Reciprocity laws for simple algebras over function fields of number curves

by

V. I. Guletskiĭ and V. I. Yanchevskiĭ

1 Introduction

Let k be a field of characteristic zero, X a smooth projective curve over k, X^1 the set of all closed points of X and $\overline{X} = X \times_k \overline{k}$ for an algebraic closure $\overline{k}$ of k. The following sequence of abelian groups and homomorphisms is well known

$$0 \to \operatorname{Br} X \to \operatorname{Br} k(X) \stackrel{\text{inv}}{\to} \bigoplus_{x \in X^1} H^1(k(x), \mathbf{Q}/\mathbf{Z}) \stackrel{\Sigma}{\to} H^1(k, \mathbf{Q}/\mathbf{Z})$$

where $\operatorname{Br} X$ is the Brauer group of X, $\operatorname{Br} k(X)$ is the Brauer group of the function field $k(X)$ on X, $k(x)$ is the residue field at $x \in X^1$ and $H^i(k, ?)$ denotes the Galois cohomology of k. Later on we shall present a cohomological interpretation of this sequence, but now we only note that it allows us to study $\operatorname{Br} k(X)$ using the local-to-global principle. The homomorphism inv is induced by the local ones $\text{inv}_x : \operatorname{Br} k(X) \to H^1(k(x), \mathbf{Q}/\mathbf{Z})$. If $a \in \operatorname{Br} k(X)$, then the character $\text{inv}_x(a)$ is called the local invariant of a at x and its order equals the ramification index at x of the algebras in a. Hence ker(inv) coincides with the unramified Brauer group $\operatorname{Br}_{nr} k(X)$ of $k(X)$ which is canonically isomorphic to $\operatorname{Br} X$ [1]. The homomorphism Σ sums corestrictions of characters. We shall say that an element from $\bigoplus_{x \in X^1} H^1(k(x), \mathbf{Q}/\mathbf{Z})$ satisfies a reciprocity law if it belongs to $\ker(\Sigma)$. It can be shown (see below), that the complete system of local invariants of any $a \in \operatorname{Br} k(X)$ satisfies the reciprocity law, i.e. $\text{im(inv)} \subset \ker(\Sigma)$. In some cases the converse statement is also true. For example, this holds if $X \cong \mathbf{P}^1$. In other words, in this case the group of local invariants of central simple algebras over $k(X)$ is comletely determined by the reciprocity law. But in general $\ker(\Sigma) \neq \text{im(inv)}$ (see [2], [3]). This means that there exists an "additional reciprocity law" describing local invariants of central simple algebras over $k(X)$. Therefore we are lead to study the quotient

$$\Delta := \ker(\Sigma)/\operatorname{im}(\text{inv})\ .$$

We shall call it the obstruction group for realizing characters satisfying the reciprocity law as systems of local invariants of algebras over $k(X)$, or shortly the obstruction group.

In 1975 B.Becker has proved ([4]) that for a curve X defined over a number field k with at least one k-rational point Δ is a group of exponent 2 which is trivial if k is totally imaginary. The case where X is a genus one curve was considered in [2] and [3]. It has been proved there that $\Delta \cong (\mathbf{Z}/2)^s$ where s is the number of real embeddings of k which leads to curves with two-component Jacobians, and that $\ker(\Sigma)$ is the direct sum of $\mathrm{im}(\mathrm{inv})$ and Δ.

In this paper we generalize the results above to an arbitrary smooth projective curve X of positive genus defined a over number field k. More precisely, we prove the following

Main Theorem. *Let k be a number field, $s = 0$ if k is totally imaginary, and s the number of real embeddings $\rho_i : k \hookrightarrow \mathbf{R}$, $i = 1, \dots, s$, for k otherwise. Let X be a smooth projective curve of arbitrary genus defined over k with a k-point, and $X_i = X \times_k \mathbf{R}$ where the product is taken with respect to ρ_i. Let also r_i be the number of components of $X_i(\mathbf{R})$ in the real topology. Then*

$$\Delta \cong (\mathbf{Z}/2)^{r_1+\ldots+r_s-s} \ .$$

Moreover, the short exact sequence $0 \to \mathrm{im}(\mathrm{inv}) \to \ker(\Sigma) \to \Delta \to 0$ splits, so

$$\ker(\Sigma) \cong \mathrm{im}(\mathrm{inv}) \oplus (\mathbf{Z}/2)^{r_1+\ldots+r_s-s} \ .$$

Notation and conventions. For any abelian group A and any natural n we denote by $A \xrightarrow{n} A$ the multiplication by n, ${}_nA$, nA and A/n are its kernel, image and cokernel respectively. $A^n = A \oplus \ldots \oplus A$ is the direct sum of n copies of A and let $A^0 = 0$. A variety over k is a geometrically integral separated scheme of finite type over k. If X is a variety over k and L/k is a field extension, then $X_L := X \times_k L$, $\overline{X} = X \times_k \overline{k}$ and $X(L)$ is the set of closed L-points of X_L. We will denote by G the absolute Galois group $\mathrm{Gal}(\overline{k}/k)$ of k.

ACKNOWLEDGEMENTS. The authors are grateful to I.A.Panin for many useful discussions. This research has been supported by the Institute of Mathematics of the Academy of Sciences of Belarus in the framework of the state program "Mathematical structures". The second author was also supported by INTAS, Project 93-2618. Also, the authors want to thank the Sonderforschungsbereich 343 ("Diskrete Strukturen in der Mathematik") for hospitality.

2 A cohomological description of the obstruction group

Let $\mathrm{Div}\,\overline{X}$ and $\overline{k}(\overline{X})$ be the divisor group and the function field of $\overline{X}$, respectively,

$$\mathrm{div} : \overline{k}(\overline{X})^* \to \mathrm{Div}\,\overline{X}\ ,$$

and

$$\deg : \mathrm{Div}\,\overline{X} \to \mathbf{Z}$$

are the G-homomorphisms defined as follows:

$$f \mapsto \mathrm{div}(f)$$

for any $f \in \overline{k}(\overline{X})^*$ where $\mathrm{div}(f)$ is the principal divisor of a function f and

$$\deg(\sum n_x x) = \sum n_x\ .$$

They induce the corresponding homomorphisms of the cohomology groups:

$$\mathrm{div}^* : H^2(k, \overline{k}(\overline{X})^*) \longrightarrow H^2(k, \mathrm{Div}\,\overline{X})$$

and

$$H^2(k, \mathrm{Div}\,\overline{X}) \to H^2(k, \mathbf{Z})\ .$$

Since

$$H^2(k, \overline{k}(\overline{X})^*) \cong \mathrm{Br}\,k(X)$$

by Tsen's theorem,

$$H^2(k, \mathrm{Div}\,\overline{X}) \cong \bigoplus_{x \in X^1} H^1(k(x), \mathbf{Q}/\mathbf{Z})$$

where $k(x)$ is the residue field at x, and

$$H^2(k, \mathbf{Z}) \cong H^1(k, \mathbf{Q}/\mathbf{Z})\ ,$$

we have homomorphisms

$$\operatorname{Br} k(X) \stackrel{\text{iny}}{\to} \bigoplus_{x\in X^1} H^1(k(x),\mathbf{Q}/\mathbf{Z}) \stackrel{\Sigma}{\to} H^1(k,\mathbf{Q}/\mathbf{Z})\ .$$

If $\{\chi_x\} \in \bigoplus_{x\in X^1} H^1(k(x),\mathbf{Q}/\mathbf{Z})$, then

$$\Sigma(\{\chi_x\}) = \sum_x \operatorname{cor}(\chi_x)$$

where $\operatorname{cor} : H^1(k(x),\mathbf{Q}/\mathbf{Z}) \to H^1(k,\mathbf{Q}/\mathbf{Z})$ is the corestriction homomorphism.

Assume that X/k satisfies the condition

$$\ker\Big(H^3(k,\overline{k}^*) \longrightarrow H^3(k,\overline{k}(\overline{X})^*)\Big) = 0\ .$$

It is known that this condition holds for any X/k if k is a number field, a local number field or the field of real numbers because in all these cases $H^3(G,\overline{k}^*) = \{0\}$. For any number field k this follows from global class field theory, in the local number case this holds since the strict cohomological dimension of G is 2. If $k = \mathbf{R}$ this is simply the Hilbert 90 Theorem. Consider a short exact sequence of discrete G-modules (from now on we shall write shortly "a G-module" instead of "a discrete G-module")

$$1 \to \overline{k}^* \longrightarrow \overline{k}(\overline{X})^* \stackrel{\text{div}}{\longrightarrow} \mathrm{P}\overline{X} \to 0$$

where $\mathrm{P}\overline{X}$ is the principal divisor group of $\overline{X}$. It follows from the condition above on X/k and the long exact sequence induced by the former short one that the homomorphism

$$\operatorname{div}^* : H^2(k,\overline{k}(\overline{X})^*) \longrightarrow H^2(k,\mathrm{P}\overline{X})$$

is surjective. Then the image of the homomorphism

$$\operatorname{div}^* : H^2(k,\overline{k}(\overline{X})^*) \longrightarrow H^2(k,\operatorname{Div}\overline{X})$$

coincides with that of

$$\gamma : H^2(k,\mathrm{P}\overline{X}) \longrightarrow H^2(k,\operatorname{Div}\overline{X})$$

where γ is induced by the inclusion $\mathrm{P}\overline{X} \subset \operatorname{Div}\overline{X}$. Since $H^1(k,\mathbf{Z}) = \{0\}$, the long exact cohomological sequence induced by

$$0 \to \operatorname{Div}^0\overline{X} \longrightarrow \operatorname{Div}\overline{X} \stackrel{\deg}{\longrightarrow} \mathbf{Z} \to 0$$

shows that the group $H^2(k, \mathrm{Div}^0 \overline{X})$ is injectively embedded to $H^2(k, \mathrm{Div}\,\overline{X})$ by the homomorphism induced by $\mathrm{Div}^0 \overline{X} \subset \mathrm{Div}\,\overline{X}$.

Now let J be the Jacobian of X. Then $\overline{J} = J \times_k \overline{k}$ is the Jacobian of $\overline{X}$ and there is the canonical isomorphism between the degree 0 divisor class group $\mathrm{Cl}\,\overline{X} = \mathrm{Div}^0 \overline{X}/\mathrm{P}\overline{X}$ and $J(\overline{k})$. Since we assume that $X(k) \neq \emptyset$, this isomorphism is defined over k. Hence we have a short exact sequence of G-modules

$$0 \to \mathrm{P}\overline{X} \longrightarrow \mathrm{Div}^0 \overline{X} \xrightarrow{\Lambda} J(\overline{k}) \to 0$$

where Λ is the composition of the epimorphism $\mathrm{Div}^0 \overline{X} \to \mathrm{Cl}\,\overline{X}$ and the isomorphism $\mathrm{Cl}\,\overline{X} \cong J(\overline{k})$. The sequence above induces the corresponding exact sequence

$$\ldots \to H^2(k,\mathrm{P}\overline{X}) \xrightarrow{\epsilon} H^2(k,\mathrm{Div}^0 \overline{X}) \xrightarrow{\zeta} H^2(G,J(\overline{k})) \xrightarrow{\delta} H^3(k,\mathrm{P}\overline{X}) \to \ldots ,$$

where ζ is induced by Λ. Using the exactness of this sequence and the arguments above we obtain:

$$\Delta \cong \ker(\deg^*)/\operatorname{im}(\mathrm{div}^*) = \ker(\deg^*)/\operatorname{im}(\gamma) \cong$$

$$\cong H^2(G, \mathrm{Div}^0 \overline{X})/\operatorname{im}(\epsilon) \cong \operatorname{im}(\zeta) = \ker(\delta) .$$

Thus we have proved

Lemma 1. *Assume that* $\ker(H^3(k, \overline{k}^*) \to H^3(k, \overline{k}(\overline{X})^*)) = 0$. *For any* $x \in \ker(\Sigma)$ *let* x' *be the element from* $\ker(\deg^*)$ *corresponding to* x *under the isomorphism* $H^2(k, \mathrm{Div}\,\overline{X}) \cong \oplus_{x\in X^1} H^1(k(x), \mathbf{Q}/\mathbf{Z})$ *and let* x'' *be the element from* $H^2(k, \mathrm{Div}^0 \overline{X})$ *corresponding to* x' *under the isomorphism between the last group and* $\ker(\deg^*)$. *Then the map*

$$\theta : \Delta \longrightarrow \ker(\delta) \ , \ x + \operatorname{im}(\mathrm{inv}) \mapsto \zeta(x'')$$

is an isomorphism.

This lemma yields a cohomological interpretation of the obstruction group Δ.

Corollary. *If* $\overline{X}$ *is a curve of genus 0, then* $\Delta = 0$.

The cohomological description of Δ permits us to examine its behavior under constant field extensions. Consider an embedding $\rho : k \hookrightarrow K$. Let

$H = \mathrm{Gal}(\overline{K}/K)$ where $\overline{K}$ is the algebraic closure of the field K and $\tau : \overline{k} \hookrightarrow \overline{K}$ is an embedding over ρ. Then τ determines a homomorphism $\tau^- : H \to G$ by the formula $\tau^-(h)(x) = \tau^{-1}(h\tau(x))$, $h \in H$, $x \in \overline{k}$. Let X_ρ be the curve determined by the cartesian square

$$\begin{array}{ccc} X_\rho & \longrightarrow & \mathrm{Spec}\, K \\ \downarrow & & \downarrow\rho \\ X & \longrightarrow & \mathrm{Spec}\, k \end{array} \quad .$$

and Δ_ρ be the obstruction group for realizing characters satisfying the reciprocity law as invariants of $\overline{K}(\overline{X}_\rho)$-algebras, i.e. the obstruction group for the curve X_ρ/K.

The embedding $X(\overline{k}) \hookrightarrow X(\overline{K})$ induces a homomorphism

$$\tau^+ : \mathrm{Div}\, \overline{X} \longrightarrow \mathrm{Div}\, \overline{X}_\rho$$

which preserves degrees and the linear equivalence of divisors. Hence τ^+ induces homomorphisms of degree zero divisor groups, groups of principal divisors and divisor class groups modulo linear equivalence. To be short, we shall denote them by τ^*. As a result, we have the following morphisms of short exact sequences of G-modules

$$\begin{array}{ccccccc} 0 \to & \mathrm{Div}^0\, \overline{X} & \to & \mathrm{Div}\, \overline{X} & \to & \mathbf{Z} & \to 0 \\ & \downarrow\tau^+ & & \downarrow\tau^+ & & \| & \\ 0 \to & \mathrm{Div}^0\, \overline{X}_\rho & \to & \mathrm{Div}\, \overline{X}_\rho & \to & \mathbf{Z} & \to 0 \end{array}$$

and

$$\begin{array}{ccccccc} 0 \to & \mathrm{P}\overline{X} & \to & \mathrm{Div}^0\, \overline{X} & \to & \overline{J} & \to 0 \\ & \downarrow\tau^+ & & \downarrow\tau^+ & & \downarrow\tau^+ & \\ 0 \to & \mathrm{P}\overline{X}_\rho & \to & \mathrm{Div}^0\, \overline{X}_\rho & \to & \overline{J}_\rho & \to 0 \end{array} \quad .$$

A straightforward check shows that the homomorphism τ^- is compatible with all homomorphisms τ^+, so the pairs $[\tau^-, \tau^+]$ induce morphisms of corresponding long exact cohomological sequences. Let

$$\delta_\rho : H^2(K, J_\rho(\overline{K})) \longrightarrow H^3(H, \mathrm{P}\overline{X}_\rho)$$

be the connecting homomorphism which is analogous to δ. It follows from the arguments above that

$$\tau^* : H^2(k, J(\overline{k})) \longrightarrow H^2(K, J_\rho(\overline{K}))$$

sends $\ker(\delta)$ to $\ker(\delta_\rho)$. In a similar way

$$\tau^* : H^2(k, \operatorname{Div} \overline{X}) \longrightarrow H^2(K, \operatorname{Div} \overline{X}_\rho)$$

sends $\ker(\deg^*)$ and $\operatorname{im}(\gamma)$ to the groups $\ker(\deg^*)$ and $\operatorname{im}(\gamma)$, respectively, but considered for the curve X_ρ/K. Then the latter homomorphism τ^* induces a homomorphism from the quotient $\ker(\deg^*)/\operatorname{im}(\gamma)$ taken for X/k to the similar quotent taken for X_ρ/K. Replacing these groups by the isomorphic obstruction groups Δ and Δ_ρ, we obtain a homomorphism

$$\xi_\rho : \Delta \longrightarrow \Delta_\rho \ .$$

Assume now that

$$\ker(H^3(k, \overline{k}^*) \longrightarrow H^3(k, \overline{k}(\overline{X}))) = 0 \ ,$$
$$\ker(H^3(K, \overline{K}^*) \longrightarrow H^3(K, \overline{K}(\overline{X}_\rho))) = 0 \ ,$$

and let $\theta_\rho : \Delta_\rho \to \ker(\delta_\rho)$ be the isomorphism from Lemma 1. The homomorphisms τ^* induced by pairs (τ^-, τ^+) on the cohomology groups commute with the homomorphisms from cohomological long exact sequences which are induced by the above short exact sequences of G-modules. This and the construction of θ and θ_ρ enables one to conclude immediately that the diagram

$$\begin{array}{ccc} \Delta & \xrightarrow{\theta} & \ker(\delta) \\ \xi_\rho\downarrow & & \downarrow\tau^* \\ \Delta_\rho & \xrightarrow{\theta_\rho} & \ker(\delta_\rho) \end{array}$$

is commutative.

Now apply the arguments above to the case of number fields. So we fix a number field k with real embeddings $\rho_i : k \hookrightarrow \mathbf{R}$, $i = 1, ..., s$. Fix an embedding $\tau_i : \overline{k} \hookrightarrow \mathbf{C}$ over ρ_i for each i and consider specializations $K = \mathbf{R}$, $\rho = \rho_i$ and $\tau = \tau_i$. Set for shortness

$$X_i = X_{\rho_i}, \ , \ \Delta_i = \Delta_{\rho_i} \ ,$$
$$J_i = J_{\rho_i}, \ , \ \delta_i = \delta_{\rho_i}, \ , \ \theta_i = \theta_{\rho_i} \ , \ \xi_i = \xi_{\rho_i} \ .$$

Taking the sums of the lower rows in the commutative diagrams above, we obtain the following commutative square

$$\begin{array}{ccc} \Delta & \xrightarrow{\theta} & \ker(\delta) \\ \xi\downarrow & & \downarrow\kappa \\ \bigoplus_{i=1}^{s} \Delta_i & \xrightarrow{\oplus_{i=1}^{s}\theta_i} & \bigoplus_{i=1}^{s} \ker(\delta_i) \end{array}$$

where the homomorphism ξ is induced by ξ_i and κ is the restriction of the localization homomorphism

$$\mu : H^2(k, J(\overline{k})) \longrightarrow \bigoplus_{i=1}^{s} H^2(\mathbf{R}, J_i(\mathbf{C}))$$

of $H^2(k, J(\overline{k}))$ at all real absolute values of k to the kernel $\ker(\delta)$. The localization homomorphism μ can be described in the following way. Let $\sigma : \mathbf{C} \to \mathbf{C}$ be the usual conjugation in the field of complex numbers $\mathbf{C}$ and $< \sigma >= \{1, \sigma\} = \mathrm{Gal}(\mathbf{C}/\mathbf{R})$.

The embedding τ_i induces injective homomorphisms

$$\tau_i^- :< \sigma > \hookrightarrow G$$

and

$$\tau_i^+ : J(\overline{k}) \hookrightarrow J_i(\mathbf{C}) \ .$$

The pairs of homomorphisms (τ_i^-, τ_i^+) are compatible and so define homomorphisms

$$\mu_i : H^2(k, J(\overline{k})) \longrightarrow H^2(\mathbf{R}, J_i(\mathbf{R}))$$

which lead to the homomorphism μ.

Let

$$\Lambda_i : \mathrm{Div}^0 \, \overline{X}_i \longrightarrow J_i(\mathbf{C})$$

be the canonical epimorphism similar to the epimorphism Λ and

$$\zeta_i : H^2(\mathbf{R}, \mathrm{Div}^0 \, \overline{X}_i) \longrightarrow H^2(\mathbf{R}, J_i(\mathbf{C}))$$

be the homomorphism induced by Λ_i on the cohomology. It is easy to show that ζ_i has a right inverse homomorphism. Indeed,

$$H^2(\mathbf{R}, J_i(\mathbf{C})) \cong \hat{H}^0(\mathbf{R}, J_i(\mathbf{C})) \cong$$

$$\cong J_i(\mathbf{C})^{<\sigma>} / \, \mathrm{Nm}(J_i(\mathbf{C})) = J_i(\mathbf{R}) / \, \mathrm{Nm}(J_i(\mathbf{C}))$$

where $\hat{H}^0$ is the zero Tate cohomology group and $\mathrm{Nm} : J_i(\mathbf{C}) \to J_i(\mathbf{C})$, $P \mapsto P + \sigma P$ is the norm homomorphism on a complex abelian variety. The same arguments show that

$$H^2(\mathbf{R}, \mathrm{Div}^0 \, \overline{X}_i) \cong \hat{H}^0(\mathbf{R}, \mathrm{Div}^0 \, \overline{X}_i) \cong$$

$$\cong (\mathrm{Div}^0 \, \overline{X}_i)^{<\sigma>} / \, \mathrm{Nm}(\mathrm{Div}^0 \, \overline{X}_i) \ ,$$

where $\mathrm{Nm}: \mathrm{Div}^0 \overline{X}_i \to \mathrm{Div}^0 \overline{X}_i$ is the norm homomorphism $D \mapsto D + \sigma D$. If ζ_i' is the composition ζ_i with the isomorphism above, then

$$\zeta_i' : (\mathrm{Div}^0 \overline{X}_i)^{<\sigma>} / \mathrm{Nm}(\mathrm{Div}^0 \overline{X}_i) \longrightarrow J_i(\mathbf{R}) / \mathrm{Nm}(J_i(\mathbf{C}))$$

and ζ_i' sends the coset of $D \in \mathrm{Div}^0 \overline{X}_i$ to the coset of $\Lambda_i(D) \in J_i(\mathbf{R})$.

Denote by r_i the number of connected components of $X_i(\mathbf{R})$ in the real topology. Observe that since $X(k) \neq \emptyset$, the set $X_i(\mathbf{R}) \neq \emptyset$ for any i. Then

$$J_i(\mathbf{R}) / \mathrm{Nm}(J_i(\mathbf{C})) \cong (\mathbf{Z}/2)^{r_i - 1}$$

(see [5]), and by the Harnak theorem, $0 \leq r_i - 1 \leq g_X$ where g_X is the genus of X. The cosets of $J_i(\mathbf{R})$ modulo $\mathrm{Nm}(J_i(\mathbf{C}))$ are just the connected components of $J_i(\mathbf{R})$ since for $Q \in J_i(\mathbf{R})$ the map

$$J_i(\mathbf{R}) \longrightarrow J_i(\mathbf{R})$$

$$P \mapsto P + Q$$

is a homeomorphism. Then any element of $J_i(\mathbf{R}) / \mathrm{Nm}(J_i(\mathbf{C}))$ is uniquely determined by fixing a point P in some connected component of $J_i(\mathbf{R})$.

Let $h \in H^2(\mathbf{R}, J_i(\mathbf{C}))$ and P be a point in $J_i(\mathbf{R})$ the coset of which corresponds to h under the isomorphism above. Since P is $\mathbf{R}$-rational, there exists a $\mathbf{R}$-rational divisor $D \in \mathrm{Div}^0 \overline{X}_i$ such that $\Lambda_i(D) = P$. If $[D]$ is a coset of D modulo linear equivalence, then we have $\zeta_i'([D]) = P + \mathrm{Nm}\, J_i(\mathbf{C})$. It follows from the arguments above that if c is the cohomology class corresponding to the coset $[D]$ under the isomorphism

$$H^2(\mathbf{R}, \mathrm{Div}^0 \overline{X}_i) \cong (\mathrm{Div}^0 \overline{X}_i)^{<\sigma>} / \mathrm{Nm}(\mathrm{Div}^0 \overline{X}_i) \ ,$$

then $\zeta_i(c) = h$.

Futhermore, $H^2(\mathbf{R}, \mathrm{Div}^0 \overline{X}_i)$ is injectively embedded in $H^2(\mathbf{R}, \mathrm{Div}\, \overline{X}_i)$ (see the arguments above). For any point $x \in X_i^1$ its residue field coincides either with $\mathbf{C}$ or with $\mathbf{R}$. In the first case $H^1(\mathbf{R}(x), \mathbf{Q}/\mathbf{Z}) = 0$ and in the second one $H^1(\mathbf{R}(x), \mathbf{Q}/\mathbf{Z})$ is a group of order 2. Then

$$H^2(\mathbf{R}, \mathrm{Div}\, \overline{X}_i) \cong \bigoplus_{x \in X_i^1, \mathbf{R}(x) = \mathbf{R}} \mathbf{Z}/2$$

is a group of exponent 2 since $H^2(\mathbf{R}, \mathrm{Div}\, \overline{X}_i) \cong \oplus_{x \in X_i^1} H^1(\mathbf{R}(x), \mathbf{Q}/\mathbf{Z})$. Hence $H^2(\mathbf{R}, \mathrm{Div}^0 \overline{X}_i)$ is also of exponent 2. In particular, c is of order 2.

Thus to any $h \in H^2(\mathbf{R}, J_i(\mathbf{C}))$ one can associate such an element $c \in H^2(\mathbf{R}, \mathrm{Div}^0 \overline{X}_i)$ of order 2 that $\zeta_i(c) = h$. If now one will do this for all basis elements of

$$H^2(\mathbf{R}, J_i(\mathbf{C})) \cong (\mathbf{Z}/2)^{r_i - 1}$$

and will extend this correspondence to the homomorphism

$$H^2(\mathbf{R}, J_i(\mathbf{C})) \longrightarrow H^2(\mathbf{R}, \mathrm{Div}^0 \overline{X}_i)\ ,$$

then the existence of a right inverse homomorphism to ζ_i will be proved.

In particular, we have $\mathrm{im}(\zeta_i) = \ker(\delta_i) = H^2(\mathbf{R}, J_i(\mathbf{C}))$. By Lemma 1

$$\Delta_i \cong (\mathbf{Z}/2)^{r_i - 1}\ .$$

Moreover, if inv_i and Σ_i are homomorphisms analogous to inv and Σ but taken for $X_i/\mathbf{R}$, then a short exact sequence

$$0 \to \mathrm{im}(\mathrm{inv}_i) \longrightarrow \ker(\Sigma_i) \longrightarrow \Delta_i \to 0$$

splits.

Now it is clear that the latter commutative square is in fact of the form

$$\begin{array}{ccc} \Delta & \xrightarrow{\theta} & \ker(\delta) \\ \xi\downarrow & & \downarrow\kappa \\ \bigoplus_{i=1}^{s}\Delta_i & \xrightarrow{\oplus_{i=1}^{s}\theta_i} & \bigoplus_{i=1}^{s} H^2(\mathbf{R}, J_i(\mathbf{C})) \end{array}\ .$$

Since $\overline{J}$ is an abelian variety, the localization homomorphism μ is an isomorphism ([6], p.111). Then κ is an injection. Summarizing the arguments above, we obtain

Proposition 1. *The homomorphism*

$$\xi : \Delta \longrightarrow \bigoplus_{i=1}^{s}\Delta_i$$

is injective, so $\Delta \cong (\mathbf{Z}/2)^n$ where $n \le r_1 + \ldots + r_s - s$. If $\delta = 0$, then ξ is an isomorphism and $n = r_1 + \ldots + r_s - s$.

This proposition shows that the problem of realizing sets of characters satisfying the reciprocity law by elements of $\mathrm{Br}\, k(X)$ can be reduced to a similar problem for curves X_i defined over $\mathbf{R}$. Note that we are interested in real localizations only because for any local field k the group $H^2(k, J(\overline{k}))$ is trivial ([7]), and hence the corresponding obstruction group is trivial too.

3 Number points of real varieties

In Section 3 we shall show that a homomorphism

$$\zeta : H^2(k, \mathrm{Div}^0 \overline{X}) \longrightarrow H^2(k, J(\overline{k}))$$

has a right inverse and hence $\ker(\delta) = H^2(k, J(\overline{k}))$. This will imply immediately (as was shown in the previous section) that the localization ξ of the obstruction group Δ at all real places of k is isomorphic to the localization μ for the second cohomology group with coefficients in $J(\overline{k})$ and hence is an isomorphism. This will allow us to compute Δ and prove the splitting of the group $\ker(\Sigma)$.

In the real case sections for ζ_i can be constructed at once. To construct a right inverse for ζ in the number field case, we need some statement on points with odd degrees of its residue fields over k in real open neighborhoods in a variety defined over the number field k embedded into $\mathbf{R}$. In fact, we shall prove this statement for even and odd cases.

Let k be a subfield of $\mathbf{R}$ which is a number field. Suppose X is a smooth projective variety over k, $\dim X > 0$ and $X(k) \neq \emptyset$. For shortness we shall call points of $X(\overline{k})$ number points and points of $X(\mathbf{R})$ real points.

Lemma 2. *Let X/k be a smooth projective variety and $\dim X > 0$. Then any subset of $X(\mathbf{R})$ open in the real topology contains infinitely many number points.*

Proof. Since X is projective we can assume that X is a closed subvariety in $\mathbf{P}^n_k$ for some n. If $X = \mathbf{P}^n$, then Lemma 2 is obvious. So we shall assume that $r = \dim X < n$.

The set $\mathbf{P}^n(k) - X(k)$ is Zariski open and so is infinite. Let $x_1 \in \mathbf{P}^n(k) - X(k)$ and

$$\pi_1 : \mathbf{P}^n - \{x_1\} \longrightarrow \mathbf{P}^{n-1}$$

be the projection from the center x_1. It is a closed morphism, so $\pi_1(X)$ is a subvariety in $\mathbf{P}^{n-1}$. If there exists $x_2 \in \mathbf{P}^{n-1} - \pi_1(X)$, then take the projection

$$\pi_2 : \mathbf{P}^{n-1} - \{x_2\} \longrightarrow \mathbf{P}^{n-2}$$

from the center x_2, and so on. After finitely many steps we obtain the projection

$$\pi : X \longrightarrow \mathbf{P}^r$$

of the variety X onto $\mathbf{P}^r$ (here the dimension of the projective space is equal to r by the fiber dimension theorem).

Consider the morphism

$$\pi(\mathbf{R}) : X(\mathbf{R}) \longrightarrow \mathbf{P}^r(\mathbf{R})$$

induced by π. Since X and $\mathbf{P}^r$ are smooth, $\pi(\mathbf{R})$ is a morphism of r-dimensional real analytic varieties. Let W be an arbitrary open (in the real topology) subset of $X(\mathbf{R})$. Since the subset of points of $X(\mathbf{R})$ such that $\pi(\mathbf{R})$ is locally linear is dense in $X(\mathbf{R})$ (see [8], Part II, Chapter III, §10), the set W contains at least one such point. By definition of local linearity the morphism $\pi(\mathbf{R})$ is locally similar at x to some linear map $E \to F$ where E and F are r-dimensional real vector spaces (see [8]). Now since the fibres of $\pi(\mathbf{R})$ are finite, the map $E \to F$ is an isomorphism. Hence there exists an open subset U in W such that the restriction

$$\pi(\mathbf{R}) \mid_U : U \longrightarrow V = \pi(\mathbf{R})(U)$$

is a homeomorphism of U onto some open $V \subset \mathbf{P}^r(\mathbf{R})$. It is clear that V contains infinitely many number points. Then preimages of these points lying in $U \subset W$ are number points because π is a finite morphism.

q.e.d.

Lemma 3. *Let* $\dim X = 1$, $g_X \geq 1$, $x_1, \ldots, x_t \in X^1$, $t \geq 2g_X$, *and* $D := x_1 + \ldots + x_t \in \operatorname{Div} X$. *Then there exists a* k*-rational covering*

$$f : X \longrightarrow \mathbf{P}^1$$

such that $f^{-1}(0) = D$ *(i.e.* $f^{-1}(0) = \{x_1, ..., x_t\}$ *and all points* x_i *are unramified over* $0 = [0:1] \in \mathbf{P}^1$.

Proof. Let K_X be the canonical class on X,

$$\mathfrak{L}(D) = \{f \in k(X)^* \mid \operatorname{div}(f) + D \geq 0\}$$

for all $D \in \operatorname{Div} X$ and $l(D) = \dim_k \mathfrak{L}(D)$. Here $\operatorname{div}(f) = \sum \operatorname{ord}_x(f)x$ where x runs through X^1 and ord_x is the order function at x.

Let $n_i = \deg(x_i) = [k(x_i) : k]$. By Riemann-Roch Theorem,

$$l(D) = l(K_C - D) + \deg(D) - g_X + 1 \geq \deg(D) - g_X + 1 \ .$$

Since $n := \deg(D) \geq t \geq 2g_X$ and $g_X \geq 1$, we have

$$\deg(D) - g_X + 1 \geq 2g_X - g_X + 1 = g_X + 1 \geq 2 \ .$$

Thus

$$l(D) \geq 2 \ .$$

Apply Riemann-Roch Theorem once more:

$$l(D - x_i) - l(K_C - D + x_i) = \deg(D - x_i) - g_X + 1 =$$

$$= \deg(D) - n_i - g_X + 1 \ .$$

In fact, $l(K_C - D + x_i) = 0$. Indeed, since $\deg(K_X) = 2g_X - 2$, one gets

$$\deg(K_C - D + x_i) = \deg(K_C) + \deg(-D + x_i) =$$

$$= \deg(K_C) - n + n_i = 2g_X - 2 - n + n_i < 0$$

where the last inequality holds as $t \geq 2g_X$ and so $n - n_i \geq t - 1 > 2g_X - 2$. But then

$$\mathfrak{L}(K_C - D + x_i) = 0$$

since

$$\deg(\operatorname{div}(f)) + \deg(K_C - D + x_i) = \deg(K_C - D + x_i) \geq 0$$

if $f \in k(X)^*$ and

$$\operatorname{div}(f) + K_C - D + x_i \geq 0 \ .$$

This contradicts the inequality above. Finally, $l(K_C - D + x_i) = 0$, and so the equality obtained after the second application of the Riemann-Roch Theorem yields

$$l(D - x_i) = \deg(D) - g_X - n_i + 1 \ .$$

Keeping in mind this equality and applying the Riemann-Roch Theorem once more, we obtain

$$l(D - x_i) = \deg(D) - g_X - n_i + 1 < \deg(D) - g_X + 1 \leq l(D) \ .$$

Thus we have

$$l(D - x_i) < l(D), \quad \text{and} \quad l(D) \geq 2\,.$$

It means that the vector subspace $\mathfrak{L}(D - x_i)$ of the vector space $\mathfrak{L}(D)$ does not coincide with $\mathfrak{L}(D)$. But then

$$U = \mathfrak{L}(D) \backslash \cup_{i=1}^{n} \mathfrak{L}(D - x_i) \neq \emptyset$$

since a finite-dimensional vector space cannot be covered by a finite family of its proper subspaces. Let $h \in U$. Then the divisor $\operatorname{div}(h)$ has poles exactly at the points $x_1, \dots, x_t$, and the multiplicities of these poles are equal to 1. This implies immediately that the divisor $D' = D + \operatorname{div}(h)$ is effective and its support does not intersect the support of the effective divisor D. If $f := h^{-1}$ and

$$f : X \longrightarrow \mathbf{P}^1$$

is the covering corresponding to f, then $\operatorname{div}(f) = D - D'$ and $f^{-1}(0) = D$.

q.e.d.

Lemma 4. *Let* $\dim X = 1$, $f : X_{\mathbf{C}} \to \mathbf{P}^1_{\mathbf{C}}$ *be the covering defined by a non-constant* $\mathbf{R}$*-rational function* f *on* X *and*

$$f(\mathbf{R}) : X(\mathbf{R}) \to \mathbf{P}^1(\mathbf{R})$$

the corresponding map for $\mathbf{R}$*-rational points. Let* $x \in \mathbf{P}^1_{\mathbf{C}}$, $x \neq \infty$,

$$f^{-1}(x) = \{x_1, \dots, x_l, x_{l+1}, \dots, x_n\} \subset X(\mathbf{C})$$

where $\{x_1, \dots, x_l\} \subset X(\mathbf{R})$ *and* $\{x_{l+1}, \dots, x_n\} \not\subset X(\mathbf{R})$. *Assume that all points* x_i *(i=1,…,n) are unramified over* x. *Then there exist an open connected interval* $I \subset \mathbf{A}^1(\mathbf{R}) \subset \mathbf{P}^1(\mathbf{R})$ *and open intervals* $I_1, \dots I_l \subset X(\mathbf{R})$ *such that* $x \in I$, $x_i \in I_i$ *with* $i \leq l$ *and the restriction of* f *to* I_i *is a homeomorphism of* I_i *onto* I. *Moreover,* $f(\mathbf{R})^{-1}(I)$ *is a disjoint union of intervals* $I_1, \dots, I_l$.

Proof. Since $X(\mathbf{C})$ is a Riemann surface, f is a branch covering of the Riemann sphere $S_\infty = \mathbf{P}^1(\mathbf{C})$. Since each point x_i is unramified over x ($i = 1, \dots, n$), for any i there exists an open disk D_i on the Riemann surface $X(\mathbf{C})$ and open disk D on S_∞ such that $x \in D$, $x_i \in D_i$ and the restriction f on D_i defines a homeomorphism D_i onto D. One can assume that $D \subset \mathbf{A}^1(\mathbf{C}) \subset$

$\mathbf{P}^1(\mathbf{C})$ since $x \neq \infty$. Then the image S_i of the path-connected set $D_i \cap X(\mathbf{R})$ under the map $f(\mathbf{R})$ is linearly connected in $\mathbf{A}^1(\mathbf{R})$ and contains x as an internal point. It is clear that we can choose such an open interval I in $\mathbf{A}^1(\mathbf{R})$ that $x \in I$ and $I \subset \cap_i S_i$. Then $f(\mathbf{R})^{-1}(I)$ is a disjoint union of intervals $I_1, \ldots, I_l$ and $x_i \in I_i$ with $i \leq l$.

q.e.d.

Lemma 5. *Let* $\dim X = 1$, $f : X \to \mathbf{P}^1$ *be the covering defined by a non-constant k-rational function f on X and* $\Lambda = \{x \in k = \mathbf{A}^1 \subset \mathbf{P}^1 \mid \#f^{-1}(x) = 1\}$. *Then Λ is dense in* $\mathbf{R}$ *(with respect to the real topology).*

Proof. Since X is geometrically integral, k is algebraically closed in the function field $k(X)$ and $k(f)$ is a purely transcendental extension of k. Let F be the minimal polynomial of some primitive element of $k(X)$ over $k(f)$. Multiplying coefficients of F by the product of their denominators, one can assume that $F = F(f, y)$ is a polynomial in two variables over k. The principal ideal (F) is prime in $k[f, y]$, and an affine plane curve

$$X_F = \{(a, b) \in \mathbf{A}^2_{\overline{k}} \mid F(a, b) = 0\}$$

is geometrically irreducible. X is birationally isomorphic over k to X_F, and there is a commutative square

$$\begin{array}{ccc} X & \xrightarrow{f} & \mathbf{P}^1_k \\ \cong | & & | \\ X_F & \xrightarrow{f_{aff}} & \mathbf{A}^1_k \end{array} .$$

Let

$$\Lambda_F = \{\lambda \in k = \mathbf{A}^1(k) \subset \mathbf{P}^1 \mid f^{-1}_{aff}(\lambda)\} .$$

It is clear that $\Lambda - \Lambda_F$ is finite since f_{aff} and f coincide except finitely many points. But then Λ_F is dense in $\mathbf{R}$ provided Λ_F is dense.

If

$$\overline{f}_{aff} : X_F \times_k \overline{k} \longrightarrow \mathbf{A}^1_{\overline{k}}$$

is a morphism obtained from f_{aff} by a base extension, then $\lambda \in \Lambda_F$ if and only if $\overline{f}^{-1}_{aff}(\lambda)$ is an orbit of some point of $X(\overline{k})$ with respect to the action of $G = \mathrm{Gal}(\overline{k}/k)$. But then Λ_F is the set of $\lambda \in k$ such that the polynomial

$F(\lambda, y)$ remains irreducible over k. This means that Λ_F is a Hilbertian set and so Λ_F is dense in $\mathbf{R}$ (see [9]).

q.e.d.

Theorem. *Let $k \subset \mathbf{R}$, X/k be a smooth projective variety and* $\dim X > 0$. *If $X(k) \neq \emptyset$, then for any open (with respect to the real topology) $U \subset X(\mathbf{R})$ the subsets*

$$U_{odd} := \{x \in U \mid [k(x) : k] \text{ is odd}\}$$

and

$$U_{even} := \{x \in U \mid [k(x) : k] \text{ is even}\}$$

are infinite.

Proof. We shall use the induction on $\dim X$. Let $\dim X = 1$ and $p : \overline{X} = X \times_k \overline{k} \to X$ be the projection morphism. It is surjective and for any $x \in X$ the inverse image $p^{-1}(x)$ is the orbit of x under the action of G. According to Lemma 2, there exist infinitely many number points in U. Hence, we can choose a set $\{x_1, \ldots, x_n\} \subset X$ satisfying the following two conditions: $n > 2g_X - 1$ and $S' \cap U \neq \emptyset$ for $S' := \{p^{-1}(x_1), \ldots, p^{-1}(x_n)\}$. Consider a divisor $D' = x_1 + \ldots + x_n$ on X. Suppose, we want to prove that U_{odd} is infinite. Then let $D = D'$ and $S = S'$ if the number of real points of S is odd. Otherwise (i.e. if this number is even) let D be the sum of D' and some k-rational point $x_{n+1} \in X(k)$ and, respectively, let $S = S' \cup \{x_{n+1}\}$. Since $k \subset \mathbf{R}$, the point $x_{n+1} \in X(\mathbf{R})$. As a result, we shall conclude that if $\{y_1, \ldots, y_l\}$ is the set of real points of S, then l is odd.

The construction of the divisor D and Lemma 3 yield that there exists a k-rational covering

$$f : X \longrightarrow \mathbf{P}^1$$

such that $f^{-1}(0) = D$, i.e. the inverse image $f^{-1}(0)$ consists of the points x_i and each x_i is unramified over $0 = [0 : 1] \in \mathbf{P}^1$. Let

$$f(\mathbf{R}) : X(\mathbf{R}) \longrightarrow \mathbf{P}^1(\mathbf{R})$$

be the corresponding map of sets of real points. According to Lemma 4, there exist an open connected interval $I \subset \mathbf{A}^1(\mathbf{R}) \subset \mathbf{P}^1(\mathbf{R})$ and open intervals $I_1, \ldots I_l$ in $X(\mathbf{R})$ such that $0 = [0 : 1] \in I$, $y_i \in I_i$ for any $i \in \{1, \ldots, l\}$ and the restriction of the map $f(\mathbf{R})$ to I_i is a homeomorphism I_i onto I.

Furthermore, $f(\mathbf{R})^{-1}(I)$ is a disjoint union of the intervals $I_1, \ldots, I_l$. This implies immediately that for any point $\lambda \in I$ there exist just l real points in its inverse image $f(\mathbf{R})^{-1}(\lambda)$.

Now apply Lemma 5 to the morphism f. Let Λ be a dense (in the real topology) subset of $\mathbf{R}$ from Lemma 5. The intersection $\Lambda \cap I$ is infinite since Λ is dense. Let $\lambda \in \Lambda \cap I$. Since $\lambda \in \Lambda$, the inverse image $f^{-1}(\lambda)$ consists of a single point $x \in X$. Then $p^{-1}(x)$ is a G-orbit T of some number point. As $\lambda \in I$, the orbit T consists of exactly l real points. Note that the number of non-real points in the G-orbit of any number point is even. The construction of S shows that l is odd, so the number of points in T is also odd. This means that for any $y \in T$ the degree $[k(y) : k]$ is odd. By the choice of x_i we have $S \cap U \neq \emptyset$ and therefore $\{y_1, \ldots, y_l\} \cap U \neq \emptyset$. Taking if it is necessary subintervals of I_i containing the points $y_i \in U$, we can assume that such intervals I_i are subsets of U. Then real points of T contained in these I_i are number points of U with residue fields of odd degree over k. Moreover, since $\Lambda \cap I$ is infinite, we can choose λ in infinitely many ways. This means that there are infinitely many number points in U with residue fields of odd degree over k.

To prove the infinity of U_{even}, let us set $D = D'$ and $S = S'$ in the case where the number of real points of S is even, and $D = D' + x_{n+1}$, $S = S' \cup \{x_{n+1}\}$, $x_{n+1} \in X(k)$, otherwise. Then arguments similar to those above finish the proof of the theorem in the case $\dim X = 1$.

Assume now that the theorem is proved for $\dim X < n$, and let $\dim X = n$ and $x_0 \in X(k)$. Using Lemma 2, choose some number point $x_1' \in U$, and let $x_2 = p(x_1)$ where $p : \overline{X} \to X$ is the projection morphism. According to one of the Bertini type theorems, see [10], there exists a smooth section Z of X by some hupersurface in general position having degree big enough and meeting points x_0 and x_2. Then $x_0 \in Z$ and the subvariety $\overline{Z}$ of $\overline{X}$ meets point x_1. It follows that Z satisfies the assumptions of the theorem, $\dim(Z) < \dim(X)$ and $U \cap Z(\mathbf{R}) \neq \emptyset$. Then according to the inductive hypothesis, there are infinitely many number points $x \in U \cap Z(\mathbf{R}) \subset U$ such that $[k(x) : k]$ is odd and there are infinitely many number points $x \in U \cap Z(\mathbf{R}) \subset U$ such that $[k(x) : k]$ is even, so that U_{odd} and U_{even} are infinite.

q.e.d.

4 The proof of the main theorem

In this section we fix the notation of Section 1. In particular, k is a number field and s is the number of all real embeddings $\rho_i : k \hookrightarrow \mathbf{R}$, $i = 1, ..., s$, of k. For $s = 0$ we have $H^2(k, J(\overline{k})) = 0$ and Lemma 1 yields $\Delta = 0$ (and $\Delta \cong (\mathbf{Z}/2)^0 = 0$ according to formula in the Main theorem). In view of this we shall assume that $s > 0$. If all the real varieties $J_i(\mathbf{R})$ are connected, i.e. $r_1 = \ldots = r_s = 1$, then as it was shown in Section 1, again $H^2(k, J(\overline{k})) = 0$ and $\Delta = 0$. So we shall also assume that for at least one $i \in \{1, \ldots, s\}$ the real variety $J_i(\mathbf{R})$ is non-connected (i.e. $r_i > 1$). For convenience we shall assume that the embeddings $\rho_i : k \hookrightarrow \mathbf{R}$ are ordered in such a way that $r_i > 1$ for $i \in \{1, \ldots, t\}$ and $r_i = 1$ for $i \in \{t+1, \ldots, s\}$. Then the localization homomorphism μ is an isomorphism

$$\mu : H^2(k, J(\overline{k})) \overset{\cong}{\rightarrow} \bigoplus_{i=1}^{t} H^2(\mathbf{R}, J_i(\mathbf{C})) .$$

Let μ' be the composition of μ and the isomorphism between the direct sum of the second cohomology groups and the direct sum of the appropriate number of groups $\mathbf{Z}/2$:

$$\mu' : H^2(k, J(\overline{k})) \overset{\cong}{\rightarrow} \bigoplus_{i=1}^{t} (\mathbf{Z}/2)^{r_i - 1} .$$

As above, we shall denote the elements of $\mathbf{Z}/2$ by 0 and 1, so that $\mathbf{Z}/2 = \{0, 1\}$. Then elements of $\oplus_{i=1}^{t}(\mathbf{Z}/2)^{r_i-1}$ can be represented as tuples with components belonging to $\{0, 1\}$. For any $z \in \{1, \ldots, t\}$ we can enumerate the groups $\mathbf{Z}/2$ in the direct sum $(\mathbf{Z}/2)^{r_i-1}$ and denote by $h_{z,r}$, $1 \le r \le r_z - 1$, the cohomology class in $H^2(k, J(\overline{k}))$ such that

$$\mu'(h_{z,r}) = \{0, \ldots, 0, 1, 0, \ldots, 0\}$$

where 1 corresponds to the embedding ρ_z and the r-th copy of $\mathbf{Z}/2$ in the sum $(\mathbf{Z}/2)^{r_i-1}$. Then $\{h_{z,r}\}_{1 \le z \le t, 1 \le r \le r_z - 1}$ is a set of independent generators for $H^2(k, J(\overline{k}))$ and each class $h_{z,r}$ has an order 2. This implies that if for any (z, r) there exists a cohomology class $h'_{z,r} \in H^2(k, \operatorname{Div}^0 \overline{X})$ such that $\zeta(h'_{z,r}) = h_{z,r}$ and the order of $h'_{z,r}$ is 2, then a right inverse homomorphism to ζ can be constructed by sending $h_{z,r}$ to the class $h'_{z,r}$ and extending this correspondence to a section of ζ.

To prove the existence of such a class $h'_{z,r}$, let $z \in \{1,\dots,t\}$, and $r \in \{1,\dots,r_z-1\}$ be arbitrary fixed indices. Set for shortness $h = h_{z,r}$ and let $E = \rho_z(k)$ be a subfield of $\mathbf{R}$.

Let I be the variety defined by the Cartesian square

$$\begin{array}{ccc} I & \longrightarrow & \operatorname{Spec} E \\ \downarrow & & \downarrow \cong \\ J & \longrightarrow & \operatorname{Spec} k \end{array}$$

where the isomorphism $\operatorname{Spec} E \cong \operatorname{Spec} k$ is induced by the embedding ρ_z. It is clear that $J_z = I \times_E \mathbf{R}$. Since J and therefore I are abelian varieties, $I(E) \neq \emptyset$. Then I is a variety over the number subfield E of $\mathbf{R}$ satisfying the assumptions of the theorem proven in the previous section. According to this theorem, there exists a point $P \in I(\mathbf{R}) = J_z(\mathbf{R})$ such that P belongs to the connected component of $J_z(\mathbf{R})$ which the isomorphism $J_z(\mathbf{R})/\operatorname{Nm} J_z(\mathbf{C}) \cong (\mathbf{Z}/2)^{r_z-1}$ sends to the tuple $\{0,\dots,0,1,0,\dots,0\}$ where 1 corresponds to the r-th copy of $\mathbf{Z}/2$, and the degree $[E(P):E]$ is odd.

The left vertical arrow in the latter cartesian square is the isomorphism which induces an isomorphism $J \times_k \mathbf{C} \cong I \times_k \mathbf{C}$ where the both products are determined by the extention τ_z (see Section 1). Let T be the point of $J \times_k \mathbf{C}$ corresponding to P under this isomorphism, and $L = k(T)$. Then it is clear that $[L:k] = [E(P):E]$ is odd. Set $H = \operatorname{Gal}(\overline{k}/k)$.

Observe now that for any embedding ρ_i, $i \in \{1,\dots,t\}$, there exists at least one real embedding of L lying over it because $[L:k]$ is odd. For any $i \in \{1,...,t\}$ fix an embedding $\varrho_i : L \hookrightarrow \mathbf{R}$ over ρ_i, and let $\{\varrho_{t+1},\dots,\varrho_l\}$ be all the remaining real embeddings of L. Choose and fix an embedding $\omega_i : \overline{k} \hookrightarrow \mathbf{C}$ lying over ϱ_i, $1 \le i \le l$. Without loss of generality we can assume $\tau_i = \omega_i$ for $i \le t$. In particular, $\tau_z = \omega_z$.

From now on for any $i \in \{1,\dots,l\}$ we shall denote by $[i]$ an index in $\{1,\dots,t\}$ determined by condition that $[i] = i$ for $i \le t$ and $\rho_{[i]} = \omega_i\mid_k$ otherwise.

As in Section 1, any embedding ω_i induces the injective homomorphisms

$$\omega_i^- : <\sigma> \hookrightarrow H$$

and

$$\omega_i^+ : J(\overline{k}) \hookrightarrow J_{[i]}(\mathbf{C}) \,.$$

Each pair (ω_i^-, ω_i^+) induces the homomorphism

$$\nu_i : H^2(L, J(\overline{k})) \longrightarrow H^2(\mathbf{R}, J_j(\mathbf{C})) \ .$$

The elements $\nu_1, \ldots, \nu_l$ determine the localization homomorphism

$$\nu : H^2(L, J(\overline{k})) \longrightarrow \bigoplus_{i=1}^{l} H^2(\mathbf{R}, J_{[i]}(\mathbf{C}))$$

which is also an isomorphism. For any $i \leq t$ there is a commutative square

$$\begin{array}{ccc} H^2(k, J(\overline{k})) & \xrightarrow{\mu_i} & H^2(\mathbf{R}, J_i(\mathbf{C})) \\ \mathrm{res} \downarrow & & \downarrow 1 \\ H^2(L, J(\overline{k})) & \xrightarrow{\nu_i} & H^2(\mathbf{R}, J_i(\mathbf{C})) \end{array}$$

where the left vertical arrow is the restriction homomorphism and the right one is the identity. Taking the sums of the right sides of such commutative squares for all $1 \leq i \leq t$, we shall obtain the commutative square

$$\begin{array}{ccc} H^2(k, J(\overline{k})) & \xrightarrow{\mu} & \bigoplus_{i=1}^{t} H^2(\mathbf{R}, J_i(\mathbf{C})) \\ \mathrm{res} \downarrow & & \downarrow 1 \\ H^2(L, J(\overline{k})) & \longrightarrow & \bigoplus_{i=1}^{t} H^2(\mathbf{R}, J_i(\mathbf{C})) \end{array}$$

and then also the commutative square

$$\begin{array}{ccc} H^2(k, J(\overline{k})) & \xrightarrow{\mu} & \bigoplus_{i=1}^{t} H^2(\mathbf{R}, J_i(\mathbf{C})) \\ \mathrm{res} \downarrow & & \downarrow f' \\ H^2(L, J(\overline{k})) & \xrightarrow{\nu} & \bigoplus_{i=1}^{l} H^2(\mathbf{R}, J_{[i]}(\mathbf{C})) \end{array} \quad .$$

Here f' sends a t-tuple $(0, \ldots, 0, \alpha, 0, \ldots, 0)$ with $\alpha \in H^2(\mathbf{R}, J_i(\mathbf{C}))$ corresponding to an index i to a l-tuple $(0, \ldots, 0, \alpha, 0, \ldots, 0)$ where α corresponds to the index i as well. Finally, replacing the groups $H^2(\mathbf{R}, J_i(\mathbf{C}))$ by the direct sums of the groups $\mathbf{Z}/2$, we shall obtain the commutative square

$$\begin{array}{ccc} H^2(k, J(\overline{k})) & \xrightarrow{\mu'} & \bigoplus_{i=1}^{t} (\mathbf{Z}/2)^{r_i - 1} \\ \mathrm{res} \downarrow & & \downarrow f \\ H^2(L, J(\overline{k})) & \xrightarrow{\nu'} & \bigoplus_{i=1}^{l} (\mathbf{Z}/2)^{r_{[i]} - 1} \end{array}$$

where the homomorphism f is induced by f' and ν' is induced by ν.

This commutative square permits us to describe an element h as the image under the corestriction map

$$\mathrm{cor} : H^2(L, J(\overline{k})) \to H^2(k, J(\overline{k}))$$

of some generator of $H^2(L, J(\overline{k}))$.

First of all, we shall prove the following lemma which shows that each automorphism $\sigma_i := \omega_i^-(\sigma)$ is separated from the other automorphisms $\sigma_j := \omega_j^-(\sigma)$, $j \neq i$, by a subgroup of H of index 2 (it is clear that all $\sigma_i \in H$).

Lemma 6. *For any $i \in \{1, \ldots, l\}$ there exists a subgroup U of index 2 in group H such that $\sigma_i \in U$ and $\sigma_j \in H - U$ if $j \neq i$.*

Proof. First, let $l > 1$. According to the Artin-Whaples approximation theorem, for any positive real number ε there exists $a \in L$ such that

$$\mid \varrho_i(a) - 1 \mid < \varepsilon$$

and

$$\mid \varrho_j(a) + 1 \mid < \varepsilon$$

for $j \neq i$ (here $\mid \mid : \mathbf{R} \to \mathbf{R}_+ \cup \{0\}$ is the canonical absolute value on $\mathbf{R}$). If ε is sufficiently small, then $\varrho_i(a) > 0$ and $\varrho_j(a) < 0$ if $j \neq i$. Assume that $a = b^2$ for some $b \in L$. Then $\varrho_j(a) = (\varrho_j(b))^2 \geq 0$, and we have a contradiction if $j \neq i$. So $L(\sqrt{a})$ is a quadratic extension of L. Let $U = \mathrm{Gal}(\overline{k}/L(\sqrt{a}))$. Since $\varrho_i(a) > 0$, then $\omega_i(L(\sqrt{a})) \subset \mathbf{R}$ and hence $\sigma_i \in U$. For $j \neq i$ we have $\varrho_j(a) < 0$ and $\omega_j(L(\sqrt{a})) \not\subset \mathbf{R}$, so $\sigma_j \notin U$.

For $s = 1$ let ord be some discrete valuation of L with local parameter π. By the Artin-Whaples approximation theorem, there exists an $a \in L$ which is sufficiently near to π^3 with respect to the topology defined by this valuation and sufficiently near to 1 with respect to the topology defined by the unique real embedding ϱ_1. Then firstly, $\varrho_1(a) > 0$ and secondly, a is a non-square in L, since if $a = b^2$, then $3 = \mathrm{ord}(a) = 2\,\mathrm{ord}(b)$ which yields a contradiction. Take $U = \mathrm{Gal}(\overline{k}/L(\sqrt{a}))$.

q.e.d.

Now let W be an arbitrary subgroup of H of index 2. Denote by χ_W the continious character of H corresponding to W. Let $\hat{\chi}_W : H \to \mathbf{Q}$ be the continious map such that $\hat{\chi}_W(x) = 0$ if $x \in W$ and $\hat{\chi}_W(x) = 1/2 + \mathbf{Z}$ otherwise. If

∂ denotes a differentiation on cochains of H with coefficients in $\mathbf{Q}$, then $\partial\hat{\chi}_W$ is a 2-cocycle of H with coefficients in $\mathbf{Z}$ and its cohomology class $\mathrm{cls}(\partial\hat{\chi}_W)$ is the image of χ_W under the connecting homomorphism $H^1(L, \mathbf{Q}/\mathbf{Z}) \to H^2(k, \mathbf{Z})$. Denote by $< T >$ the subgroup of $J(\overline{k})$ generated by an L-rational point T and by $\phi_{W,T}$ the composition of $\partial\hat{\chi}_W$ and the homomorphism $\mathbf{Z} \to < T >$ sending 1 to T. Then

$$\phi_{W,T}(g_1, g_2) = \begin{cases} T & \text{if } g_1, g_2 \in H - W \\ O & \text{otherwise} \end{cases}$$

where O is the identity element in $J(\overline{k})$.

Let U be a subgroup of H of index 2 such that $\sigma_z \in U$ and $\sigma_i \in H - U$ if $i \neq z$. Such a subgroup exists according to Lemma 6. Let also $V = \mathrm{Gal}(\overline{k}/L(\sqrt{-1}))$, and set

$$\phi = \phi_{V,T} + \phi_{U,T} \ .$$

Then we have

Lemma 7. *Let* $\mathrm{cor} : H^2(L, J(\overline{k})) \to H^2(k, J(\overline{k}))$ *be the corestriction map and* ϕ *be the 2-cocycle constructed above. Then*

$$h = h_{z,r} = \mathrm{cor}(\mathrm{cls}(\phi)) \ .$$

Proof. Let us show that $\nu(\mathrm{cls}(\phi)) = (0, ..., 0, 1, 0, ..., 0)$ where 1 corresponds to the embedding ϱ_z and the r-th direct summand $\mathbf{Z}/2$ of $(\mathbf{Z}/2)^{r_z-1}$.

The component of the tuple $\nu'(cls(\phi))$ corresponding to the embedding ϱ_i and the a-th direct summand $\mathbf{Z}/2$ of $(\mathbf{Z}/2)^{r_{[i]}-1}$ is equal to 0 (respectively, to 1) if the sum

$$\omega_i^+(\phi(1, \sigma_i) + \phi(\sigma_i, \sigma_i))$$

is contained in the connected component of $J_{[i]}(\mathbf{R})$ which is sent to the tuple with the a-th component equal to 0 (respectively, to 1) by the isomorphism $J_{[i]}(\mathbf{R})/\operatorname{Nm} J_{[i]}(\mathbf{C}) \cong (\mathbf{Z}/2)^{r_{[i]}-1}$.

Since the identity 1 of G is contained in every subgroup of G, the formula above for $\phi_{W,T}$ shows that $\phi(1, \sigma_i) = 0$ for any i. Let us compute $\omega_i^+(\phi(\sigma_i, \sigma_i))$.

Note for this that since $L(\sqrt{-1})$ is totally imaginary, $\sigma_i \notin V$ for any i. If $i \neq z$, then $\sigma_i \notin U$ in view of Lemma 6. Then it follows from the formula for $\phi_{W,T}$ that

$$\omega_i^+(\phi(\sigma_i, \sigma_i)) = \omega_i^+(2T) = 2\omega_i^+(T) \ .$$

Since ω_i is an embedding over the real embedding ϱ_i of L, $\omega_i^+(2T)$ is contained in $2J_{[i]}(\mathbf{R}) \subset \mathrm{Nm}\, J_{[i]}(\mathbf{C})$. If $i = z$, we obtain

$$\omega_z^+(\phi(\sigma_i, \sigma_i)) = \omega_z^+(T) = \tau_z^+(T) = P$$

since the element $\sigma_z \in U$.

So we have that the component of $\nu(cls(\phi))$ corresponding to ϱ_i and the a-th direct summand $\mathbf{Z}/2$ of $(\mathbf{Z}/2)^{r_{[i]}-1}$ is equal to 1 only for $i = z$ and $a = r$.

But then $\nu'(\mathrm{cls}(\phi)) = f(\mu'(h))$. In view of commutativity of the last square we have $\nu'(\mathrm{res}(h)) = \nu'(\mathrm{cls}(\phi))$. Since ν' is an isomorphism,

$$\mathrm{res}(h) = \mathrm{cls}(\phi) \ .$$

Finally, since $H^2(k, J(\overline{k}))$ is of exponent 2 and $[L : k]$ is odd,

$$h = [L : k]h = \mathrm{cor}(\mathrm{res}(h)) = \mathrm{cor}(\mathrm{cls}(\phi)) \ .$$

q.e.d.

The L-rationality of $T \in J(\overline{k})$ and the condition $X(k) \neq \emptyset$ imply that there exists an L-rational divisor $D_T \in \mathrm{Div}^0\,\overline{X_L}$ such that $\Lambda_L(D_T) = T$ where $\Lambda_L : \mathrm{Div}^0\,\overline{X_L} \to J(\overline{k})$ is the canonical epimorphism. Let $\Phi_{W,T}$ be a continious map from $H \times H$ to $\mathrm{Div}^0\,\overline{X_L}$ defined by

$$\Phi_{W,T}(g_1, g_2) = \begin{cases} D_T & \text{if } g_1, g_2 \in H - W \\ 0 & \text{otherwise .} \end{cases}$$

It is clear that the composition of $\Phi_{W,T}$ and Λ_L yields the cocycle $\phi_{W,T}$. Moreover, the map $\Phi_{W,T}$ is itself a 2-cocycle of H since the divisor D_T is rational over L. Specialize the group W and set

$$\Phi = \Phi_{V,T} + \Phi_{U,T}$$

where V and U are subgroups of H introduced above. Let also

$$\zeta_L : H^2(L, \mathrm{Div}^0\,\overline{X_L}) \to H^2(L, J(\overline{k}))$$

be a homomorphism induced by Λ_L. Then $\zeta_i(\mathrm{cls}(\Phi)) = \mathrm{cls}(\phi)$ where $\mathrm{cls}(\phi)$ is the cohomology class mentioned in Lemma 7.

Note that corestriction homomorphisms of cohomology groups commute with homomorphisms of cohomology groups induced by homomorphisms of discrete modules. So we have a commutative square

$$\begin{array}{ccc} H^2(k, \mathrm{Div}^0\,\overline{X}) & \xrightarrow{\zeta} & H^2(k, J(\overline{k})) \\ \mathrm{cor}\uparrow & & \uparrow\mathrm{cor} \\ H^2(L, \mathrm{Div}^0\,\overline{X_L}) & \xrightarrow{\zeta_L} & H^2(L, J(\overline{k})) \end{array} \quad .$$

Then

$$h = \mathrm{cor}(\mathrm{cls}(\phi)) = \mathrm{cor}(\zeta_L(\mathrm{cls}(\Phi))) = \zeta(\mathrm{cor}(\mathrm{cls}(\Phi))) \ .$$

In view of the construction of the cocycle Φ we observe that Φ is a sum of two cocyles of the form $\Phi_{W,T}$, where W is a subgroup of H of index 2. Since the restriction of the 2-cocycle $\Phi_{W,T}$ to $W \times W$ is trivial, $\mathrm{res}(\mathrm{cls}(\Phi_{W,T})) = 0$ where res is the restriction homomorphism of the cohomology induced by an extension of the L to the invariant field of W. Now if cor is the corresponding corestriction map, then $2\,\mathrm{cls}(\Phi_{W,T}) = \mathrm{cor} \circ \mathrm{res}(\mathrm{cls}(\Phi_{W,T})) = 0$. Consequently, $2\,\mathrm{cls}(\Phi) = 0$ and

$$2\,\mathrm{cor}(\mathrm{cls}(\Phi)) = 0$$

where cor is the corestriction induced by the extention L/k. Since $h = \zeta(\mathrm{cor}(\mathrm{cls}(\Phi)))$ and $h \neq 0$, we have $\mathrm{cor}(\mathrm{cls}(\Phi)) \neq 0$. Hence $\mathrm{cor}(\mathrm{cls}(\Phi))$ is of order 2. Set $h'_{z,r} = \mathrm{cor}(\mathrm{cls}(\Phi))$.

Thus for any generator $h = h_{z,r}$ of $H^2(k, J(\overline{k}))$ we constructed an element $h'_{z,r}$ of order 2 in $H^2(k, \mathrm{Div}^0\,\overline{X})$ such that $\zeta(h'_{z,r}) = h_{z,r}$. Extending by linearity the correspondence

$$h_{z,r} \mapsto h'_{z,r} \ ,$$

we shall obtain a homomorphism from $H^2(k, J(\overline{k}))$ to $H^2(k, \mathrm{Div}^0\,\overline{X})$ which is right inverse to ζ.

This implies immediately that $\mathrm{im}(\zeta) = H^2(k, J(\overline{k})) = \ker(\delta)$. By Lemma 1 and the proposition proven in Section 1, we have

$$\Delta \cong \ker(\delta) \cong (\mathbf{Z}/2)^{r_1+\ldots+r_s-s} \ ,$$

and the localization homomorphism

$$\xi : \Delta \longrightarrow \bigoplus_{i=1}^{s} \Delta_i$$

is an isomorphism. Moreover, the exact sequence

$$0 \to \mathrm{im}(\mathrm{inv}) \longrightarrow \ker(\Sigma) \longrightarrow \Delta \to 0$$

splits, so

$$\ker(\Sigma) \cong \mathrm{im}(\mathrm{inv}) \oplus \Delta \cong \mathrm{im}(\mathrm{inv}) \oplus (\mathbf{Z}/2)^{r_1+\ldots+r_s-s} \ .$$

The main theorem is proved.

Institute of Mathematics
Academy of Sciences of Belarus
11 Surganova str.
Minsk 220072, Belarus
e-mail: guletskii@im.bas-net.by
e-mail: yanch@im.bas-net.by

References

[1] J.-L. Colliot-Thélène (with the collaboration of J.-J.Sansuc). *The rationality problem for fields of invariants under linear algebraic groups (with special regard to the Brauer group).* Unpublished Lecture Notes from the 9th ELAM, Santiago de Chile, 1988.

[2] V.I.Guletskiĭ, V.I.Yanchevskiĭ. *Ramification and reciprocity laws in Brauer groups of function fields of numerical curves of genus one.* St. Petersburg Math. J. Vol. 8 (1997), no. 5, pp. 863-877.

[3] V.I.Guletskiĭ. *Invariants of simple algebras over function fields of homogeneous spaces defined over number fields.* Vesti AN Belarusi (1996) no. 3, pp. 64-68 (in Russian).

[4] B.M.Becker. *Reciprocity laws for algebras over function fields.* Mat. Zametki. Vol 17 (1975), no. 3, pp. 419-422 (in Russian).

[5] M.Knebusch. *On Algebraic Curves over Real Closed Fields* - I. Math. Z. Bd.150 (1976), pp.49-70.

[6] J.S.Milne. *Arithmetic Duality Theorems.* Perspectives in Mathematics. Vol.1. Academic Press, 1986.

[7] J.-P.Serre. *Galois cohomology.* Springer-Verlag, 1964.

[8] J.-P.Serre. *Lie Algebras and Lie Groups.* Benjamin, 1965.

[9] S.Lang. *Fundamentals of Diophantine Geometry.* Springer-Verlag, 1983.

[10] S.L.Kleiman, A.B.Altman. *Bertini theorems for hypersurface sections containing a subscheme.* Communications in Algebra, 7 (8), 775-790 (1979).