Hardy-Ramanujan Journal 42 (2019), 85-99 submitted 27/08/2019, accepted 16/12/2019, revised 06/02/2019

Divisibility of Selmer groups and class groups

Kalyan Banerjee, Kalyan Chakraborty and Azizul Hoque

Dedicated to the memory of Alan Baker

Abstract. In this paper, we study two topics. One is the divisibility problem of class groups of quadratic number fields and its connections to algebraic geometry. The other is the construction of Selmer group and Tate-Shafarevich group for an abelian variety defined over a number field.

Keywords. Picard group, Class group, Hyperelliptic surface, Imaginary quadratic field, Selmer group, Tate-Shafarevich group, Chow group, Abelian variety.

2010 Mathematics Subject Classification. Primary: 11G10, 11R29, 11R65, 14C25; Secondary: 14C05, 14C20.

1. Introduction

An interesting and important fact about the ideal class group of the ring of integers in a number field is that it is finite. So it is natural to ask whether given any positive integer n there exists n-torsion elements in the class group of the number field. This is related to the so called 'divisibility problem' of the class group: given a positive integer n whether it divides the order of the class group. In the paper [BaHo19], the authors studied the relations of this divisibility problem with the elements of n-torsions in the Picard group of a hyperelliptic surface. More precisely, suppose that we consider a hyperelliptic surface S defined over $\bar{\mathbb{Q}}$ given by a precise equation. Suppose that S admits a regular map to the affine plane $\mathbb{A}^2_{\bar{\mathbb{Q}}}$ defined over $\bar{\mathbb{Q}}$. Then spreading out $S, \mathbb{A}^2$ over $\mathrm{Spec}(\mathbb{Z})$ we have a family of ring of integers of a family of specific number fields. Now suppose that we start with a n-torsion element in the Picard group of S, then restricting it to fibers we have n-torsion elements in the class group of each member of the above family of ring of integers. Moreover a certain family of subgroups of n-torsions' of the class group of each member of the above family has same cardinality for each fiber over a Zariski open subgroup of $\mathbb{A}^2_{\mathbb{Z}}$. This phenomena supports the so called Cohen-Lenstra heuristic which proposes the conjectural fact that given any n a positive proportion of the number fields has an element whcih are n-torsion in its class group. Atleast we can say that for the above family the number fields having the divisibility property is"parametrized" by a Zariski open subset of the affine plane over $\mathrm{Spec}(\mathbb{Z})$.

The main theme of this work was to use the Mumford-Roĭtman argument for the natural map from relative Chow schemes to the relative Picard group, which says that the fibers of this map are countable union of Zariski closed subsets varying in a family.

The other theme of this paper is the Selmer and Tate-Shafarevich group constructions of an abelian variety defined over a number field. The notion of Selmer group and the Tate-Shafarevich group is very much important from the perspective of local-global principle in arithmetic geometry. The Tate-Shafarevich group measures the failure of the local to global principle. The studies of these groups have been initiated by Cassels, Lang, Selmer, Shafarevich, Tate, [Cas62a], [Cas62b], [LaTa58], [Sel51], [Sha59], [Ta58]. The famous conjecture about the Tate-Shafarevich group tells that this group associated to an abelian variety is finite. The first case where it has been proven is the case of elliptic curves with complex multiplication having rank atmost 1, by Karl Rubin, [Rub87]. The next is the

We thank episciences.org for providing open access hosting of the electronic journal *Hardy-Ramanujan Journal*

case of modular elliptic curves with analytic rank atmost 1, by V.Kolyvagin, [Kol88]. The paper by Selmer [Sel51] has many examples of genus one curves for which the Tate-Shafarevich group has non-trivial elements. The perception of the Tate-Shafarevich group of abelian varieties comes from the first Galois cohomology of the Abelian variety defined over a number field. On the other hand it can be described as the non-trivial torsors on the abelian variety which become trivial over a local field. The Selmer group has been defined by a certain kernel at the level of first Galois cohomology and it is known that this group is finite.

In the paper [BaCh19], the aim was to study the notion of Selmer group and the Tate-Shafarevich group from the perspective of algebraic cycles. That is the authors, consider the Galois action of the absolute Galois group of a number field on the group of degree zero cycles on an abelian variety defined over a number field. Then consider the Selmer and the Tate-Shafarevich group associated to this group of degree zero cycles on the abelian variety by considering the kernel at the level of first Galois cohomology of this particular Galois module.

There are certain things known about the group of degree zero cycles on a smooth projective variety over the algebraic closure of a number field. One is the Mumford-Roĭtman argument [Mum68],[Roi72] about Chow schemes which says that the natural map from the symmetric power of an abelian variety to the Chow group has fibers given by a countable union of Zariski closed subsets in the symmetric power. This result enables us to give a scheme theoretic structure on the first Galois cohomology of the group of degree zero cycles on the abelian variety. Next, there is the famous theorem due to Roĭtman, [Roi80], which says that the torsion subgroup of the group of degree zero cycles on an abelian variety and the torsion subgroup on the abelian variety are isomorphic. This leads us to study of n-divisibility of the group of the degree zero cycles defined over the number field from a cohomological perspective. The main result of [BaCh19] is:

Theorem 1.1. *Let A denote an abelian variety defined over a number field K. Let $A_0(A)$ denote the group of degree zero cycles on the abelian variety. Let G be the absolute Galois group of automorphisms of $\bar{K}$ fixing K. Let $A_0(A)(K)$ denote the group of G-fixed elements of $A_0(A)$. Then the group $A_0(A)(K)/nA_0(A)(K)$ is finite.*

The importance of this result from the perspective of algebraic cycles lies in the Bloch-Beinlinson's conjecture on the albanese kernel which says that the kernel of the albanese map from the group of degree zero cycles on a smooth projective variety over $\bar{\mathbb{Q}}$ to the albanese variety has trivial kernel. It is known that this restriction on the ground field is sharp. That is, if we consider an one variable transcendental extension of the field $\bar{\mathbb{Q}}$, then over this field there are varieties for which the albanese kernel is non-trivial (see [GoGu13],[GGP04]). From the above result we can only say that the quotient $T(A(K))/nT(A(K))$ of the Albanese kernel (denoted by $T(A)$) for an abelian variety A is finite. Here n-is a positive integer and $A(K)$ denote the group of K-points on A. So it is worth studying the Tate-Shafarevich group and the Selmer group of the albanese kernel.

Here we have two constructions: one is the link between divisibility of class groups in a family with that of the Picard group of a hyperelliptic surface. On the other hand we can consider the Selmer group and the Tate-Shafarevich group of the Chow group of degree zero cycles on the hyperelliptic surface. A natural question is: What is the connection between n-divisibility of the Selmer group with that of the class group of the number fields in the above mentioned family?

The paper is organized as follows: in the second and third section we recall the results and techniques used in [BaCh19],[BaHo19] and then in the fourth section we attempt to connect these two techniques by answering the question posed in the last paragraph.

Acknowledgements: K. Banerjee and A. Hoque thanks the hospitality of Harish-Chandra Research Institute, India, for hosting this project. K.Banerjee was funded by DAE, Govt. of India, for this project and A. Hoque is supported by SERB N-PDF (PDF/2017/001958), Govt. of India.

2. Mumford-Roĭtman argument on Chow schemes and relative Picard schemes

For a smooth, projective scheme X, let D denote a Weil divisor on it. For a flat morphism $X \to B$ of projective schemes, we consider the Chow scheme, $C^1_d(X/B)$ of relative divisors, that is co-dimension one subschemes of $X \to B$ of degree d, that is

$$C^1_d(X/B) = \{(D_b, b) | \mathrm{Supp}(D_b) \subset X_b, \deg(D_b) = d\}.$$

Then there is a natural map $C^1_d(X_b) \to \mathrm{Pic}(X_b)$ associating to a D in its divisor class $[D]$. In this set up, we consider the following:

$$\mathcal{Z} := \{(b, D_b) | [D_b] = 0 \in \mathrm{Pic}(X_b)\}.$$

The proof of the following theorem is based on the idea introduced by Mumford in [Mum68]. This idea had been elaborated by Roĭtman in [Roi71] and Voisin in [Voi12]. This idea had also been used in [BaGu].

Theorem 2.1. *$\mathcal{Z}$ is a countable union of Zariski closed subsets in $C^1_d(X/B)$.*

Proof. Assume that the relation $D_b = D_b^+ - D_b^-$ is rationally equivalent to zero. This means that there exists a map $f : \mathbb{P}^1 \to C^1_{d,d}(X_b)$ such that

$$f(0) = D_b^+ + \gamma \text{ and } f(\infty) = D_b^- + \gamma,$$

where γ is a positive divisor on X_b. In other words, we have the following map:

$$ev : Hom^v(\mathbb{P}^1_k, C^1_d(X/B)) \to C^1_d(X/B) \times C^1_d(X/B),$$

given by $f \mapsto (f(0), f(\infty))$ and image of f is contained in $C^1_{d,d}(X_b)$.

Let us denote $C^1_d(X/B)$ by $C^1_d(X)$ for simplicity.

We now consider the subscheme $U_{v,d}(X)$ of $B \times Hom^v(\mathbb{P}^1_k, C^1_d(X))$ consisting of the pairs (b, f) such that image of f is contained in $C^1_d(X_b)$ (such a universal family exists, for example see [Kol88, Theorem 1.4]). This gives a morphism from $U_{v,d}(X)$ to $B \times C^1_{d,d}(X)$ defined by

$$(b, f) \mapsto (b, f(0), f(\infty)).$$

Again, we consider the closed subscheme $\mathcal{V}_{d,d}$ of $B \times C^1_{d,d}(X)$ given by (b, z_1, z_2), where $(z_1, z_2) \in C^1_{d,d}(X_b)$. Suppose that the map from $\mathcal{V}_{d,u,d,u}$ to $\mathcal{V}_{d+u,d+u}$ is given by

$$(A, C, B, D) \mapsto (A + C, C, B + D, D).$$

Then one writes the fiber product $\mathcal{V}$ of $U_{v,d}(X)$ and $\mathcal{V}_{d,u,d,u}$ over $\mathcal{V}_{d+u,d+u}$. If we consider the projection from $\mathcal{V}$ to $B \times C^1_{d,d}(X)$, then we observe that A and B are supported as well as rationally equivalent on X_b. Conversely, if A and B are supported as well as rationally equivalent on X_b, then one gets the map

$$f : \mathbb{P}^1 \to C^1_{d+u,u,d+u,u}(X_b)$$

of some degree v satisfying

$$f(0) = (A + C, C) \text{ and } f(\infty) = (B + D, D),$$

where C and D are supported on X_b. This implies that the image of the projection from $\mathcal{V}$ to $B \times C^1_{d,d}(X)$ is a quasi-projective subscheme $W_d^{u,v}$ consisting of the tuples (b, A, B) such that A and B are supported on X_b, and that there exists a map

$$f : \mathbb{P}^1_k \to C^1_{d+u,u}(X_b)$$

such that $f(0) = (A + C, C)$ and $f(\infty) = (B + D, D)$. Here f is of degree v, and C, D are supported on X_b and they are of co-dimension 1 and degree u cycles. This shows that $W_d = \cup_{u,v} W_d^{u,v}$. We now prove that the Zariski closure of $W_d^{u,v}$ is in W_d for each u and v. For this, we prove the following:

$$W_d^{u,v} = pr_{1,2}(\widetilde{s}^{-1}(W^{0,v}_{d+u} \times W^{0,v}_u)),$$

where

$$\widetilde{s} : B \times C^1_{d,d,u,u}(X) \to B \times C^1_{d+u,d+u,u,u}(X)$$

defined by

$$\widetilde{s}(b, A, B, C, D) = (b, A + C, B + D, C, D).$$

We assume $(b, A, B, C, D) \in B \times C^1_{d,d,u,u}(X)$ in such a way that $\widetilde{s}(b, A, B, C, D) \in W^{0,v}_{d+u} \times W^{0,v}_u$. This implies that there exists an element $(b, g) \in B \times \mathrm{Hom}^v(\mathbb{P}^1_k, C^p_{d+u}(X))$ and an element $(b, h) \in \mathrm{Hom}^v(\mathbb{P}^1_k, C^p_u(X))$ satisfying

$$g(0) = A + C,\ g(\infty) = B + D \text{ and } h(0) = C, h(\infty) = D$$

as well as the image of g and h are contained in $C^1_{d+u}(X_b)$ and $C^1_u(X_b)$ respectively.

Also if $f = g \times h$ then $f \in \mathrm{Hom}^v(\mathbb{P}^1_k, C^p_{d+u,u}(X))$ such that the image of f is contained in $C^1_{d+u,u}(X_b)$ as well as it satisfies the following:

$$f(0) = (A + C, C) \text{ and } (f(\infty)) = (B + D, D).$$

This shows that $(b, A, B) \in W^d_{u,v}$.

On the other hand, we assume that $(b, A, B) \in W^d_{u,v}$. Then there exists $f \in \mathrm{Hom}^v(\mathbb{P}^1_k, C^1_{d+u,u}(X_b))$ such that

$$f(0) = (A + C, C) \text{ and } f(\infty) = (B + D, D),$$

and image of f is contained in the Chow scheme of X_b.

We now compose f with the projections to $C^1_{d+u}(X_b)$ and to $C^1_u(X_b)$ to get a map $g \in \mathrm{Hom}^v(\mathbb{P}^1_k, C^1_{d+u}(X))$ and a map $h \in \mathrm{Hom}^v(\mathbb{P}^1_k, C^1_u(X))$ satisfying

$$g(0) = A + C,\ g(\infty) = B + D$$

and

$$h(0) = C,\ h(\infty) = D.$$

Also, the image of g and h are contained in the respective Chow schemes of the fibers X_b. Therefore, we have

$$W_d = pr_{1,2}(\widetilde{s}^{-1}(W_{d+u} \times W_u)).$$

We are now in a position to prove that the closure of $W_d^{0,v}$ is contained in W_d. Let (b, A, B) be a closed point in the closure of $W_d^{0,v}$. Let W be an irreducible component of $W_d^{0,v}$ whose closure contains (b, A, B). Assume that U is an affine neighborhood of (b, A, B) such that $U \cap W$ is non-empty. Then there is an irreducible curve C in U passing through (b, A, B). Suppose that $\bar{C}$ is the Zariski closure of C in $\overline{W}$. The map

$$e : U_{v,d}(X) \subset B \times \mathrm{Hom}^v(\mathbb{P}^1_k, C^1_d(X)) \to C^1_{d,d}(X)$$

given by

$$(b, f) \mapsto (b, f(0), f(\infty))$$

is regular and $W_d^{0,v}$ is its image. We now choose a curve T in $U_{v,d}(X)$ such that the closure of $e(T)$ is $\bar{C}$. Let $\widetilde{T}$ be denote the normalization of the Zariski closure of T, and $\widetilde{T_0}$ be the pre-image of T in this normalization. Then the regular morphism $\widetilde{T_0} \to T \to \bar{C}$ extends to a regular morphism from $\widetilde{T}$ to $\bar{C}$. If (b, f) is a pre-image of (b, A, B), then $f(0) = A$, $f(\infty) = B$ and the image of f is contained in $C_d^p(X_b)$ by the definition of $U_{v,d}(X)$. Therefore, A and B are rationally equivalent. This completes the proof.

As a consequence, one gets the following:

Corollary 2.2. *The collection*

$$\mathcal{Z}_d := \{(b, D_b) | n[D_b] = 0 \in \mathrm{Pic}(X_b)\}$$

is a countable union of Zariski closed subsets in the scheme $C_d^1(X/B)$.

2.A. Mumford-Roĭtman arguments and monodromy representation

Following an idea using monodromy due to Voisin [Voi02, Chapter 3] and the above mentioned argument due to Mumford and Roĭtman, we have the following theorem:

Theorem 2.3. *The cardinality of the subgroup of torsions in* X_b *coming from the fibration* $\mathcal{Z}_{i\mathbb{C},U} \to U_{\mathbb{C}}$ *for each* $b \in U$ *remains constant and they vary in a family.*

Proof. For a proof see [BaHo19, Thoerem 3.1].

We now consider a smooth projective curve C over an algebraically closed field $K \subset \mathbb{C}$ in the projective plane $\mathbb{P}^2$ over K. Let U be an affine piece of C. That is, U is C minus finitely many points, viz. $P_1, \cdots, P_m$. Consider the following localization exact sequence of Picard groups

$$\oplus_i \mathbb{Z}[P_i] \to \mathrm{Pic}(C) \to \mathrm{Pic}(U) \to 0.$$

Then the set of all torsion points in $\mathrm{Pic}(U)$ gives rise to elements of $\mathrm{Pic}(C)$ of the form nz such that

$$nz = \sum_i n_i P_i$$

where $P_1, \cdots, P_m$ are the finite number of points that are deleted. As before, we consider a fibration of smooth projective schemes $X \to B$ over $\bar{\mathbb{Q}}$, where X is a surface embedded in $\mathbb{P}^3$ such that each fiber X_b is contained in a projective plane $\mathbb{P}^2$ over $\bar{\mathbb{Q}}$ and B is an algebraic curve. Suppose that the degree of the algebraic curve X_b remains constant over a Zariski open set U in B. For an affine piece U_b of the algebraic curve X_b, we consider the following:

$$\mathcal{P} := \{(x, b) | x \in X_b \setminus U_b\} \to U.$$

By the above assumption, this a finite-to-one map from $\mathcal{P}$ to U and the degree of this map is constant. For given any $b \in U$, let us suppose the fiber $\mathcal{P}_b$ contains the points $P_{1b}, \cdots, P_{mb}$. We define the set:

$$\mathcal{Z}_d = \{(b, z) | \mathrm{Supp}(z) \subset X_b, nz = \sum_i n_i P_{ib}\} \to U.$$

Then as a conseqeunce of Theorem 2.1 one gets the following result.

Corollary 2.4. *$\mathcal{Z}_d$ is a countable union of Zariski closed subsets in the ambient relative Chow scheme $C_d^1(X_U/U)$, where $X_U \to U$ is the pullback of the family $X \to B$ to U.*

This corollary along with the Theorem 2.3 gives the following:

Corollary 2.5. *The cardinality of the set of z in $\mathcal{Z}_{ib}$ for $b \in U$ such that*

$$nz = \sum_i n_i P_{ib}$$

for points $P_{ib} \in X_b$ is constant as b varies over U.

These points on $\mathrm{Pic}(X_b)$ correspond to the torsion elements in $\mathrm{Pic}(U_b)$, where U_b is the open complement of X_b obtained from X_b by deleting the points $P_{1b}, \cdots, P_{mb}$.

2.B. Example of hyperelliptic surfaces

In this section, we will show that certain algebraic surfaces have n-torsion elements in the Picard group. We begin section with the algebraic surface defined by

$$y^2 = t^2q^2 - z^n$$

over $\mathbb{Q}$. Its co-ordinate ring is given by

$$\mathbb{Q}[y,t,z]/(y^2 - t^2q^2 + z^n).$$

We now consider the maximal ideal $(t-m, z-\ell)$, for some algebraic numbers m, ℓ, in the polynomial ring $\mathbb{Q}[t,z]$. We also consider the map

$$\mathbb{Q}[t,z] \to \mathbb{Q}[y,t,z]/(y^2 - t^2q^2 + z^n)$$

which is defined by

$$t \mapsto t, z \mapsto z$$

and the map $\mathbb{Q}[t,z] \to \mathbb{Q}$ which is given by

$$f(t,z) \mapsto f(m,\ell).$$

Then the tensor product

$$\mathbb{Q}[y,t,z]/(y^2 - t^2q^2 + z^n) \otimes_{\mathbb{Q}[t,z]} \mathbb{Q}$$

is given by $\mathbb{Q}[y]/(y^2 - m^2q^2 + \ell^n)$. Further, if the polynomial $p(y) := y^2 - m^2q^2 + \ell^n$ is irreducible over $\mathbb{Q}$, then the above co-ordinate ring is isomorphic to L, where L is the imaginary quadratic extension of $\mathbb{Q}$ given by adjoining a root of $p(y)$. Therefore if we consider the family

$$\mathbb{Z}[y,t,z]/(y^2 - t^2q^2 + z^n) \to \mathbb{Z}[t,z],$$

then the normalizations of the fibers are the ring of integers of

$$\mathbb{Q}(\sqrt{m^2q^2 - \ell^n})$$

Let us consider an affine surface S fibered over $\mathring{A}^2_{\mathbb{Q}}$ as mentioned in the beginning of this section. Let the pullback of the fibration over $\mathring{A}^2_{\mathbb{Z}}$, be $S_{\mathbb{Z}} \to \mathring{A}^2_{\mathbb{Z}}$. Then the family of mormalizations to $S_{\mathbb{Z}}$ is the family of ring of integers $\mathcal{O}(\sqrt{m^2q^2 - \ell^n})$. For the convenience of notation, let us continues to denote this family as $S_{\mathbb{Z}}$. Consider the Zariski closure of S in $\mathbb{P}^3_{\mathbb{Q}}$ and the Zariski closure of the family $S_{\mathbb{Z}} \to \mathring{A}^2_{\mathbb{Z}}$ in $\mathbb{P}^3_{\mathbb{Z}}$. We denote it by $\bar{S}_{\mathbb{Z}}$. We also consider the Chow scheme

$$C_d^1(\bar{S}_{\mathbb{Z}}/\mathbb{P}^2_{\mathbb{Z}})$$

and the subset

$$\mathcal{Z}_d := \{(z,b)|\mathrm{Supp}(z) \subset X_b, [z] = \sum_i n_i[P_{ib}] \in \mathrm{Pic}(S_{\mathbb{Z},b})\},$$

where $P_{1b}, \cdots, P_{mb}$ are the points in the complement of $S_{\mathbb{Z},b}$ inside the Zariski closure $\bar{S}_{\mathbb{Z},b}$. Then by Theorem 2.1, we get the following result.

Proposition 2.6. *The set $\mathcal{Z}_d$ is a countable union of Zariski closed subsets in the Chow scheme.*

Applying the same argument as in Corollary 2.5, we see that there exists an irreducible Zariski closed subset $\mathcal{Z}_i$ inside the relative Picard scheme $\mathrm{Pic}(\overline{S_{\mathbb{Z}U}} \to U)$, where U is Zariski open in $\mathring{A}^2_{\mathbb{Z}}$, such that the complexification of $\mathcal{Z}_{i,\mathbb{C}}$ maps dominantly onto $U_{\mathbb{C}}$ as well as the number of points in the fiber of this map is constant. Therefore, one gets the following:

Theorem 2.7. *The cardinality of a certain subgroup of* $\mathrm{Pic}(S_{\mathbb{Z},b})$ *which is nothing but the class group of the quadratic field* $\mathbb{Q}(\sqrt{m^2q^2 - \ell^n})$ *for some fixed integers m and ℓ, remains constant as b varies over U.*

This concludes that given an element of order n in $\mathrm{Pic}(S_{\mathbb{Z},b})$, one can find an element of the same order in $\mathrm{Pic}(S_{\mathbb{Z},b'})$ for some $b' \in U$ which is different from b.

3. Tate-Shafarevich group of the Chow group of an abelian variety

Let K be a number field and let $\overline{K}$ denote its algebraic closure. Let A be an abelian variety defined over K. Then we have a natural Galois action of the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$. This action induces further an action on the Chow group of zero cycles on the abelian variety A. Here the Chow group is the free abelian group generated by closed points on $A(\bar{K})$ modulo the rational equivalence. We denote this group by $\mathrm{CH}_0(A)$.

Consider the continuous functions f from $G = \mathrm{Gal}(\bar{K}/K)$ to $\mathrm{CH}_0(A)$ satisfying the property that

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau)\ .$$

The set of all such functions form a group denoted by $Z^1(G, \mathrm{CH}_0(A))$. Let us consider the subgroup of $Z^1(G, \mathrm{CH}_0(A))$ consisting of elements f such that

$$f(\sigma) = \sigma.x - x$$

where x some element in the group $\mathrm{CH}_0(A)$. Denote this subgroup by $B^1(G, \mathrm{CH}_0(A))$. Then we define the quotient

$$Z^1(G, \mathrm{CH}_0(A))/B^1(G, \mathrm{CH}_0(A))$$

as

$$H^1(G, \mathrm{CH}_0(A))\ .$$

Let $A_0(A)$ denote the subgroup of degree zero cycles modulo rational equivalence in $\mathrm{CH}_0(A)$. We consider as previous the Galois cohomology

$$H^1(G, A_0(A))$$

of the group $A_0(A)$.

We observe that there is a natural homomorphism of abelian groups from $A_0(A)$ to A. Then by functoriality of group cohomology we have that this homomorphism descends to a homomorphism of Galois cohomology groups of the corresponding Galois modules:

$$H^1(G, A_0(A)) \to H^1(G, A)$$

The map from $A_0(A)$ to A is denoted by alb, the albanese map. We denote the map from $H^1(G, A_0(A))$ to $H^1(G, A)$ as alb. We are interested in understanding the structure of the group $H^1(G, A_0(A))$. Consider the natural map from $\mathrm{Sym}^n A$ to $A_0(A)$, which sends an unordered n-tuple $\{P_1, \cdots, P_n\}$ of $\bar{K}$ points on A to the cycle class

$$\sum_{i=1}^{n} [P_i - P_0] \ ,$$

where P_0 is a fixed K-point on A.

Now consider the fact that the group $H^1(G, A_0(A))$ is actually isomorphic to the colimit of Galois cohomology of finite groups

$$H^1(\mathrm{Gal}(L/K), A_0(A_L))$$

Here L/K is a finite Galois extension and A_L is the collection of L-points on A. Since G is a profinite group, the range of any function η from G to $A_0(A)$ is finite. Consider Z_l to be the collection of all maps η from G to $A_0(A)$ such that η factors through $\mathrm{Sym}^l A \times \mathrm{Sym}^l A$ (this can be achieved by decomposing a zero cycle into positive and negative parts). That is we identify the maps η, factoring through $\mathrm{Sym}^l A \times \mathrm{Sym}^l A$, with its image inside $\mathrm{Sym}^l A \times \mathrm{Sym}^l A$. There exists a normal subgroup of G of finite index, call it N, such that η is factoring through G/N. On the other hand suppose that we have a collection of points on $\mathrm{Sym}^l A \times \mathrm{Sym}^l A$. Then we can define a map from G/N to $\mathrm{Sym}^l A \times \mathrm{Sym}^l A$ by assigning the cosets of N to this finite collection of points of $\mathrm{Sym}^l A \times \mathrm{Sym}^l A$. Such a map will be continuous from G/N to $\mathrm{Sym}^l A \times \mathrm{Sym}^l A$ equipped with discrete topology, as G/N is finite. Since the quotient map from G To G/N is continuous we have that the map from G to $\mathrm{Sym}^l A \times \mathrm{Sym}^l A$ is continuous. But these maps are non-canonical as its depends on the choice of the points and their assignments to the left cosets of N. Now consider the relation that defines $Z^1(G, A_0(A))$,

$$\eta(\sigma\tau) = \eta(\sigma) + \sigma\eta(\tau) \ .$$

Since this relation happens on $A_0(A)$ we have that the cycles

$$\eta(\sigma\tau)$$

is rationally equivalent to

$$\eta(\sigma) + \sigma\eta(\tau) \ .$$

This means that there exists a map from $\mathbb{P}^1_{\bar{K}}$ to $\mathrm{Sym}^d A$, and a positive zero cycle B such that

$$f(0) = \eta(\sigma\tau) + B, \quad f(\infty) = \eta(\sigma) + \sigma\eta(\tau) + B \ .$$

By the theorem of Roitman [Roi71] the collection of all such η, such that

$$\eta(\sigma\tau)$$

is rationally equivalent to

$$\eta(\sigma) + \sigma\eta(\tau)$$

is a countable union of Zariski closed subsets inside the symmetric power $\mathrm{Sym}^l A \times \mathrm{Sym}^l A$ such that range of η is contained in $\mathrm{Sym}^l A \times \mathrm{Sym}^l A$. So following [Roi71] we have:

Theorem 3.1. *The collection of all η contained in $Z_{l,l}$ such that*

$$\eta(\sigma\tau)$$

is rationally equivalent to

$$\eta(\sigma) + \sigma\eta(\tau)$$

is a countable union of Zariski closed subsets inside $\mathrm{Sym}^l A \times \mathrm{Sym}^l A$ *denoted by* Z^1_l.

Proof. For details of the proof see [BaCh19, Theorem 2.1].

Similarly we can prove that the collection of η in Z_l such that $\eta(\sigma)$ is rationally equivalent to $\sigma.z - z$ (for a fixed zero cycle z) is a countable union of Zariski closed subsets in Z_l^1. Call it B_l^1.

Therefore we can conclude from the above theorem that:

Theorem 3.2. *The group $H^1(G, A_0(A))$ admits a surjective map from the countable union $\cup_l Z_l^1$ such that $\cup_l B_l^1$ is mapped to a point under this surjective map.*

Now we further study the property of this map:

$$Z_l^1 \to H^1(G, A_0(A))$$

Consider an element η in the set Z_l^1. Then for every σ, τ we have

$$\eta(\sigma\tau) = \eta(\sigma) + \sigma\eta(\tau) \ .$$

This equality happens in $A_0(A)$. So consider the tuples

$$(\eta, f, B) \in Z_l \times \mathrm{Hom}^v(\mathbb{P}^1, \mathrm{Sym}^{n+u,n+u} A) \times \mathrm{Sym}^u B$$

such that the following equations are satisfied:

$$f(0) = \eta(\sigma\tau) + B$$

$$f(\infty) = \eta(\sigma) + \sigma\eta(\tau) + B.$$

So if we denote the above quasiprojective variety by $\mathcal{V}$ and consider the projection map from $\mathcal{V}$ to $\mathrm{Hom}^v(\mathbb{P}^1, \mathrm{Sym}^{n+u,n+u} A)$, then it is a $\mathbb{P}^1$-bundle. This is because it is the pull-back of the $\mathbb{P}^1$-bundle given by

$$\{(x, f) | x \in \mathrm{im}(f)\} \subset \mathrm{Sym}^{n+u,n+u} A \times \mathrm{Hom}^v(\mathbb{P}^1, \mathrm{Sym}^{n+u,n+u} A) \ .$$

So over Z_l^1 we have the universal variety $\mathcal{U}_{l,m}^1$ consisting of tuples (η, f, B) such that the above equations are satisfied and it has the structure of a rationally connected fibration over the Hom-scheme. Therefore if we consider the finite map from A^{2l} to $\mathrm{Sym}^l A \times \mathrm{Sym}^l A$, the degree of this finite map is $(l!)^2$. The pullback of Z_l^1 under this map is a finite branched cover of Z_l^1 denoted by $\widetilde{Z_l^1}$. Correspodningly we have the pull-back of the universal family $\mathcal{U}_l^1$ over $\widetilde{Z_l^1}$ denoted by $\widetilde{\mathcal{U}_l^1}$. This is a family of branched covers of $\mathbb{P}^1$ over the Hom-scheme.

3.A. The group cohomology of the group of degree zero cycles on A

Let $A_0(A)$ denote the group of degree zero cycles or the zero cycles algebraically equivalent to zero on A. Then there is a natural homomorphism from A^n to $A_0(A)$ Given by

$$\sum_i P_i \mapsto \sum_i [P_i - n0]$$

here 0 is the neutral element of the abelian variety A. Then the map from A^n to $A_0(A)$ induces by functoriality a natural homomorphism from $H^1(G, A^n)$ to $H^1(G, A_0(A))$. Consider the natural map from A^n to A^{n+1} given by

$$(P_1, \cdots, P_n) \mapsto (P_1, \cdots, P_n, 0)$$

Then this map gives rise to the homomorphism from $H^1(G, A^n)$ to $H^1(G, A^{n+1})$ and the homomorphism

$$\theta_n : H^1(G, A^n) \to H^1(G, A_0(A))$$

factors through the above map

$$H^1(G, A^n) \mapsto H^1(G, A^{n+1}) .$$

Hence we have a natural homomorphism from the colimit of the groups

$$H^1(G, A^n)$$

to

$$H^1(G, A_0(A))$$

denoted by θ. So we have

$$\theta : \varinjlim H^1(G, A^n) \to H^1(G, A_0(A)) .$$

Now for each n we have the group law from A^n to A given by

$$(a_1, \cdots, a_n) \mapsto \sum_i a_i$$

This map gives rise to a natural map from $H^1(G, A^n)$ to $H^1(G, A)$. Note that this map factors through the homomorphism

$$H^1(G, A^n) \to H^1(G, A^{n+1})$$

Therefore we have a homomorphism from

$$\varinjlim H^1(G, A^n) \to H^1(G, A) .$$

Since the map $H^1(G, A^n)$ to $H^1(G, A_0(A))$ factors through the map

$$H^1(G, A) \to H^1(G, A_0(A))$$

we have that the map

$$\varinjlim H^1(G, A^n) \to H^1(G, A_0(A))$$

factors through the map

$$H^1(G, A) \to H^1(G, A_0(A)) .$$

Now the group on the left is the the Weil-Chatelet group of the respective A, which consists of the equivalence classes of principal homogeneous spaces over A. This group is denoted by $WC(A)$. Under the identification

$$H^1(G, A) \cong WC(A)$$

we have that

$$\theta : WC(A) \to H^1(G, A_0(A)) .$$

It is natural to consider when this map is injective and surjective.

Now due to the famous result on torsions by Roĭtman [Roi80] in $A_0(A)$, we know that this group of torsions is isomorphic to the group of torsions in A. So we expect a similar result when we consider the group cohomology $H^1(G, A)$ and $H^1(G, A_0(A))$.

Theorem 3.3. *The kernel of the map $H^1(G, A)[n] \to H^1(G, A_0(A))[n]$ is isomorphic to the group*

$$A_0(A)(K)/nA_0(A)(K) .$$

Proof. For a proof see [BaCh19, Theorem 2.4].

3.B. Tate-Shafarevich and Selmer group of $A_0(A)$ and their properties

Consider the exact sequence

$$0 \to A_0(A)(K)/nA_0(A)(K) \to H^1(G, A_0(A)[n]) \to H^1(G, A_0(A))[n] \to 0 \,.$$

Now we consider a place v of K and consider the complection of K at v, denote this completion by K_v. Then consider the algebraic closure $\bar{K}_v$ of K_v and embed $\bar{K}$ into $\bar{K}_v$. This embedding gives us an injection of the Galois group $\mathrm{Gal}(\bar{K}_v/K_v)$ into $\mathrm{Gal}(\bar{K}/K)$. Considering the Galois cohomology, we have a homomorphism from

$$H^1(\mathrm{Gal}(\bar{K}/K), A_0(A(\bar{K})) \to H^1(\mathrm{Gal}(\bar{K}_v/K_v), A_0(A(\bar{K}_v))) \,.$$

We write the groups $\mathrm{Gal}(\bar{K}/K), \mathrm{Gal}(K_v/K_v)$ as G, G_v for simplicity. Then we have the following commutative diagrams:

$$\begin{array}{ccc} A_0(A)(K)/nA_0(A)(K) & \longrightarrow & H^1(G, A_0(A)[n]) \\ \downarrow & & \downarrow \\ A_0(A)(K_v))/nA_0(A)(K_v)) & \longrightarrow & H^1(G_v, A_0(A_v)[n]) \end{array}$$

$$\begin{array}{ccc} H^1(G, A_0(A)[n]) & \longrightarrow & H^1(G, A_0(A))[n] \\ \downarrow & & \downarrow \\ H^1(G_v, A_0(A_v)[n]) & \longrightarrow & H^1(G_v, A_0(A_v))[n] \end{array}$$

Consider the map

$$H^1(G, A_0(A)[n]) \to \prod_v H^1(G_v, A_0(A_v)).$$

Note: *The kernel of this map will be called the Selmer group associated to the map $z \mapsto nz$, denoted by $S^n(A_0(A)/K)$. And, the kernel of the map $H^1(G, A_0(A)) \to \prod_v H^1(G_v, A_0(A_v))$ will be called the Tate-Shafarevich group, denoted by $TS(A_0(A)/K)$.*

Now consider the commutative diagram:

$$\begin{array}{ccc} H^1(G, A[n]) & \longrightarrow & \prod_v H^1(G_v, A_v)[n] \\ \downarrow & & \downarrow \\ H^1(G, A_0(A)[n]) & \longrightarrow & \prod_v H^1(G_v, A_0(A_v))[n] \end{array}$$

Now by Roĭtman's theorem as in [Roi80], the groups $A[n]$ and $A_0(A)[n]$ are isomorphic, as Galois modules (after a possible finite extension of the given number field). This fact is explained in details in the next section 4. Therefore the group cohomologies are isomorphic. So the left vertical arrow in the above diagram is an isomorphism. Suppose that we have an element in $S^n(A/K)$, then by the commutativity of the above diagram we have that the image of the element under the left vertical homomorphism is in $S^n(A_0(A)/K)$. Now we recall the following theorem proved in [BaCh19, Theorem 3.3].

Theorem 3.4. *The group $S^n(A_0(A)/K)$ is finite and hence*

$$A_0(A)(K)/nA_0(A)(K)$$

is finite.

4. Divisibility problem of class groups and Selmer groups

Considering the group of n-torsion elements in the Picard variety of the hyperelliptic surface S, say $\mathrm{Pic}^0(S)$, we have a bijection of this group with the n-torsion subgroup of $\mathrm{Alb}(S)$, the albanese variety of S. This isomrophism is defined over a finite extension of the ground field. On the other hand by the Roĭtman's theorem in [Roi80], the n-torsions in $A_0(S)$ corresponds to n-torsions' in $\mathrm{Alb}(S)$. Suppose that after a finite extension of the ground field, say K, we have a K-rational point on S. Call it P_0. Let g be an element in the absolute Galois group of K. Then we have a functorial morphism:

$$g_* : \mathrm{Sym}^n S \to \mathrm{Sym}^n S$$

given by

$$P_1 + \cdots + P_n \mapsto g(P_1) + \cdots + g(P_n)$$

where $P_1 + \cdots + P_n$ denote the unordered n-tuple consisting of closed points $P_1, \cdots, P_n$ in S. Consider the natural map

$$\mathrm{Sym}^n S \to A_0(S)$$

given by

$$P_1 + \cdots + P_n \mapsto [P_1 + \cdots + P_n - nP_0]$$

The right hand side above denote the cycles class corresponding to the cycle

$$\sum_{i=1}^{n} P_i - nP_0 \ .$$

Note that the above map gives rise to the formula:

$$g_*([P_1 + \cdots + P_n - nP_0]) = [g_*(P_1) + \cdots + g_*(P_n) - ng_*(P_0)]$$

for g an element in the Galois group. Therefore we have

$$g_* : A_0(S) \to A_0(S)$$

composing this map with the albanese map we have

$$A_0(S) \to A_0(S) \to \mathrm{Alb}(S) \ .$$

If we compose the map $S \to A_0(S)$, with the above map then we have P_0 mapping to zero in $\mathrm{Alb}(S)$. Hence we have a unique morphism of abelian varieties (denote it again by g_*):

$$\mathrm{Alb}(S) \to \mathrm{Alb}(S)$$

such that we have

$$\mathrm{alb}_S \circ g_* = g_* \circ \mathrm{alb}_S$$

Here alb_S is the albanese map. This gives that the map

$$A_0(S) \to \mathrm{Alb}(S)$$

is a map of Galois modules (ensured by the universal property of the albanese variety), provided that S has a K-rational point. Let for an abelian group A, the n-torsions are denoted by $A[n]$. So we have the isomorphisms of Galois modules

$$\mathrm{Pic}^0(S)[n] \to \mathrm{Alb}(S)[n] \to A_0(S)[n]$$

where the fist one comes from Autoduality of Picard and Albanese varieties and the second one is the isomorphism coming from Roĭtman's theorem described above. Then we have an isomorphism between

$$H^1(G, \mathrm{Pic}^0(S)[n])$$

and

$$H^1(G, A_0(S)[n]) \ .$$

Therefore considering the Tate-Shafarevich groups we have an isomorphism

$$TS(A_0(S)[n]/K) \cong TS(\mathrm{Pic}^0(S)[n]/K)$$

where TS denote the Tate-Shafarevich group of n-torsions of the corresponding group. Now suppose that we start from an element of order n on $A_0(S)$, this will correspond to an element of order n in the Selmer group in $\mathrm{Pic}^0(S)$. Now consider a fibration of this surface over $\mathbb{P}^1_{\bar{\mathbb{Q}}}$. Then for a closed point $b \in \mathbb{P}^1_{\bar{\mathbb{Q}}}$, we have the restriction homomorphism

$$\mathrm{Pic}^0(S) \to \mathrm{Pic}^0(S_b)$$

So considering both $\mathrm{Pic}^0(S), \mathrm{Pic}^0(S_b)$ as Galois modules we have a map of Galois cohomology

$$H^1(G, \mathrm{Pic}^0(S)) \to H^1(G, \mathrm{Pic}^0(S_b))$$

Thus we have the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Pic}^0(S)(K)/n\mathrm{Pic}^0(S)(K) & \longrightarrow & H^1(G, \mathrm{Pic}^0(S)[n]) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(S_b)(K)/n\mathrm{Pic}^0(S_b)(K) & \longrightarrow & H^1(G, \mathrm{Pic}^0(S_b)[n]) \end{array}$$

Also we have an analogue of the above diagram at the level of local fields that is K_v, where v is a place of K. Therefore functorially we have the homomorphism from

$$TS(\mathrm{Pic}^0(S)/K) \to TS(\mathrm{Pic}^0(S_b)/K)$$

and

$$S^n(\mathrm{Pic}^0(S)/K) \to S^n(\mathrm{Pic}^0(S_b)/K).$$

Composing this map with the map

$$S^n(A_0(S)/K) \to S^n(\mathrm{Pic}^0(S)/K)$$

we have established a homomorphism from $S^n(A_0(S)/K)$ to $S^n(\mathrm{Pic}^0(S_b)/K)$ and corresponding homomorphism

$$TS(A_0(S)/K) \to TS(\mathrm{Pic}^0(S_b)/K) \ .$$

By a diagram chase we have the following diagrams

$$\begin{array}{ccc} A_0(S)(K)/nA_0(S)(K) & \longrightarrow & S^n(A_0(S)/K) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(S_b)(K)/n\mathrm{Pic}^0(S_b)(K) & \longrightarrow & S^n(\mathrm{Pic}^0(S_b)) \end{array}$$

$$\begin{array}{ccc} S^n(A_0(S)/K) & \longrightarrow & TS^n(A_0(S)/K) \\ \downarrow & & \downarrow \\ S^n(\mathrm{Pic}^0(S_b)) & \longrightarrow & TS^n(\mathrm{Pic}^0(S_b)/K) \end{array}$$

Therefore the elements of order n in the Selmer or the Tate-Shafarevich group of $A_0(S)$ corresponds to an element of order n in the Selmer or the Tate-Shfarevich group respectively of $\mathrm{Pic}^0(S_b)$. So the n-divisibility of the Selmer or the Tate-Shafarevich group of $A_0(S)$ corresponds to n-divisibility of the Selmer or the Tate-Shafarevich group of $\mathrm{Pic}^0(S_b)$. Now spreading out S_b over $\mathrm{Spec}(\mathbb{Z})$ and considering an affine piece of the spread we have the $\mathrm{Spec}(\mathcal{O}_b)$, where $\mathcal{O}_b$ is the ring of integers of a number field. The above construction then corresponds to the following:

Theorem 4.1. *The n-divisibility of the Tate-Shafarevich or the Selmer group of the group $A_0(S_U)$ of an affine piece S_U of the surface S corresponds to the respective n-divisibility of the Tate-Shafarevich or the Selmer group of corresponding class group of $\mathcal{O}_b$.*

References

[BaCh19] K. Banerjee and K. Chakraborty, *Tate-Shafarevich group and Selmer group constructions for Chow group of an abelian variety* , `arxiv:1906.08233`, 2019.

[BaGu] K. Banerjee and V. Guletskii, *Étale monodromy and rational equivalence for 1-cycles on cubic hypersurfaces in* $\mathbb{P}^5$, Mat. Sb. (to appear) `arXiv:1405.6430v1`.

[BaHo19] K. Banerjee and A. Hoque, *Picard group, pull back and class group*, `arxiv:1903.04210`, 2019.

[Cas62a] J. Cassels, *Arithmetic of curves of genus 1. III. Tate-Shafarevich and Selmer groups* , Proc. London Math. Soc. Third series, **12** (1962), 259–296.

[Cas62b] J. Cassels, *Arithmetic of curves of genus 1. IV. Proof of Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112.

[GoGu13] S. Gorchinsky and V. Guletskii, Non-trivial elements in the kernel of Abel-Jacobi kernels of higher dimensional varities, Adv. Math. **241** (2013), 162–191.

[GGP04] M. Green, P. Griffiths and K. Paranjape, Cycles over fields of transcendence degree one, Michigan Math. J. **52** (2004), 181–187.

[Kol88] V. Kolyvagin, *Finiteness of E(Q) and SH(E(Q)) for a subclass of Weil-Curves*, Izvestiya Akademii Nauk SSSR, Seriya Matematicheskaya, **52** (1988), 522–540, 670–671.

[LaTa58] S.Lang, J.Tate, *Principal homogeneous spaces over abelian varities*, Americal journal of Mathematics, **80** (1958), 659–684.

[Mum68] D. Mumford, *Rational equivalence for* 0*-cycles on surfaces.*, J.Math Kyoto Univ. **9** (1968), 195–204.

[Roi71] A. Roitman, Γ*-equivalence of zero dimensional cycles (Russian)*, Math. Sbornik. **86** (1971), 557–570.

[Roi72] A. Roitman, *Rational equivalence of 0-cycles*, Math USSR Sbornik, **18** (1972), 571–588.

[Roi80] A. Roitman, *The torsion of the group of 0-cycles modulo rational equivalence*, Ann. of Math. **111** (1980), 553–569.

[Rub87] K. Rubin, *Tate-Shafarevich group and L-functions of elliptic curves with complex multiplication*, Inventiones Mathematicae, **89** (1987), 527–559.

[Sel51] E. Selmer, *On the diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951), 203-362.

[Sil86] J.H.Silverman, *The Arithmetic of elliptic curves*, Springer, Berlin-Heidelberg-Newyork, 1986.

[Sha59] I. R. Shafarevich, *The group of principal homogeneous algebraic manifolds*, Dokaldy Academii Nauk SSSR, (in Russian), **124** (1959), 42–43.

[Ta58] J.Tate, *WC-groups over p-adic fields*, Seminaire Bourbaki, 1957-58, 13 Paris, Secretariat Mathematique.

[SuVoe] A.Suslin, V.Voevodsky, *Relative cycles and Chow sheaves* in: Cycles, transfers, motivic homology theories, Annals of Math studies 143, 10–86, 2000.

[Voi12] C. Voisin,*Symplectic invoultions of K*3 *surfaces act trivially on* CH_0, Documenta Mathematicae **17** (2012), 851–860.

[Voi02] C. Voisin, *Complex algebraic geometry and Hodge theory II*, Cambridge studies of Mathematics, 2002.

Kalyan Banerjee
Harish-Chandra Research Institute, HBNI
Chhatnag Road, Jhunsi
Allahabad 211 019, India
e-mail: banerjeekalyan@hri.res.in

Kalyan Chakraborty
Harish-Chandra Research Institute, HBNI
Chhatnag Road, Jhunsi
Allahabad 211 019, India
e-mail: kalyan@hri.res.in

Azizul Hoque
Harish-Chandra Research Institute, HBNI
Chhatnag Road, Jhunsi
Allahabad 211 019, India
e-mail: ahoque.ms@gmail.com