DESCENT ON PICARD GROUPS USING FUNCTIONS ON CURVES

SAMIR SIKSEK

ABSTRACT. Let k be a perfect field, X a smooth curve over k, and denote by X^c the subset of closed points of X. We show that for any non-constant element f of the function field $k(X)$ there exists a natural homomorphism

$$\mathrm{Pic}(X) \to k^*/G_f(k)$$

where

$$G_f(k) := \prod_{\mathcal{P} \in X^c} \mathrm{Norm}_{k(\mathcal{P})/k} (k(\mathcal{P})^*)^{\mathrm{ord}_{\mathcal{P}}(f)}.$$

We explain how this generalizes the usual results on descents on Jacobians and Picard groups of curves.

1. INTRODUCTION

Let k be a perfect field and X a smooth curve over k, by which we mean a complete, non-singular and absolutely irreducible curve over k. Denote the function field of X over k by $k(X)$, the Jacobian by J_X, and the Picard group by $\mathrm{Pic}(X)$ (see Section 2 for the definition of the Picard group). The groups J_X and $\mathrm{Pic}(X)$ are often studied (particularly when k is a number field) by constructing homomorphisms from either of these groups to groups of finite exponent. For example:

(1) Descent algorithms on curves are usually concerned with the construction of homomorphisms from the Jacobian $J_X(k)$ to groups of the form L^*/L^{*q}, for suitably defined finite k-algebras L, and positive integers q. As observed by Schaefer ([6]), virtually all such descents utilize functions on the curve whose divisors are q-divisible.

(2) Let Y be a non-singular projective variety and f a non-constant element of the function field $k(Y)$ whose divisor is a norm for some finite extension K/k. Then there is a homomorphism $\mathrm{CH}_0(Y) \to k^*/\mathrm{Norm}(K^*)$ (see for example [1, pages 447-448]). If Y is our (smooth) curve X then we have a homomorphism $\mathrm{Pic}(X) \to k^*/\mathrm{Norm}(K^*)$.

In view of this it is natural to ask the following question: given an arbitrary non-constant function $f \in k(X)$, is there an induced homomorphism of $J_X(k)$ or $\mathrm{Pic}(X)$ into some group of finite exponent as above? In this paper we answer this question affirmatively. It is our hope that these homomorphisms will find interesting applications in the study of the arithmetic of curves.

Before stating the main theorem of this paper we set some notation. A closed point $\mathcal{P}$ of X corresponds to a discrete valuation ring $\mathcal{O}_{\mathcal{P}}$ of $k(X)$ containing k, with maximal ideal $\mathfrak{m}_{\mathcal{P}}$. The residue field of $\mathcal{P}$ is by definition $k(\mathcal{P}) := \mathcal{O}_{\mathcal{P}}/\mathfrak{m}_{\mathcal{P}}$,

Date: 7, January 2002.

2000 *Mathematics Subject Classification.* Primary 11G30, Secondary 11G25.

Key words and phrases. curves, descents, Jacobians, Picard groups.

and is a finite extension of k. The degree of $\mathcal{P}$ is given by $|\mathcal{P}| := [k(\mathcal{P}) : k]$. If $g \in k(X)$ is regular at point $\mathcal{P}$, that is $g \in \mathcal{O}_{\mathcal{P}}$, then the value of g at $\mathcal{P}$, denoted by $g(\mathcal{P})$, is defined to be the image of g in $k(\mathcal{P})$; it thus makes sense to speak of the $\mathrm{Norm}_{k(\mathcal{P})/k}(g(\mathcal{P})) \in k$. If K is a finite extension of k, and n is an integer then, as usual, we let

$$\underset{K/k}{\mathrm{Norm}}(K^*)^n := \{\alpha^n : \alpha \in \underset{K/k}{\mathrm{Norm}}(K^*)\}.$$

Clearly $\mathrm{Norm}_{K/k}(K^*)^0 = \{1\}$. For a closed point $\mathcal{P} \in X$ let $\mathrm{ord}_{\mathcal{P}} : k(X)^* \to \mathbb{Z}$ be the corresponding valuation. We denote the set of closed points on X by X^c; this of course is all of X except for the generic point. Now suppose $f \in k(X)$ is a non-constant function on the curve, and we let

$$G_f(k) := \prod_{\mathcal{P} \in X^c} \underset{k(\mathcal{P})/k}{\mathrm{Norm}}(k(\mathcal{P})^*)^{\mathrm{ord}_{\mathcal{P}}(f)}. \tag{1}$$

The product makes sense since all but finitely many of the terms are $\{1\}$, and the result is clearly a subgroup of k^*. Our main theorem defines a homomorphism from the Picard group $\mathrm{Pic}(X)$ to the quotient group $k^*/G_f(k)$ (see Section 2 for the definition of the Picard group). In essence, this means that we are doing descent on the Picard group of the curve.

Theorem 1. *Let X be a smooth curve over the perfect field k. Suppose f is a non-constant element of the function field $k(X)$, and let $G_f(k)$ be the subgroup of k^* defined above. Then f induces a unique homomorphism*

$$\phi_f : \mathrm{Pic}(X) \to k^*/G_f(k) \tag{2}$$

satisfying the following property: if $\sum m_j \mathcal{Q}_j$ is a divisor on X whose support is disjoint from the poles and zeros of f, then the class $[\sum m_j \mathcal{Q}_j]$ of this divisor in $\mathrm{Pic}(X)$ is mapped, by ϕ_f, to the coset represented by

$$\prod \underset{k(\mathcal{Q}_j)/k}{\mathrm{Norm}}(f(\mathcal{Q}_j))^{m_j}$$

in the group on the right-hand side.

2. Proof and Discussion of Theorem 1

Throughout this section X denotes a smooth curve over a perfect field k, and $\overline{k}$ the separable closure of k.

2.1. **Preliminaries.** It is worth recalling at the outset the relationship between the points of X, and the elements of $X(\overline{k})$. We started out by saying that a closed point $\mathcal{P}$ of X corresponds to discrete valuation rings $\mathcal{O}_{\mathcal{P}}$ of $k(X)$ containing k. Such a point would simultaneously correspond to an orbit of elements of $X(\overline{k})$, say $\{P_1, \ldots, P_d\}$, under the action of $\mathrm{Gal}\left(\overline{k}/k\right)$. When convenient, we may identify the two by writing $\mathcal{P} = \{P_1, \ldots, P_d\}$. Note that the size d of the orbit corresponding to $\mathcal{P}$ equals its degree $|\mathcal{P}| = [k(\mathcal{P}) : k]$. The points $P_1, \ldots, P_d$ in fact correspond to the distinct embeddings of the residue field $k(\mathcal{P})$ into $\overline{k}$. If $g \in \mathcal{O}_{\mathcal{P}}$ then

$$\underset{k(\mathcal{P})/k}{\mathrm{Norm}}(g(\mathcal{P})) = \prod g(P_i)$$

where as stated before, $g(\mathcal{P})$ is the image of g in $k(\mathcal{P}) := \mathcal{O}_{\mathcal{P}}/\mathfrak{m}_{\mathcal{P}}$, and the $g(P_i)$ have the usual meaning.

We now come to the definition of the Picard group, $\mathrm{Pic}(X)$, which we reproduce here since there is some discrepancy in the literature. Recall that we have defined X^c to be the set of closed points of X. The divisor group of X, denoted $\mathrm{Div}(X)$, is the free group on the points of X^c. The subgroup of principal divisors is denoted by $\mathrm{Princ}(X)$, and we let $\mathrm{Pic}(X) := \mathrm{Div}(X)/\mathrm{Princ}(X)$. If $X_{\overline{k}} := X \times_k \overline{k}$, then there is a natural injection

$$\mathrm{Pic}(X) \hookrightarrow H^0(\mathrm{Gal}\left(\overline{k}/k\right), \mathrm{Pic}(X_{\overline{k}})),$$

that is not always an isomorphism, though it often is. In particular, this natural injection is known to be an isomorphism in the following cases (see [5, Section 3]):

- when k is a local field and X possesses a k-rational divisor of degree 1.
- when k is a number field and, for every prime v of k, the corresponding curve $X_v = X \times_k k_v$ possesses a k_v-rational divisor of degree 1.

It follows in these cases that the degree 0 part of the Picard group, $\mathrm{Pic}^0(X)$, can be identified with $J_X(k)$, where J_X is the Jacobian of the curve X. Although it is useful to be aware of this, *we do not make any such assumption in this paper.*

We now come to discuss the notation and tools needed for the proof of Theorem 1. By the support of a divisor $\sum m_j \mathcal{Q}_j$ we mean the set $\{\mathcal{Q}_j : m_j \neq 0\}$. We say that a divisor is coprime to a set of points S if its support is disjoint from S. The support of a non-constant function $h \in k(X)$ is the support of its divisor. If $h \in k(X)$ is a non-constant function, and $\sum m_j \mathcal{Q}_j$ is a divisor coprime to the support of h then we define

$$h\left(\sum m_j \mathcal{Q}_j\right) := \prod \underset{k(\mathcal{Q}_j)/k}{\mathrm{Norm}} (h(\mathcal{Q}_j))^{m_j}.$$

Recall the identification made above between closed points of X and orbits of elements of $X(\overline{k})$ under the action of $\mathrm{Gal}\left(\overline{k}/k\right)$. One immediately sees that this definition of $h(\sum m_j \mathcal{P}_j)$ is in harmony with the usual definition found elsewhere (for example [7, page 37] or [8, page 43]). Before proving Theorem 1 we need to recall Weil's reciprocity.

Weil's Reciprocity. *Suppose X is a smooth curve over a perfect field k, and $h_1,\ h_2 \in k(X)$ are non-constant functions having disjoint supports. Then*

$$h_1(\mathrm{div}(h_2)) = h_2(\mathrm{div}(h_1)).$$

See [7, page 37], or [8, page 43].

2.2. **Proof of Theorem 1.** Let S be the support of f. We let $\mathrm{Div}(X)_S$ be the subgroup of $\mathrm{Div}(X)$ of divisors coprime to S. Define a map

$$\mathrm{Div}(X)_S \to k^*/G_f(k) \tag{3}$$

sending $\sum m_j \mathcal{Q}_j$ to the coset represented by $f(\sum m_j \mathcal{Q}_j)$. Clearly this map is a homomorphism. Now let $\mathrm{Princ}(X)_S$ be the subgroup of principal divisors coprime to S; thus

$$\mathrm{Princ}(X)_S := \mathrm{Div}(X)_S \cap \mathrm{Princ}(X).$$

We first show that $\mathrm{Princ}(X)_S$ is contained in the kernel of the homomorphism (3). Thus suppose $g \in k(X)$ is a non-constant function such that $\mathrm{div}(g) \in \mathrm{Princ}(X)_S$. Clearly $f,\ g$ have disjoint support. The map in (3), sends $\mathrm{div}(g)$ to the coset

represented by $f(\mathrm{div}(g))$ in $k^*/G_f(k)$, and hence to show that $\mathrm{div}(g)$ is in the kernel it is sufficient to show that $f(\mathrm{div}(g)) \in G_f(k)$. We observe that

$$\begin{aligned} f(\mathrm{div}(g)) &= g(\mathrm{div}(f)) && \text{(By Weil's reciprocity)} \\ &= g\left(\sum_{\mathcal{P}\in X^c} \mathrm{ord}_{\mathcal{P}}(f)\mathcal{P}\right) \\ &= \prod_{\mathcal{P}\in X^c} \mathrm{Norm}_{k(\mathcal{P})/k}(g(\mathcal{P}))^{\mathrm{ord}_{\mathcal{P}}(f)} \end{aligned}$$

However, $\mathrm{Norm}_{k(\mathcal{P})/k}(g(\mathcal{P}))$ is in $\mathrm{Norm}_{k(\mathcal{P})/k}(k(\mathcal{P})^*)$, and it immediately follows that $f(\mathrm{div}(g))$ is in $G_f(k) := \prod_{\mathcal{P}\in X} \mathrm{Norm}_{k(\mathcal{P})/k}(k(\mathcal{P})^*)^{\mathrm{ord}_{\mathcal{P}}(f)}$, and so $\mathrm{div}(g)$ is in the kernel of the map (3). We thus obtain an induced homomorphism

$$\mathrm{Div}(X)_S/\mathrm{Princ}(X)_S \to k^*/G_f(k),$$

sending the class of a divisor $\sum m_j\mathcal{Q}_j$ that is coprime to S to the coset on the right-hand side represented by $f(\sum m_j\mathcal{Q}_j) = \prod \mathrm{Norm}_{k(\mathcal{Q}_j)/k}(f(\mathcal{Q}_j))^{m_j}$. The proof of Theorem 1 is complete upon observing that the obvious injection

$$\mathrm{Div}(X)_S/\mathrm{Princ}(X)_S \hookrightarrow \mathrm{Pic}(X)$$

is indeed an isomorphism. This follows from the fact, proven by Lang, that any divisor class containing a k-rational divisor also contains a k-rational divisor whose support is disjoint from a given finite set[1] (see [3, page 166]).

2.3. **A discussion of Theorem 1.** It is appropriate to make some remarks regarding the proof of Theorem 1.

(1) The proof of Theorem 1 is similar to Schaefer's proof of his [6, Lemma 2.1]; the main difference is the replacement of q-th powers by norms.
(2) Moving the divisor in its class so as to avoid the 'bad set' is a standard device in algebraic geometry; compare the above proof to the construction of the intersection pairing $\mathrm{Pic}(X) \times \mathrm{Pic}(X) \to \mathbb{Z}$ for a surface (see [2, page 357]), and to the construction of the pairing $\mathrm{Pic}(X) \times \mathrm{Br}(X) \to \mathrm{Br}(k)$ for a curve (see [4]). As far as we are aware, Schaefer was the first to apply this to the construction of descent maps. The older approach used patching arguments, and extending these to work in our situation would have been infinitely troublesome, if not outright impossible!
(3) We have taken the domain of our map ϕ_k to be $\mathrm{Pic}(X)$ where as in descent maps the domain is usually $J_X(k)$ (after making suitable assumptions to identify this with $\mathrm{Pic}^0(X)$; see page 3).

2.4. **An Example.** It is a good idea to give an example to show how Theorem 1 extends descent maps even when we restrict the domain to $\mathrm{Pic}^0(X)$. Let X be the elliptic curve (over $\mathbb{Q}$) given by the Weierstrass equation

$$X : y^2 = x^3 + ax + b.$$

[1] This is in fact an easy consequence of the weak approximation theorem for function fields. To see this suppose that $\sum m_j\mathcal{Q}_j$ is a divisor and that we want to find an equivalent divisor avoiding the finite set S. By the weak approximation theorem (see [9, page 11]) there exists a function $h \in k(X)$ such that $\mathrm{ord}_{\mathcal{Q}_j}(h) = m_j$ for all j and $\mathrm{ord}_{\mathcal{Q}}(h) = 0$ for any $\mathcal{Q} \in S$ that is not one of the $\mathcal{Q}_j$. Then $-\mathrm{div}(h) + \sum m_j\mathcal{Q}_j$ avoids S and is equivalent to $\sum m_j\mathcal{Q}_j$.

We denote the point at infinity by O, and take $f = x$. Theorem 1 defines a homomorphism $\phi_x : \mathrm{Pic}(X) \to \mathbb{Q}^*/G_x(\mathbb{Q})$. Now the map $X(\mathbb{Q}) \to \mathrm{Pic}^0(X)$ given by $P \mapsto [P - O]$ is an isomorphism (where $X(\mathbb{Q})$ has the usual group law). Thus composing with ϕ_x we obtain a homomorphism

$$\psi : X(\mathbb{Q}) \to \mathbb{Q}^*/G_x(\mathbb{Q})$$

given by

$$\psi(P) = x(P)G_x(\mathbb{Q})$$

for $P \neq O$ and $x(P) \neq 0$ (it is not hard to show that $\phi_x([O]) = 1 \cdot G_x(\mathbb{Q})$). It remains to compute $G_x(\mathbb{Q})$, and there are three cases:

Case 1: $b = 0$. The divisor of x is just $2(0,0) - 2O$. Both points in the support of the divisor have residue field $\mathbb{Q}$. Hence $G_x(\mathbb{Q}) = \mathbb{Q}^{*2}$, and the map $\psi : X(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ is the usual one arising from the descent via 2-isogeny.

Case 2: $b \neq 0$, $b \in \mathbb{Q}^{*2}$, say $b = c^2$. The divisor of x is $(0,c) + (0,-c) - 2O$. The residue fields are all $\mathbb{Q}$ again, but this time $G_x(\mathbb{Q}) = \mathbb{Q}^*$ and so the map $\psi = 1$.

Case3: $b \neq 0$, $b \notin \mathbb{Q}^{*2}$. The divisor of x is $(0,\sqrt{b}) + (0,-\sqrt{b}) - 2O$. We find that $G_x(\mathbb{Q}) = \mathrm{Norm}(\mathbb{Q}(\sqrt{b})^*)\mathbb{Q}^{*-2} = \mathrm{Norm}(\mathbb{Q}(\sqrt{b})^*)$. Hence we obtain a homomorphism

$$\psi : X(\mathbb{Q}) \to \mathbb{Q}^*/\,\mathrm{Norm}(\mathbb{Q}(\sqrt{b})^*)$$

given by

$$\psi(P) = \begin{cases} x(P)\,\mathrm{Norm}(\mathbb{Q}(\sqrt{b})^*) & \text{if } P \neq O, \\ 1 \cdot \mathrm{Norm}(\mathbb{Q}(\sqrt{b})^*) & \text{if } P = O. \end{cases}$$

Acknowledgment. I would like to thank J. Cremona, B. Poonen, E. Schaefer, A. Skorobogatov, and J. Top for useful discussions during the course of writing this paper. I am deeply indebted to Professor J.-L. Colliot-Thélène for detailed criticisms of a previous version of this paper, and for drawing to my attention [1].

References

[1] J.-L. Colliot-Thélène and J.-J. Sansuc *La descente sur les variétés rationnelles, II*, Duke J. Math. **54** (1987), 375–492.
[2] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, 1977.
[3] S. Lang, *Abelian varieties*, Interscience Publishers, New York, 1959.
[4] S. Lichtenbaum, *Duality theorems for curves over P-adic Fields*, Invent. math. **7** (1969), 120–136.
[5] B. Poonen, E.F. Schaefer, *Explicit descent for the Jacobians of cyclic covers of the projective line*, J. reine angew. Math. **488** (1997), 141–188.
[6] E.F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310** (1998), 447-471.
[7] J.-P. Serre, *Algebraic groups and class fields*, Springer-Verlag, New York, 1988.
[8] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM **106**, Springer-Verlag, 1986.
[9] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, 1993.

Department of Mathematics, Faculty of Science, Sultan Qaboos University, P.O. Box 36, Al-Khod 123, Oman
E-mail address: siksek@squ.edu.om