Rational points of Abelian varieties in Γ-extension

By Hideji ITO

Let K be an algebraic number field, and L/K the Γ-extension associated to the rational prime p. We put $\Gamma_n=\Gamma^{p^n}$, and denote by K_n corresponding subfields. Let A be an abelian variety defined over K.

The purpose of this short note is to improve B. Mazur's result on the asymptotic behavior of the *rank* $A(K_n)$, where $A(K_n)$ is the K_n-rational-point-group of A. The known asymptotic estimate is the following, somewhat weak, one: there is a non-negative integer ρ such that *rank* $A(K_n)+$ *corank*$H^1(\Gamma_n, A(L))=\rho\cdot p^n+const.$ for all sufficiently large n. Here, for a p-primary Γ-module G, *corank* G means the Z_p-rank of G^*, where G^* is the Pontrjagin dual of G (see [1], p. 22).

We shall show that the *corank* $H^1(\Gamma_n, A(L))$ is in fact constant for all sufficiently large n, so that we get an asymptotic formula for the rank of $A(K_n)$.

In section 1, we shall prove above fact in general setting, and in section 2 apply it to $A(L)$.

NOTATIONS.

For a finite group X, $|X|$ denotes its order. If G is a group and if B is a G-module, B^G means the subgroup of B consisted of the invariant elements under the action of G.

1. The aim of this section is to prove the following

THEOREM 1. *Let B be a Γ-module, such that B^{Γ_n} is a free Z-module of finite rank for all n. Then the corank $H^1(\Gamma_n, B)$ is constant for all sufficiently large n.*

Before beginning the proof, we recall the well-known structure of $H^i(\mathfrak{g}, C)$ for $i=1,2$, where $\mathfrak{g}$ is a finite cyclic group and C is a $\mathfrak{g}$-module:

$$H^1(\mathfrak{g}, C)={}_{\mathfrak{g}}C/D_{\mathfrak{g}}C\,,\qquad H^2(\mathfrak{g}, C)=C^{\mathfrak{g}}/N_{\mathfrak{g}}C\,.$$

Here $N_{\mathfrak{g}}$ is the homomorphism $C\rightarrow C^{\mathfrak{g}}$, defined by $N_{\mathfrak{g}}(x)=\sum_{\tau\in\mathfrak{g}}\tau x$ for $x\in C$, ${}_{\mathfrak{g}}C=\mathrm{Ker}\ (N_{\mathfrak{g}})$, and $D_{\mathfrak{g}}C=\{\tau x-x|x\in C, \tau\in\mathfrak{g}\}=\{\sigma x-x|x\in C\}$ for any generator σ of $\mathfrak{g}$.

First we observe that corank $H^1(\Gamma_n, B)$ is monotone increasing.

LEMMA 1. *Suppose $m \geqq n$, then corank $H^1(\Gamma_m, B) \geqq$ corank $H^1(\Gamma_n, B)$.*

PROOF. Obvious from the inflation-restriction sequence $0 \to H^1(\Gamma_n/\Gamma_m, B^{\Gamma_n}) \to H^1(\Gamma_n, B) \to H^1(\Gamma_m, B)$.

Therefore, without loss of generality, we may assume that the corank $H^1(\Gamma_n, B)$ is finite for all n.

Next we discuss the action of Γ/Γ_m of B^{Γ_m} and obtain non-negative integers $e(p^i)$, by which $|H^1(\Gamma/\Gamma_m, B^{\Gamma_m})|$ is expressed in case $B^\Gamma = 0$.

Put $r_m = \text{rank}\,(B^{\Gamma_m})$. From the action of Γ/Γ_m on B^{Γ_m}, we get representations $\psi_m : \Gamma/\Gamma_m \to GL_{r_m}(\boldsymbol{Z})$. For $m \geqq n$, let $j_{m,n}$ be the natural surjection $\Gamma/\Gamma_m \to \Gamma/\Gamma_n$. Combining ψ_m and $j_{m,n}$, we get representations $\psi_{m,n} = \psi_n \circ j_{m,n}$: $\Gamma/\Gamma_m \to GL_{r_n}(\boldsymbol{Z})$. For a fixed generator σ_m of $\Gamma/\Gamma_m (\cong \boldsymbol{Z}/p^m\boldsymbol{Z})$, we put $M_m = \psi_m(\sigma_m)$, $M_{m,n} = \psi_{m,n}(\sigma_m)$. From the construction, $M_{m,n}$ and M_n are equivalent. Denote by $F_m(X) \in \boldsymbol{Z}[X]$ the characteristic polynomial of M_m. Since $F_m(X)$ divides $(X^{p^m} - 1)^{r_m}$, we can write $F_m(X) = \prod_{i=0}^{m} \Phi_{p^i}(X)^{e_m(p^i)}$, $0 \leqq e_m(p^i) \leqq r_m$. Here $\Phi_d(X)$ means the cyclotomic polynomial. Since deg $\Phi_d(X) = \varphi(d)$, we have $r_m = \sum_{i=0}^{m} \varphi(p^i) \cdot e_m(p^i)$, ($\varphi$ = Euler's function). Of course $e_m(p^i)$ does not depend on the choice of the $\boldsymbol{Z}$-basis of B^{Γ_m}, nor on the choice of σ_m. And indeed $e_m(p^i)$ is independent of m. For the proof we need the following

LEMMA 2. *Suppose G is a finite group and C is a free $\boldsymbol{Z}$-module of finite rank on which G acts. Then there are submodules D and E of C which have the following properties respectively.*

1) $C = C^G \oplus D$, *rank* $D =$ *rank* $({}_GC)$,

2) $C = E \oplus {}_GC$, *rank* $E =$ *rank* (C^G).

PROOF. By the elementary divisor theory the existence of the above direct sum is easily verified. As for the rank, we have only to note the exact sequence $0 \to {}_GC \to C \to N_G(C) \to 0$, and the relation $C^G \supset N_G(C) \supset |G| \cdot C$.

PROPOSITION 1. *Notations being as above, suppose $m \geqq n$. Then we have $e_m(p^i) = e_n(p^i)$, for $0 \leqq i \leqq n$. Hence we can drop the suffix of e_m, so that we get the relations $r_m = \sum_{i=0}^{m} \varphi(p^i) \cdot e(p^i)$, $r_m - r_{m-1} = \varphi(p^i) \cdot e(p^i)$, for all m.*

PROOF. Apply lemma 2. 1) to $G = \Gamma_n/\Gamma_m \cong \boldsymbol{Z}/p^{m-n}\boldsymbol{Z}$, $C = B^{\Gamma_m}$. (Note that $(B^{\Gamma_m})^{\Gamma_n/\Gamma_m} = B^{\Gamma_n}$). On account of the direct sum decomposition, matrix $M_m (= M$, we write for short) can be written in the following form: $M = \left(\begin{array}{c|c} M' & * \\ \hline 0 & R \end{array}\right)$, $M' = M_{m,n}$, $R \in GL_{r_m - r_n}(\boldsymbol{Z})$. Hence we have $F_m(X) = F_n(X) \cdot F_R(X)$, where $F_R(X)$ is the characteristic polynomial of R. Therefore it suffices to show that all the roots of $F_R(X)$ i.e. all the characteristic roots of R are

p^i-th primitive roots of unity ($i>n$). The generator $\sigma_m{}^{p^n}$ of Γ_n/Γ_m is represented in the form $M^{p^n}=\left(\begin{array}{c|c} \begin{matrix}1 & 0\\ & \ddots \\ 0 & 1\end{matrix} & * \\ \hline 0 & R^{p^n}\end{array}\right)$. Put $T=R^{p^n}$. We must show that among the characteristic roots of T there is not a 1. Norm homomophism $N_{\Gamma_n/\Gamma_m}=\sum_{j=1}^{p^{m-n}}(\sigma_m^{p^m})^j:\ B^{\Gamma_m}\to B^{\Gamma_n}$ is represented in the form

$$\sum_{j=1}^{p^{m-n}}(M^{p^n})^j=\left(\begin{array}{c|c} \begin{matrix}p^{m-n} & & \\ & \ddots & \\ 0 & & p^{m-n}\end{matrix} & * \\ \hline 0 & \sum_{j=1}^{p^{m-n}} T^j\end{array}\right).$$

Hence $\sum_{j=1}^{p^{m-n}} T^j=0$. This implies the desired result (note that $T^{p^{m-n}}=1$).

The relation between $e(p^i)$ and $|H^1(\Gamma/\Gamma_m, B^{\Gamma_m})|$ mentioned above is as follows.

PROPOSITION 2. *Suppose $B^\Gamma=0$, then*

1) $|H^1(\Gamma/\Gamma_m, B^{\Gamma_m})|=p^{\sum_{i=1}^{m} e(p^i)}$,

2) *in general, for $m\geqq n$, $H^1(\Gamma_n/\Gamma_m, B^{\Gamma_m})^{\Gamma/\Gamma_n}=H^1(\Gamma_n/\Gamma_m, B^{\Gamma_m})$, and* $|H^1(\Gamma_n/\Gamma_m, B^{\Gamma_m})|=p^{\sum_{i=n+1}^{m} e(p^i)}$.

PROOF. 1) Put $C=B^{\Gamma_m}$, $\mathfrak{g}=\Gamma/\Gamma_m$. By our assumption $B^\Gamma=0$, we have ${}_{\mathfrak{g}}C=C$. In $GL_{r_m}(\boldsymbol{C})$, the matrix M_m-1 is equivalent to the matrix $\begin{pmatrix}\omega_1-1 & & 0\\ & \ddots & \\ 0 & & \omega_{r_m}-1\end{pmatrix}$, where ω_i's are the p^m-th roots of unity ($\neq 1$). Hence M_m-1 is regular. As $D_{\mathfrak{g}}(C)=C(M_m-1)$, we get $|H^1(\mathfrak{g}, C)|=|C/D_{\mathfrak{g}}(C)|=|\det(M_m-1)|=\left|\prod_{i=1}^{r_m}(\omega_i-1)\right|=\left|\prod_{i=1}^{m}\Phi_{p^i}(1)^{e(p^i)}\right|=p^{\sum_{i=1}^{m} e(p^i)}$.

2) Notations being as in the proof of 1), put $\mathfrak{h}=\Gamma_n/\Gamma_m$. Apply lemma 2.1, taking $\mathfrak{h}$ in place of G. Then $M_m=\left(\begin{array}{c|c} * & 0\\ \hline * & S\end{array}\right)$, $S\in GL_k(\boldsymbol{Z})$, $k=r_m-r_n$. The same reasoning as in the proof of 1) gives $|H^1(\mathfrak{h}, {}_{\mathfrak{h}}C)|=|\det(S-1)|=p^{\sum_{i=n+1}^{m} e(p^i)}$. Since $|H^1(\mathfrak{h}, C)|\leqq|H^1(\mathfrak{h}, {}_{\mathfrak{h}}C)|$, we have $|H^1(\mathfrak{h}, C)|\leqq p^{\sum_{i=n+1}^{m} e(p^i)}$. But the exact sequence of Hochschild-Serre $0\to H^1(\mathfrak{g}/\mathfrak{h}, C^{\mathfrak{h}})\to H^1(\mathfrak{g}, C)\to H^1(\mathfrak{h}, C)^{\mathfrak{g}/\mathfrak{h}}\to\cdots$ implies $p^{\sum_{i=n+1}^{m} e(p^i)}\leqq|H^1(\mathfrak{h}, C)^{\mathfrak{g}/\mathfrak{h}}|$. Hence we have our assertion.

Now we can prove theorem 1. By means of the exact sequence of Hochschild-Serre, we easily see that corank $H^1(\Gamma, B)$=corank $H^1(\Gamma_n, B)^{\Gamma/\Gamma_n}$. Since $\Gamma_n=\varprojlim_{m\geqq n}\Gamma_n/\Gamma_m$, and $B=\varinjlim_m B^{\Gamma_m}$, we have $H^1(\Gamma_n, B)=\varinjlim_{m\geqq n} H^1(\Gamma_n/\Gamma_m, B^{\Gamma_m})$. So the validity of our assertion in case $B^\Gamma=0$ is obvious, on account of Prop. 2. 2).

To prove the theorem in general case, put $B'=B/B^\Gamma$. Then we have $(B')^\Gamma=0$. Indeed from the exact sequence; (*) $0\to B^\Gamma\to B\to B'\to 0$, we get the exact sequence $0\to B^\Gamma\to B^\Gamma\to(B')^\Gamma\to H^1(\Gamma, B^\Gamma)=\varinjlim_m H^1(\Gamma/\Gamma_m, B^\Gamma)=0$. From (*), we also get the exact sequence

$$0=H^1(\Gamma_n, B^\Gamma)\to H^1(\Gamma_n, B)\to H^1(\Gamma_n, B')\to H^2(\Gamma_n, B^\Gamma).$$

But $H^2(\Gamma_n, B^\Gamma)=\varinjlim_{m\geqq n} H^2(\Gamma_n/\Gamma_m, B^\Gamma)\cong\varinjlim_{m\geqq n} B^\Gamma/p^{m-n}B^\Gamma$. So, dualizing above sequence, we obtain the following inequality:

$$\text{corank } H^1(\Gamma_n, B)\leqq\text{corank } H^1(\Gamma_n, B')\leqq\text{corank } H^1(\Gamma_n, B)+\text{rank}(B^\Gamma).$$

(Note that $B^\Gamma/p^{m-n}B^\Gamma\cong\overbrace{Z/p^{m-n}Z\oplus\cdots\oplus Z/p^{m-n}Z}^{r}$, where r is the rank of B^Γ). As theorem 1 holds in case $B^\Gamma=0$, corank $H^1(\Gamma_n, B')$ is constant for all n. Therefore, by means of the above inequality and lemma 1, the corank $H^1(\Gamma_n, B)$ must be constant for all sufficiently large n. This completes the proof of our theorem 1.

2. In order to apply the theorem 1 to $A(L)$, we need some modifications on $A(K_n)$. Let $\tilde{A}(K_m)$ be the set of points of finite order in $A(K_m)$. By Mordell-Weil's theorem $\tilde{A}(K_m)$ is finite. Denote its order by N_m. We put $\overline{A_m}=N_m\cdot A(K_m)$ (=free Z-module of the same rank as of $A(K_m)$), and for $m\geqq n$ define homomorphisms $f_{n,m}$: $\overline{A_n}\to\overline{A_m}$ by $f_{n,m}(x)=\dfrac{N_m}{N_n}x$, for x in $\overline{A_n}$. Since the system $(\overline{A_n}, \{f_{n,m}\})$ is inductive, we can define $\overline{A_L}=\varinjlim A_n$. The group $\overline{A_L}$ has obvious Γ-module structure and $(\overline{A_L})^{\Gamma_n}\cong\overline{A_n}$ as Γ-module. Hence rank $(\overline{A_L})^{\Gamma_n}$=rank $\overline{A_n}$=rank $A(K_n)$.

LEMMA 3. *We have corank* $H^1(\Gamma_n, A(L))$ = *corank* $H^1(\Gamma_n, \overline{A_L})$, *for all* n.

PROOF. Let $m\geqq n$. The exact sequence of Γ_n/Γ_m-modules: $0\to\tilde{A}(K_m)\to A(K_m)\xrightarrow{g_m}N_m\cdot A(K_m)=\overline{A_m}\to 0$, where g_m is the multiplication by N_m, yields the exact sequence of cohomology groups:

$$\cdots\to H^1\bigl(\Gamma_n/\Gamma_m, \tilde{A}(K_m)\bigr)\to H^1\bigl(\Gamma_n/\Gamma_m, A(K_m)\bigr)\to$$
$$H^1(\Gamma_n/\Gamma_m, \overline{A_m})\to H^2\bigl(\Gamma_n/\Gamma_m, \tilde{A}(K_m)\bigr)\to\cdots.$$

Since $H^1(\Gamma_n, A(L))=\varinjlim_{m\geqq n} H^1(\Gamma_n/\Gamma_m, A(K_m))$ etc., we get the exact sequence

$$\to H^1\bigl(\Gamma_n, \tilde{A}(L)\bigr)\to H^1\bigl(\Gamma_n, A(L)\bigr)\to H^1(\Gamma_n, \overline{A_L})\to H^2\bigl(\Gamma_n, \tilde{A}(L)\bigr).$$

Now independent of m, the order of $H^i(\Gamma_n/\Gamma_m, \tilde{A}(K_m))$ is bounded (for $i=1, 2$). Indeed, as Γ_n/Γ_m is a finite cyclic group and $\tilde{A}(K_m)$ is finite, $|H^1(\Gamma_n/\Gamma_m, \tilde{A}(K_m))|=|H^2(\Gamma_n/\Gamma_m, \tilde{A}(K_m))|\leqq|\tilde{A}(K_n)|$. So their inductive limit $\mathrm{H}^i(\Gamma_n, \tilde{A}(L))$ must be finite (for $i=1, 2$). Hence we have our assertion.

THEOREM 2. *Let A be an abelian variety defined over a number field K, L/K the Γ-extension associated to the rational prime p, and K_n the subfield of L/K such that Gal (K_n/K) is isomorphic to $\mathbf{Z}/p^n\mathbf{Z}$. Then there exists a non-negative integer ρ, for which we have rank $A(K_n)=\rho\cdot p^n+const.$ for all sufficiently large n.*

For the proof, apply theorem 1 and lemma 3 to B. Mazur's estimate mentioned in the introduction.

Although we do not know at present even an example in which ρ is positive, by means of Prop. 1, 2 we easily get the following

PROPOSITION 3. *If corank $H^1(\Gamma, A(L))>0$, then rank $A(K_n)$ grows arbitralily large, as $n\to\infty$.*

Department of Mathematics
Hokkaido University

Reference

[1] Y. I. MANIN: Cyclic fields and modular curves, Uspehi. Acad. Nauk. CCCP, Vol. 26, No. 6, 7–71 (1971).
English transl.: Russian Mathematical Surveys, Vol. 26, No. 6, 7–78 (1971).

(Received April 2, 1973)