sum

$$\mathrm{Lie}(\mathrm{Im}(\rho_l)) = \mathfrak{c}_l \oplus \mathfrak{g}_l$$

of its center $\mathfrak{c}_l$ and a semisimple $\mathbf{Q}_l$– Lie algebra $\mathfrak{g}_l$. Let $r(X)$ be the rank of $\mathfrak{g}_l$. The results of [7] combined with the theorem of Faltings imply that $r(X)$ does not depend on l .

3.1. Theorem . *Let us put*

$$H = H(r(X)) = \max\{D(j,1)\ ,\ 0 \le j \le r(X)\}$$

where D *are as in Theorem 0.5 . Then*

$$\dim(X) \le H\,\mathrm{rk}(\mathrm{End}\ X)/2\ .$$

In particular , the dimension of X is bounded above by rk(End X) times certain constant , depending only on $r(X)$.

Example. If $r(X) = 0$ then X is of **CM**–type and

$\dim X \le \mathrm{rk}(\mathrm{End}\ X)/2$.

Remark. If $r(X) = 1$ then results of [9] imply that

$\dim X \le \mathrm{rk}(\mathrm{End}\ X)$.

Remark . One may deduce from several conjectures [8](e. g., the conjecture of Mumford – Tate or a conjecture of Serre [12]) that $\dim X$ does not exceed $2^{r(X)-1}\,\mathrm{rk}(\mathrm{End}\ X)$.

3.2. Proof of Theorem 3.1. In the course of the proof we may and will assume that all endomorphisms of X are defined over K and X is absolutely simple . Then $\mathrm{End}^\circ X = \mathrm{End}\ X \otimes \mathbf{Q}$ is a division algebra of finite dimension over $\mathbf{Q}$. Let us fix a maximal commutative $\mathbf{Q}$–subalgebra E in $\mathrm{End}^{\circ}X$. Then E is a number field, coinciding with its centralizer in $\mathrm{End}^{\circ}X$; the degree [E:Q] divides rk(End X) . In particular,

$$[\mathrm{E}:\mathbf{Q}] \leq \mathrm{rk}(\mathrm{End}\ X) .$$

In addition , [E:Q] divides 2 dim X and the natural embedding

$$\mathrm{E} \otimes_{\mathbf{Q}} \mathbf{Q}_l \to \mathrm{End}^{\circ}X \otimes_{\mathbf{Q}} \mathbf{Q}_l = \mathrm{End}\ X \otimes \mathbf{Q}_l \subset \mathrm{End}\ V_l(X)$$

provides $V_l(X)$ with the structure of a free $\mathrm{E} \otimes_{\mathbf{Q}} \mathbf{Q}_l$–module of rank 2 dim X /[E:Q] [5] .

Let $\mathfrak{O}$ be the ring of integers in E . There is a natural splitting

$$\mathrm{E} \otimes_{\mathbf{Q}} \mathbf{Q}_l = \oplus\, \mathrm{E}_{\lambda}$$

where λ runs through the set of dividing l prime ideals in $\mathfrak{O}$. Clearly,

$$[\mathrm{E}:\mathbf{Q}] = \Sigma\, [[\mathrm{E}_{\lambda}:\mathbf{Q}_l] .$$

Since $V_l(X)$ is the free $\mathrm{E} \otimes_{\mathbf{Q}} \mathbf{Q}_l$–module of rank 2 dim X /[E:Q] , there is a natural splitting

$$V_l(X) = \oplus\, V_{\lambda}$$

where $V_{\lambda} = \mathrm{E}_{\lambda} V_l(X)$ is the E_{λ}–vector space of dimension 2 dim X/[E:Q] . Clearly, each V_{λ} is $G(K)$–invariant and ρ_l is the direct sum of the corresponding λ–adic representations

$$\rho_{\lambda} : G(K) \to \mathrm{Aut}_{\mathrm{E}_{\lambda}} V_{\lambda} .$$

One may easily check , using the theorem of Faltings, that each ρ_{λ} is absolutely irreducible and even infinitisemally absolutely irreducible λ–adic representation (see [9], Sect. 0.11.1) .

Let us split the reductive $\mathbf{Q}_l$– Lie algebra $\mathrm{Lie}(\mathrm{Im}(\rho_{\lambda})$ into the direct sum

$$\mathrm{Lie}(\mathrm{Im}(\rho_{\lambda}) = \mathfrak{c}_{\lambda} \oplus \mathfrak{g}_{\lambda}$$

of its center $\mathfrak{c}_{\lambda}$ and a semisimple $\mathbf{Q}_l$– Lie algebra $\mathfrak{g}_{\lambda}$. Let r_{λ}' be the rank of $\mathfrak{g}_\lambda$.

Claim . $r_\lambda' \le r(X)$.

In order to prove this inequality it suffices to construct a surjective homomorphism $\mathfrak{g}_l \to \mathfrak{g}_\lambda$ of semisimple $\mathbf{Q}_\ell$– Lie algebras . In turn, in order to construct such a homomorphism it suffices to construct a surjective homomorphism

$$\mathfrak{c}_l \oplus \mathfrak{g}_l = \mathrm{Lie}(\mathrm{Im}(\rho_l)) \to \mathfrak{c}_\lambda \oplus \mathfrak{g}_\lambda = \mathrm{Lie}(\mathrm{Im}(\rho_\lambda))$$

of reductive $\mathbf{Q}_\ell$– Lie algebras and take its restriction to $\mathfrak{g}_l$. But it is very easy to constuct the latter homomorphism . One has only to consider the surjective homomorphism $\mathrm{Im}(\rho_l) \to \mathrm{Im}(\rho_\lambda)$ of $\mathbf{Q}_\ell$– Lie groups, induced by the projection map $V_l(X) \to V_\lambda$, and take the corresponding homomorphism of the $\mathbf{Q}_\ell$– Lie algebras .

It is well known [6,5] that for all but finitely many places v of K the following conditions hold:

1) ρ is unramified at v ;

2) the characteristic polynomial

$$\det(t\ \mathrm{id} - \mathrm{Fr}_v , V_\lambda)$$

lies in $\mathcal{O}[t]$; all its (complex) roots and their conjugate over $\mathbf{Q}$ have absolute value $q(v)^{1/2}$ (a theorem of A. Weil) .

In order to obtain E–integral λ–adic representation of weight 1 let us consider the dual E_λ–vector space

$$V_\lambda^* = \mathrm{Hom}_{E_\lambda}(V_\lambda , E_\lambda)$$

and the isomorphism

$$\tau\colon \mathrm{Aut}_{E_\lambda}(V_\lambda) \to \mathrm{Aut}_{E_\lambda}(V_\lambda^*)$$

defined by the formula $\tau(u) = (u^*)^{-1}$ where u^* is the adjoint of u .

Clearly, $\dim_{E_\lambda} V_\lambda = \dim_{E_\lambda} V_\lambda^*$.

Let us consider the dual λ–adic representation

$$\rho_\lambda^* = \tau\rho_\lambda : G(K) \to \mathrm{Aut}_{E_\lambda}(V_\lambda) \to \mathrm{Aut}_{E_\lambda}(V_\lambda^*) .$$

Clearly , ρ_λ^* is E–integral λ–adic representation of weight 1 . One may easily check that ρ_λ^* is also infinitisemally absolutely irreducible . Notice that τ induces an isomorphism $\mathrm{Im}(\rho_\lambda) \approx \mathrm{Im}(\rho_\lambda^*)$ of $\mathbf{Q}_l$– Lie groups , which , in turn , induces an isomorphism

$$\mathrm{Lie}(\mathrm{Im}(\rho_\lambda)) \approx \mathrm{Lie}(\mathrm{Im}(\rho_\lambda^*))$$

of the corresponding $\mathbf{Q}_l$– Lie algebras . This implies that the rank of the semisimple part of the $\mathbf{Q}_l$– Lie algebra $\mathrm{Lie}(\mathrm{Im}(\rho_\lambda^*))$ is also equal to r_λ' and, therefore,does not exceed $r(X)$.

Applying Corollary of Theorem 0.5 to infinitisemally absolutely irreducible E–integral λ–adic representation ρ_λ^* of weight 1 we obtain that

$$\dim_{E_\lambda} V_\lambda^* \leq \max\{D(j, 1) , 0 \leq j \leq r_\lambda'\} .$$

Since $r_\lambda' \leq r(X)$ and $\dim_{E_\lambda} V_\lambda^* = \dim_{E_\lambda} V_\lambda$,

$$\dim_{\mathbf{Q}_l} V_\lambda = [E_\lambda : \mathbf{Q}_l] \dim_{E_\lambda} V_\lambda \leq [E_\lambda : \mathbf{Q}_l] \max\{D(j,1) , 0 \leq j \leq r(X)\} =$$
$$= [E_\lambda : \mathbf{Q}_l]\, H .$$

Summing up over λ we obtain that

$$2 \dim X = \dim_{\mathbf{Q}_l} V_l(X) = \Sigma \dim_{\mathbf{Q}_l} V_\lambda(X) \leq H \Sigma [E_\lambda : \mathbf{Q}_l] =$$
$$= H [E : \mathbf{Q}] \leq H\, \mathrm{rk}(\mathrm{End}\, X) .$$

REFERENCES

1. N. Bourbaki, Groupes et algèbres de Lie, Ch. 2 – 3, Hermann, Paris, 1972.
2. N. Bourbaki, Groupes et algèbres de Lie, Ch. 7 – 8, Hermann, Paris, 1975.
3. G.Faltings, Endlichkeitssätze fur Abelsche Varietäten uber Zahlkörpern, Invent. Math. , 73, 349 – 366 (1983) .
4. G. Henniart, Représentations l–adiques abeliennes, Séminaire de Théorie de Nombres, Paris, 1980–81, Progress in Math., 22, Birkhäuser, 1981, 107 – 126 .
5. K. A. Ribet, Galois actions on division points of abelian variety with many real multiplications, Amer. J. of Math., 98, 751 – 804 (1976) .
6. J. – P. Serre, Abelian l–adic representations and elliptic curves, Benjamin, New – York, Amsterdam, 1968 .
7. Yu. G. Zarhin, Abelian varieties, l–adic representations and Lie algebras. Rank independence on l, Invent. Math. , 55, 165 – 176 (1979) .
8. Yu. G. Zarhin, Weights of simple Lie algebras in the cohomology of algebraic varieties, Math. USSR Izvestija, 24, 245 – 282 (1985) .
9. Yu. G. Zarhin, Torsion of Abelian varieties over GL(2)–extensions of number fields, Math. Ann., 1989, to appear .
10. C. Chevalley, Théorie de groupes de Lie, Groupes algèbriques, Hermann, Paris, 1951 .
11. Yu. G. Zarhin, Linear semisimple Lie algebras containing an operator with small number of eigen values, Arch. Math. , Basel , 46 , 522 – 532 (1986) .
12. J. – P. Wintenberger, Motifs et ramification pour les points d'ordre fini des variétés abéliennes, Séminaire de Théorie de Nombres, Paris, 1986–87, Progress in Math., 75, Birkhäuser, 1988, 453 – 471 .