KYUNGPOOK Math. J. 56(2016), 755-761
http://dx.doi.org/10.5666/KMJ.2016.56.3.755
pISSN 1225-6951 eISSN 0454-8124

On the Invariant of Chen-Kuan for Abelian Varieties

Hyunsuk Moon
Department of Mathematics, Kyungpook National University, Daegu 702-701, Korea
e-mail : hsmoon@knu.ac.kr

Abstract. Let A be an abelian variety over a global field K. We show that, in "many" cases, Chen-Kuan's invariant $M(A[n])$, that is the average number of n-torsion points of A over various residue fields of K, has the minimal possible value.

1. Introduction

Let K be a global field and G_K its absolute Galois group. Let R be a discrete valuation ring with maximal ideal $\mathfrak{m} = (\pi)$ and finite residue field $k := R/(\pi)$. For a positive integer n, we let V_n be a free $R/\mathfrak{m}^n$-module of finite rank $d \geq 1$. Set $U_{n,i} = \pi^i V_n \smallsetminus \pi^{i+1} V_n$ for each $0 \leq i \leq n-1$. Consider a continuous Galois representation $\rho_n : G_K \to \mathrm{GL}(V_n)$ unramified outside a finite set S of places of K, where $\mathrm{GL}(V_n)$ denotes the group of all automorphisms of V_n as an $R/\mathfrak{m}^n$-module. For $\mathfrak{p} \notin S$, we let $N_\mathfrak{p}$ be the number of fixed points of the action of the Frobenius conjugacy class $\mathrm{Frob}_\mathfrak{p} \subset G_K$ on V_n by ρ_n. We consider the average number of $N_\mathfrak{p}$ when $\mathfrak{p}$ runs through the non-archimedean places in K, that is

$$M(\rho_n) = \lim_{x\to\infty} \frac{1}{\pi_K(x)} \sum_{\kappa(\mathfrak{p})\leq x,\ \mathfrak{p}\notin S} N_\mathfrak{p},$$

where $\kappa(\mathfrak{p})$ is the number of elements of the residue field of $\mathfrak{p}$ and $\pi_K(x)$ is the number of places of K with $\kappa(\mathfrak{p}) \leq x$.

It is known that the limit $M(\rho_n)$ exists and it is equal to the number of orbits of G_K in V_n ([4], cf. [1], [3]). In general, $M(\rho_n) \geq n+1$ since each $\pi^i V_n$ is stable under the Galois action and so $U_{n,i}$ for each $0 \leq i \leq n-1$ is stable. Also, there is a certain relationship between $M(\rho_n)$ and the size of the image of Galois representations. For instance, if ρ_n is surjective, then $M(\rho_n) = n+1$, because G_K acts transitively on $U_{n,i}$ for each $0 \leq i \leq n-1$ ([4], Theorem 4). Applying this result to the n-torsion subgroup $E[n]$ of an elliptic curve without complex multiplication, we proved that $M(E[n])$ is equal to the divisor function $d(n)$ for all integers n prime to a certain

Received March 22, 2016; revised May 17, 2016; accepted July 5, 2016.
2010 Mathematics Subject Classification: primary 11F80; secondary 11G05, 11N45.
Key words and phrases: Galois representations, torsion points, Galois orbits.

constant $C_{E/K}$ (which depends on E and K). The aim of this paper is to generalize the above result to the case where ρ_n is not necessarily surjective. For instance, our theorem is applicable if $d = 2g$ and $\mathrm{Im}(\rho_n)$ contains $\mathrm{Sp}_{2g}(R/\pi^n)$, which is the case if ρ_n comes from an abelian variety of a rather general class:

Theorem 1.1. (=Corollary 3.3, §3) *Let K be a number field and A an abelian variety defined over K. Suppose that $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$ and $\dim(A) =$ odd or 2 or 6. Then there exists an integer $C_{A/K}$ depending on A and K such that for all n prime to $C_{A/K}$, we have*

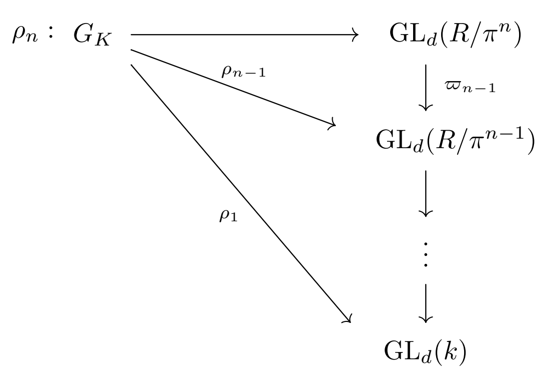
$$M(A[n]) = d(n),$$

where $d(n)$ is the number of positive divisors of n.

2. A Sufficient Condition for the Transitivity

In this section, we find a sufficient condition for the transitivity of the Galois action.

For a continuous representation $\rho_n : G_K \to \mathrm{GL}_d(R/\pi^n)$, we let $G_n := \mathrm{Im}(\rho_n) \subset \mathrm{GL}_d(R/\pi^n)$ and $\varpi_m : \mathrm{GL}_d(R/\pi^{m+1}) \to \mathrm{GL}_d(R/\pi^m)$ a mod π^m reduction map for an integer $1 \leq m < n$.



For each $0 \leq i < m$, the actions of G_m on $U_{m,i} = \pi^i V_m \setminus \pi^{i+1} V_m$ and G_{m-i} on $U_{m-i,0} = V_{m-i} \setminus \pi V_{m-i}$ are compatible in the sense that

$$(*) \qquad g(\pi^i v) = \pi^i(\bar{g} v)$$

for all $g \in G_m$ and $v \in V_{m-i}$, where $\bar{g}$ is the mod π^{m-i} reduction of g.

$$\begin{array}{ccc}
\pi^i v & & v \\
\rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\
U_{m,i} & \xleftarrow{\text{multiplication by } \pi^i} & U_{m-i,0} \\
\circlearrowleft & & \circlearrowright \\
G_m & \xrightarrow{\bmod \pi^{m-i}} \!\!\!\!\rightarrow & G_{m-i} \\
\rotatebox{90}{$\ni$} & & \rotatebox{90}{$\ni$} \\
g & \longmapsto & \bar{g}
\end{array}$$

In particular, the action of G_m on $\pi^{m-1}V_m$ and G_1 on V_1 are compatible, so G_m acts on V_1 in the sense of $(*)$.

On the other hand, the kernel of ϖ_{m-1} is $1+\pi^{m-1}\,\mathrm{M}_d(R/\pi^m)$ for $m \geq 2$. Since $\pi^{m-1}x$ for $x \in \mathrm{M}_d(R/\pi^m)$ depends only on the class of $x \pmod{\pi}$, we may regard x as an element of $\mathrm{M}_d(R/\pi^m)/\pi\,\mathrm{M}_d(R/\pi^m) \simeq \mathrm{M}_d(k)$. So, we can identify each element of the kernel with $1+\pi^{m-1}x$ for some $x \in \mathrm{M}_d(k)$. We put

$$\mathfrak{g}_m := \{x \in \mathrm{M}_d(k) | 1+\pi^{m-1}x \in \mathrm{Ker}(\varpi_{m-1}) \cap G_m\}.$$

Since $(1+\pi^{m-1}x)(1+\pi^{m-1}y) \equiv 1+\pi^{m-1}(x+y) \pmod{\pi^m}$, $\mathfrak{g}_m$ is an abelian group under the addition. Via $(*)$, we regard V_1 as $\mathfrak{g}_m$-module:

$$\begin{array}{ccccc}
\mathfrak{g}_m & \subset & \mathrm{M}_d(R/\pi^m) \big/ \pi\,\mathrm{M}_d(R/\pi^m) & \simeq & \mathrm{M}_d(R/\pi) \\
 & & \curvearrowright & & \curvearrowright \\
 & & V_m \big/ \pi V_m & \simeq & V_1
\end{array}$$

Lemma 2.1. *We assume that*

(1) *the action of G_1 on $V_1 \setminus \{0\}$ is transitive, and*

(2) *for any $v' \in V_1$ and $v \in V_1 \setminus \{0\}$, there exists an $x \in \mathfrak{g}_m$ for each $2 \leq m \leq n$ satisfying $v' = xv$.*

Then G_n acts on $U_{n,i}$ transitively for each $0 \leq i \leq n-1$.

Proof. Since the action of G_n on $U_{n,i}$ is compatible with the action of G_{n-i} on $U_{n-i,0}$ in the sense of $(*)$, we show that G_m acts on $U_{m,0}$ transitively for $1 \leq m \leq n$. Use induction on m. If $m = 1$, then it is trivial by the assumption (1). Assume that G_{m-1} acts on $U_{m-1,0}$ transitively. Let $v,\ v' \in U_{m,0} = V_m \setminus \pi V_m$. By the assumption of the induction and using that ϖ_{m-1} is surjective, we have $g_m \in G_m$ such that $v' \equiv g_m v \pmod{\pi^{m-1}}$. So, we may assume $v' \equiv v \pmod{\pi^{m-1}}$. Then $v' - v \in \pi^{m-1}V_m \simeq V_1$ and by the assumption (2), we have $x \in \mathfrak{g}_m$ satisfying $v' - v = x(\pi^{m-1}v)$. Thus $v' = v + x\pi^{m-1}v = (1 + \pi^{m-1}x)v$ for $1 + \pi^{m-1}x \in G_m$. Hence the proof is complete. □

3. The Results

Theorem 3.1. *If the image of ρ_n contains $\mathrm{SL}_d(R/\pi^n)$, then $M(\rho_n) = n + 1$.*

Proof. We use the same notation as in §2. Since $M(\rho_n) \geq n + 1$, we may assume $G_n = \mathrm{SL}_d(R/\pi^n)$. We apply Lemma 2.1 with $G_n = \mathrm{SL}_d(R/\pi^n)$ by checking the assumptions therein. For assumption (1), it is well-known that the action of SL_d over a field k on $k^{\oplus d} \setminus \{0\}$ is transitive ([2], §4.7). For assumption (2), at first, we determine $\mathfrak{g}_m$, $2 \leq m \leq n$. Since $\det(1 + \pi x) \equiv 1 + \mathrm{tr}(x)\pi \pmod{\pi^2}$, if $1 + \pi x \in \mathrm{SL}_d(R/\pi^2)$, we have $\mathrm{tr}(x) \equiv 0 \pmod{\pi}$. So,

$$\mathfrak{g}_2 = \{x \in \mathrm{M}_d(k) \mid \mathrm{tr}(x) = 0\}$$

and similarly

$$\begin{aligned}\mathfrak{g}_m &= \{x \in \mathrm{M}_d(k) \mid 1 + \pi^{m-1}x \in \mathrm{SL}_d(R/\pi^m)\} \\ &= \{x \in \mathrm{M}_d(k) \mid \mathrm{tr}(x) = 0\}.\end{aligned}$$

Hence we know that $\mathfrak{g}_2 = \mathfrak{g}_3 = \cdots = \mathfrak{g}_n$.

Now, let $v,\ v' \in V_1 \setminus \{0\}$. Then we show that there exists an element $x \in \mathfrak{g}_2$ satisfying $v' = xv$. It is equivalent to showing that there exists an $x_i \in \mathfrak{g}_2$ satisfying $x_i v = e_i$ where $\{e_1, \cdots, e_d\}$ is the standard basis for V_1. We only show the case $i = 1$. Other cases of i are similar. For a nonzero $v = {}^t(v_1 \ \cdots \ v_d) \in V_1$, if $v_1 \neq 0$, then we take $x_1 \in \mathfrak{g}_2$ such that

$$x_1 v = \begin{pmatrix} v_1^{-1} & & & & \\ & 0 & & & \\ & & \ddots & & \\ & & & 0 & \\ t & & & & -v_1^{-1} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

where $t = (v_1^{-1})^2 v_d$. If $v_1 = 0$ and $v_i \neq 0$ for some $i \neq 1$, then we take $x_1 \in \mathfrak{g}_2$ such as

$$x_1 v = \begin{pmatrix} 0 & & v_i^{-1} & 0 \\ & \ddots & & \\ & & \ddots & \\ & & & 0 \end{pmatrix} \begin{pmatrix} 0 \\ v_2 \\ \vdots \\ v_d \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Therefore G_n acts on $U_{n,i}$ transitively for $0 \leq i \leq n-1$, so the number of orbits is $n + 1$. □

Remark 3.2. In general, if $G \subset \mathrm{GL}_d$ is an algebraic group over R and $G_n = G(R/\pi^n)$, then $\mathfrak{g}_m$ coincides for all positive integers $m \geq 2$.

From now on, we assume $d \geq 1$ is an even integer $d = 2g$.

Theorem 3.3. *If the image of ρ_n contains $\mathrm{Sp}_{2g}(R/\pi^n)$, then $M(\rho_n) = n+1$.*

Proof. We use the same notation as in §2. Since $M(\rho_n) \geq n+1$, we may assume $G_n = \mathrm{Sp}_{2g}(R/\pi^n)$. We apply Lemma 2.1 with $G_n = \mathrm{Sp}_{2g}(R/\pi^n)$ by checking the assumptions therein. For assumption (1), it is well-known that the action of Sp_{2g} over a finite field k on $k^{\oplus 2g} \setminus \{0\}$ is transitive ([2], §8.5). For assumption (2), we determine $\mathfrak{g}_m$, $2 \leq m \leq n$. If we let $J = \begin{pmatrix} 0 & \mathrm{I}_g \\ -\mathrm{I}_g & 0 \end{pmatrix}$, then we have

$$^t(1+\pi x)J(1+\pi x) \equiv J + \pi Jx + \pi\, {}^t xJ \pmod{\pi^2}.$$

So, if $1+\pi x \in \mathrm{Sp}_{2g}(R/\pi^2)$, then we have $Jx + {}^t xJ \equiv 0 \pmod{\pi}$. Hence,

$$\begin{aligned}\mathfrak{g}_2 &= \{x \in \mathrm{M}_{2g}(k) \mid Jx + {}^t xJ = 0\} \\ &= \{\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{M}_{2g}(k) \mid B = {}^tB, C = {}^tC, {}^tA = -D\}.\end{aligned}$$

Now, let $v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \in V_1 \setminus \{0\}$, where v_1, v_2 are column vectors of $k^{\oplus g}$. We show that there exists an element $x_i = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathfrak{g}_2 \cap \mathrm{GL}_{2g}(k)$ such that $v = x_i \mathbf{e}_i$ for each $1 \leq i \leq 2g$, where $\{\mathbf{e}_1, \cdots, \mathbf{e}_{2g}\}$ (resp. $\{e_1, \cdots, e_g\}$) is the standard basis for V_1 (resp. $k^{\oplus g}$) (so $\mathbf{e}_i = {}^t(e_i \ \ 0)$ for $1 \leq i \leq g$). This implies $x_i^{-1} v = \mathbf{e}_i$. We only show the case $i = 1$. Other cases of i are similar. We divide into two cases.

Case 1. v_1 is a nonzero vector: Consider the equation

$$v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = x\mathbf{e}_1 = \begin{pmatrix} A & B \\ C & -{}^tA \end{pmatrix} \begin{pmatrix} e_1 \\ 0 \end{pmatrix} = \begin{pmatrix} Ae_1 \\ Ce_1 \end{pmatrix}.$$

Then we have $Ae_1 = v_1$ and $Ce_1 = v_2$. Since there exists a basis for $k^{\oplus g}$ containing v_1, we can find an invertible matrix with the first column v_1, which implies $Ae_1 = v_1$. We take a symmetric matrix C with the first column v_2 and $B = 0$. Then $x = \begin{pmatrix} A & 0 \\ C & -{}^tA \end{pmatrix}$ is invertible since $\det x = \det A \det(-{}^tA) \neq 0$.

Case 2. $v_1 = 0$ and v_2 is a nonzero vector: If we let $v_2 = {}^t(t_1 \ t_2 \ \cdots \ t_g)$, then we take a symmetric matrix

$$C = \begin{pmatrix} t_1 & t_2 & \cdots & t_g \\ t_2 & a_2 & 0 & 0 \\ \vdots & & \ddots & \vdots \\ t_g & 0 & \cdots & a_g \end{pmatrix}$$

with the first column v_2. In this case, we have

$$\det C = t_1 a_2 \cdots a_g - t_2^2 a_3 \cdots a_g - \cdots - t_g^2 a_2 \cdots a_{g-1}.$$

When $t_i \neq 0$ for some $i \neq 1$, if we let $a_i = 0$, then we have

$$\det C = -t_i^2 a_2 \cdots a_{i-1} a_{i+1} \cdots a_g.$$

When $t_2 = \cdots = t_g = 0$ and $t_1 \neq 0$, then we have

$$\det C = t_1 a_2 \cdots a_g.$$

Thus we can always find an invertible symmetric matrix C for any nonzero v_2 such that $Ce_1 = v_2$. Hence if we take $A = 0$ and any invertible symmetric matrix B, then $x = \begin{pmatrix} 0 & B \\ C & 0 \end{pmatrix}$ is invertible since $\det x = (-1)^g \det C \det B \neq 0$. Therefore the proof is complete. □

Let A be an abelian variety defined over K of dimension g. We apply Theorem 3.2 to the Galois representations $\rho : G_K \to \mathrm{Aut}(A[n])$ over the n-division points of A. We write $M(A[n])$ for $M(\rho)$. The following corollary generalizes Corollary 5 of [4].

Corollary 3.4. *Let K be a number field and A an abelian variety defined over K of dimension g. Suppose that $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$ and $\dim(A) =$ odd or 2 or 6. Then there exists an integer $C_{A/K}$ depending on A and K such that for all n prime to $C_{A/K}$, we have*

$$M(A[n]) = d(n),$$

where $d(n)$ is the number of positive divisors of n.

Proof. Let $n = \prod p^{e_p}$ be the prime factorization of n and

$$\rho : G_K \to \mathrm{Aut}(A[n]) \simeq \mathrm{GL}_{2d}(\mathbb{Z}/n\mathbb{Z}) \simeq \prod \mathrm{GL}_{2d}(\mathbb{Z}/p^{e_p}\mathbb{Z})$$

the Galois representation on $A[n]$. By a theorem of Serre ([5], Théorème 3), there exists an integer $C_{A/K}$ such that the image of p-factor ρ_p of ρ is $\mathrm{GSp}_{2g}(\mathbb{Z}/p^{e_p}\mathbb{Z})$ for any prime $p \nmid C_{A/K}$. By Theorem 3.2, we have $M(A[p^{e_p}]) = e_p + 1$ for such p. By the multiplicativity of $M(\rho)$ ([4], Cor. 3), we have for all n prime to $C_{A/K}$,

$$\begin{aligned} M(A[n]) &= \prod M(A[p^{e_p}]) \\ &= \prod (e_p + 1) \\ &= d(n). \end{aligned}$$

□

References

[1] Yen-Mei J. Chen and Yen-Liang Kuan, *On the distribution of torsion points modulo primes*, Bull. Aust. Math. Soc., **86**(2012), 339–347.

[2] P. M. Cohn, *Algebra*, Second edition Volume 3, John Wiley & Sons, 1991.

[3] Hsiu-Lien Huang, *The average number of torsion points on elliptic curves*, J. Number Theory, **135**(2014), 374–389.

[4] H. Moon, *On the invariant $M(A_{/K}, n)$ of Chen-Kuan for Galois representations*, Proc. Japan Acad., **90**(2014), 98-100.

[5] J.-P. Serre, *Résumé des cours de 1985–1986*, Annuaire du Collége de France (1986), 95–99.