Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Rony A. BITAN

**The Geometric Gauss–Dedekind**

Tome 37, nº 1 (2025), p. 373-387.

https://doi.org/10.5802/jtnb.1325



CENTRE MERSENNE

*Le* Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

*Journal de Théorie des Nombres*
*de Bordeaux* **37** (2025), 373–387

# The Geometric Gauss–Dedekind

par Rony A. BITAN

Résumé. Gauss et Dedekind ont établi une bijection entre l'ensemble des $\mathrm{SL}_2(\mathbb{Z})$-orbites de $\mathbb{Z}$-formes quadratiques binaires positives de discriminant fixé et le groupe des classes de l'anneau des entiers du corps quadratique imaginaire de même discriminant. En utilisant la cohomologie étale, nous montrons un analogue de cette correspondance en caractéristique positive. Cela nous ramène à la description de l'ensemble des genres et à un autre résultat, analogue à celui de Gauss, selon lequel toute forme composée avec elle-même appartient au genre principal.

Abstract. Gauss and Dedekind have shown a bijection between the set of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of positive binary quadratic $\mathbb{Z}$-forms of the discriminant of an imaginary quadratic field and the class group of its ring of integers. Using étale cohomology we show an analogue of this correspondence in the positive characteristic. This leads to the description of the set of genera and to another result analogous to Gauss' one by which any form composed with it belongs to the principal genus.

## 1. Introduction

Let $R$ be a unital commutative domain, $M$ an $R$-module of rank 2 and $N$ an invertible $R$-module. A map $q : M \to N$ is called a *binary quadratic map* if $q(rx) = r^2 q(x)$ for all $x \in M, r \in R$, and the induced symmetric map

$$B_q : M \times M \longrightarrow N : \ (x,y) \longmapsto q(x+y) - q(x) - q(y)$$

is $R$-bilinear ([18, §6]). In particular if $N = R$, this $q$ is the familiar binary *quadratic form* ([19, §5.3.5]). The quadratic module $(M,q)$ is called *primitive* if $Rq(M) = N$. In that case, fixing an $R$-basis $\{e_1, e_2\}$ of $M$, there exist co-prime elements $a, b, c \in R$ such that:

$$\widetilde{q}(X,Y) := q(Xe_1 + Ye_2) = aX^2 + bXY + cY^2.$$

For brevity we denote $q = (a,b,c)$. Throughout, all quadratic maps will be assumed primitive.

Manuscrit reçu le 19 décembre 2023, révisé le 7 décembre 2024, accepté le 17 janvier 2025.
2020 *Mathematics Subject Classification.* 11R65, 14G17, 14G25.
*Mots-clefs.* Quadratic binary forms over integer rings of global fields of positive characteristic.

Let $A$ be a quadratic $R$-algebra. It admits a standard involution $\sigma$, thus a norm map $n_A : A \to R : x \mapsto x\sigma(x)$. Given an invertible $A$-module $M$ equipped with a quadratic map $q : M \to N$, we say that $(M, q)$ is *of type* $A$, if $q$ is compatible with $n_A$, namely, if it satisfies $q(xa) = q(x)n_A(a)$ for all $x \in M, a \in A$ (cf. [19, III, §7.2]). M. Kneser showed in ([18, Prop. 2]), that given an invertible $A$-module $M$, there exists a unique pair $(N, q)$ up to isomorphism, such that $(M, q)$ is primitive of type $A$.

A change of variables by $H \in \mathrm{GL}(M)$, such that the quadratic map $q' = q \circ H$ is still defined over $R$, is called an *isometry* of $q$. It is *proper* if $\det(H) = 1$ and *improper* otherwise. If $H$ is proper and defined over an $R$-algebra $S$, then $q'$ is said to be *equivalent modulo* $\mathrm{SL}_2(S)$ to $q$. The *discriminant* of $q$, up to $R$-equivalence, is defined as the coset ([9, §2.1])

$$\mathrm{disc}(q) := \det(B_q) \cdot (R^\times)^2 \in R/(R^\times)^2,$$

where $\det(B_q)$ stands for $\det(B_q(e_i, e_j))$.

**Definition 1.1.** Given $\Delta \in R/(R^\times)^2$ we set:

$$\begin{aligned} \mathfrak{cl}_0(\Delta) &:= \{\text{primitive quadratic forms } q : \mathrm{disc}(q) = \Delta\}/\,\mathrm{SL}_2(R) \\ \subseteq \mathfrak{cl}_1(\Delta) &:= \{\text{primitive quadratic maps } q : \mathrm{disc}(q) = \Delta\}/\,\mathrm{SL}_2(R). \end{aligned}$$

If $\mathrm{Pic}(R) = 1$ then $\mathfrak{cl}_0(\Delta) = \mathfrak{cl}_1(\Delta)$. A coarser classification, up to also improper isometries, is:

$$\mathfrak{cl}(\Delta) := \{q : \mathrm{disc}(q) = \Delta\}/\,\mathrm{GL}_2(R).$$

Over a domain of positive characteristic there is no notion of a definite quadratic form (positive or negative). We may generalize this concept by defining *definite forms* as the representatives in

$$\mathfrak{cl}_1'(\Delta) := \mathfrak{cl}_1(\Delta)/[q] \sim [\lambda q] \;:\; \lambda \in R^\times - (R^\times)^2.$$

Over $R = \mathbb{Z}$ for which $(R^\times)^2 = 1$, a discriminant is an integer $d$ and

$$[q] \sim [\lambda q] \;:\; \lambda \in R^\times - (R^\times)^2$$

gives $[q] \sim [-q]$, which means (when $d < 0$) that any positive definite form is identified with its negative, thus $\mathfrak{cl}_1'(d)$ classifies the positive ones.

Gauss, in his famous *Disquisitiones Arithmeticae* [12], defined the composition law of two binary quadratic $R$-forms. Later, R. Dedekind identified the obtained group structure with the one of an abelian group; given an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$, $d < 0$ is squarefree, with ring of integers $\mathcal{O}_K$ and discriminant $\Delta_K$ there is a bijection of pointed sets:

$$\mathfrak{cl}_1'(\Delta_K) \xrightarrow{\sim} \mathrm{Pic}(\mathcal{O}_K) : \;[(a,b,c)] \longmapsto \left[\left\langle a, \frac{b - \sqrt{\Delta_K}}{2}\right\rangle\right],$$

where $\mathrm{Pic}(\mathcal{O}_K)$ is the Picard group of $\mathcal{O}_K$ ([11, Thm. 58]).

M. Kneser showed in [18, p. 412] in 1982, that quadratic modules of type $A$, where $A$ is a quadratic $R$-algebra, are classified by $\mathrm{Pic}(A)$. In 1991, M. A. Knus in [19, IV §5], used étale cohomology in the nondegenerate case to classify regular quadratic $R$-forms with trivial Arf invariant. M. M. Wood has proved in [25] in 2011, using actions on the symmetric space of a quadratic module, a similar correspondence over $R$, but without restricting to positive definite forms (which are not defined in the positive characteristic).

In this paper, assuming $R$ is a domain in which 2 is invertible, due to a recent result of [1] regarding the smoothness of the special orthogonal group $\underline{\mathrm{SO}}_q$ of a quadratic form $q$ with squarefree discriminant, thus being primitive (though maybe degenerate), we generalize the cohomological approach to such quadratic forms and maps.

In Section 2 we form a bijection of pointed sets, having a structure of an abelian group: $\mathfrak{cl}_0(\mathrm{disc}(q)) \cong H^1_{\text{ét}}(R, \underline{\mathrm{SO}}_q)$. The above new definition of definite forms leads us in Section 3 to formulate the following correspondence, which is a general constructive analogue of the one of Dedekind, in the geometric case (Theorem 3.1 below):

**Theorem 1.2.** *Given a finite field $\mathbb{F}$ of odd characteristic, let $k/\mathbb{F}(x)$ be an imaginary extension and $\mathcal{O}$ the domain of $k$-elements regular everywhere away of the prime $\infty_k$ lying over $\infty = \langle 1/x \rangle$. Let $K/k$ be a geometric imaginary quadratic extension and $\mathcal{O}_K$ the domain of $K$-elements regular everywhere away of the prime $\infty_K|\infty_k$, with discriminant $\Delta_K = -\alpha(\mathbb{F}^\times)^2$, $\alpha \in \mathcal{O}$. There is an isomorphism of abelian groups:*

$$\widetilde{i}_* : \mathfrak{cl}'_1(\Delta_K) \xrightarrow{\sim} \mathrm{Pic}(\mathcal{O}_K) : \ [(a,b,c)] \longmapsto [\langle a, b/2 + \sqrt{\alpha} \rangle] \, .$$

In Section 4 we show that the above coarser classification $\mathfrak{cl}(\Delta)$ (which is not necessarily a group), is bijective to: $\mathfrak{cl}_1(\Delta)/([q] \sim [q^{\mathrm{op}}])$, where for $q = (a,b,c)$, $q^{\mathrm{op}} = (a,-b,c)$. Similarly: $\mathfrak{cl}'(\Delta_K) = \mathfrak{cl}'_1(\Delta_K)/([q] \sim [q^{\mathrm{op}}])$.

For any prime $\mathfrak{p}$ of $k$ let $\widehat{\mathcal{O}}_\mathfrak{p}$ be the completion of $\mathcal{O}$ with respect to the discrete valuation induced by $\mathfrak{p}$. The *principal genus* $\mathrm{Cl}_\infty(q)$ of $q$ is the set of classes of $\mathcal{O}$-forms that are properly $K$- and $\widehat{\mathcal{O}}_\mathfrak{p}$-isomorphic to $q$ for any $\mathfrak{p}$. In Section 5, after dividing the classes in $\mathfrak{cl}_1(\mathrm{disc}(q))$ into genera, we prove in Corollary 5.4 another result analogous to a one of Gauss in characteristic 0: denote by $\star$ the operation in the group $\mathfrak{cl}_0(\mathrm{disc}(q))$. Then for any $[q'] \in \mathfrak{cl}_0(\mathrm{disc}(q))$ one has: $[q' \star q'] \in \mathrm{Cl}_\infty(q)$. In Section 6 an application towards elliptic curves is demonstrated.

## 2. Torsors of norm forms

From now on $R$ is a domain in which 2 is invertible, with fraction field $k$. Schemes defined over $\mathrm{Spec}\, R$ are underlined, omitting the underline for the generic fiber over $k$. Given a binary primitive quadratic $R$-form $q : M \to R$, the *orthogonal group* of $(M, q)$ is the affine $R$-group of its self isometries ([19, p. 8]):

$$\underline{\mathrm{O}}_q := \{H \in \underline{\mathrm{GL}}(M) : q \circ H = q\}.$$

As 2 is a unit in $R$, the *special orthogonal subgroup* $\underline{\mathrm{SO}}_q$ is $\ker[\underline{\mathrm{O}}_q \xrightarrow{\det} \underline{\mathbb{G}}_m]$ ([8, §1,p.1]), and since $\mathcal{O}$ is an integral domain, det factors through the group $\underline{\mu}_2 = \operatorname{Spec} R[t]/(t^2-1)$ ([7, Lem. 4.3.0.21]), thus we may just write $\underline{\mathrm{SO}}_q := \ker[\underline{\mathrm{O}}_q \overset{\det}{\twoheadrightarrow} \underline{\mu}_2]$.

Let $A$ be a quadratic $R$-algebra. If $A$ has a basis $\Omega$ over $R$, inducing a representation $\varphi_\Omega : \underline{\mathrm{Aut}}(A) \hookrightarrow \underline{\mathrm{GL}}_2$, then the above norm $n_A$ coincides with $\det \circ \varphi_\Omega$ ([2, Def. 2.3]). In particular, let $\Omega := \{1, \sqrt{\alpha}\}$ where $\alpha \neq 0$ is a nonsquare element of $R$. The quadratic $R$-algebra $A_\alpha := R\langle\Omega\rangle = R \oplus \sqrt{\alpha}R$ is closed under multiplication and contains $R$, thus carries a ring structure. The Weil restriction of scalars $\underline{\mathrm{R}} := \mathrm{Res}_{A_\alpha/R}(\underline{\mathbb{G}}_m)$, is a two-dimensional $R$-group whose generic fiber is a $k$-torus. The group of points $\underline{\mathrm{R}}(R)$, via its isomorphism with $A_\alpha^\times$ [6, §7.6], naturally acts on $A_\alpha$ through its basis $\Omega$, yielding a canonical embedding of $\underline{\mathrm{R}}$ in $\underline{\mathrm{Aut}}(A_\alpha)$. We get a commutative diagram:

$$\begin{array}{ccccc} \underline{\mathrm{R}} & \hookrightarrow & \underline{\mathrm{Aut}}(A_\alpha) & \overset{\varphi_\Omega}{\hookrightarrow} & \underline{\mathrm{GL}}_2 \\ & {\scriptstyle n_\alpha}\searrow\!\!\searrow & & \swarrow\!\!\swarrow{\scriptstyle \det} & \\ & & \underline{\mathbb{G}}_m & & \end{array}.$$

Consider the $R$-group $\underline{\mathrm{N}} := \ker[\underline{\mathrm{R}} \xrightarrow{n_\alpha} \underline{\mathbb{G}}_m]$. Its generic fiber N is a one-dimensional $k$-torus. At any prime $\mathfrak{p}$ the map applied to the reductions $\overline{R}_\mathfrak{p} \xrightarrow{(n_\alpha)_\mathfrak{p}} (\overline{\mathbb{G}}_m)_\mathfrak{p}$ cannot be trivial as $\overline{R}_\mathfrak{p}$ is two-dimensional, thus the local norm $(n_\alpha)_\mathfrak{p}$ is surjective, hence $n_\alpha$ as well. This surjectivity holds even at a ramified prime $\mathfrak{p}|\langle\det(B_q)\rangle$ in which $\underline{\mathrm{R}}_\mathfrak{p} = \operatorname{Spec} \widehat{\mathcal{O}}_\mathfrak{p}[x,y,t]/(t(x^2-\alpha y^2)-1)$ is not reductive.

**Lemma 2.1.** *The scheme* $\underline{\mathrm{N}}$ *is flat over* $\operatorname{Spec} R$.

*Proof.* The schemes in $\underline{\mathrm{R}} \xrightarrow{n_\alpha} \underline{\mathbb{G}}_m$ are smooth (e.g., [10, Cor. A.5.4]), hence regular and Cohen–Macaulay, thus it suffices to check that all the geometric fibers of $\underline{\mathrm{N}} = \ker(n_\alpha)$ are one-dimensional. This is guaranteed by the surjectivity of $n_\alpha$. □

The quadratic module $(A_\alpha, q_\alpha)$ where

$$\widetilde{q}_\alpha(X,Y) = q_\alpha(X + \sqrt{\alpha}Y) := n_\alpha(X + \sqrt{\alpha}Y) = X^2 - \alpha Y^2$$

i.e., $q_\alpha = (1, 0, -\alpha)$ is of type $A_\alpha$ ([19, III, p. 164]). From now on, just $n$ and $q$ will stand for $n_\alpha$ and $q_\alpha$, respectively.

**Remark 2.2.** As $\det(B_q)$ is squarefree and 2 is invertible, according to [1, Prop. 2.3.] $\underline{\mathrm{O}}_q$ and $\underline{\mathrm{SO}}_q$ are smooth (thus flat). Then by the correspondence between flat closed subschemes of $\underline{\mathrm{O}}_q$ and closed subschemes of the generic fiber $\mathrm{O}_q$ [16, Prop. 2.8.1], $\underline{\mathrm{SO}}_q$ is the unique flat and closed subgroup of $\underline{\mathrm{O}}_q$ whose generic fiber is $\mathrm{SO}_q$.

**Lemma 2.3.** $\underline{\mathrm{SO}}_q = \underline{\mathrm{N}}$.

*Proof.* Recall that $\underline{\mathrm{N}} \subset \underline{\mathrm{SL}}(A_\alpha)$. Then:

$$\begin{aligned}\underline{\mathrm{SO}}_q &= \{a \in \underline{\mathrm{SL}}(A_\alpha) : q \circ a = q\} \\ &\supseteq \{a \in \underline{\mathrm{N}} : q \circ a = q\} \\ &= \{a \in \underline{\mathrm{N}} : q(xa) = q(x) \cdot n(a) = q(x) \ \ \forall\, x \in A_\alpha\} \\ &= \{a \in \underline{\mathrm{N}} : n(a) = 1\} = \underline{\mathrm{N}}.\end{aligned}$$

Both groups $\underline{\mathrm{SO}}_q$ and $\underline{\mathrm{N}}$ are $\mathcal{O}$-flat (see Remark 2.2 and Lemma 2.1) closed subgroups of $\underline{\mathrm{O}}_q$. Thus, the injection holds for the generic fibers as well. This injection is an equality as both groups $\mathrm{SO}_q$ and N are one-dimensional $k$-tori, implying by Remark 2.2, that $\underline{\mathrm{SO}}_q = \underline{\mathrm{N}}$. ☐

Given an affine $R$-group scheme $\underline{G}$, a *$\underline{G}$-torsor in the étale topology* is a sheaf of sets on $R$ equipped with a (right) $\underline{G}$-action, which is locally trivial in the étale topology. The pointed set $H^1_{\text{ét}}(R, \underline{G})$ classifies these $\underline{G}$-torsors up to $R$-isomorphisms. The following correspondence is due to Giraud (see [7, §2.2.4]):

**Proposition 2.4.** *Let $S$ be a scheme and $X_0$ an object of a fibered category of schemes defined over $S$. Let* $\mathrm{Aut}(X_0)$ *be its $S$-group of automorphisms. Let* $\mathfrak{Forms}(X_0)$ *be the category of $S$-forms that are locally isomorphic for some topology to $X_0$, and let* $\mathfrak{Tors}(\mathrm{Aut}(X_0))$ *be the category of* $\mathrm{Aut}(X_0)$*-torsors in that topology.*

$$\mathfrak{Forms}(X_0) \longrightarrow \mathfrak{Tors}(\mathrm{Aut}(X_0)) : \ X \longmapsto \mathrm{Iso}(X_0, X)$$

*is an equivalence of fibered categories.*

In particular the category of torsors of $\underline{\mathrm{O}}_q = \underline{\mathrm{Aut}}(q)$ in the étale topology is equivalent to the one of $R$-schemes of the form $\mathrm{Iso}(q, q')$ where $q'$ is a quadratic $R$-form étale-equivalent to $q$. Its associated *discriminant algebra* is $D(q') = (\wedge^2 M', \det(q'))$ and its isomorphism class in $H^1_{\text{ét}}(R, \underline{\mu}_2)$ is its *Arf invariant.*

Being diagonal, $q = (1, 0, -\alpha)$ admits the improper isometry $\mathrm{diag}(1, -1)$ defined over $R$, so $\underline{\mathrm{O}}_q(R) \xrightarrow{\det} \underline{\mu}_2(R)$ is surjective. Then étale cohomology applied to the exact sequence of smooth $R$-groups:

$$1 \longrightarrow \underline{\mathrm{SO}}_q \longrightarrow \underline{\mathrm{O}}_q \xrightarrow{\det} \underline{\mu}_2 \longrightarrow 1, \tag{2.1}$$

gives rise to the exact sequence of pointed-sets:

$$1 \longrightarrow H^1_{\text{ét}}(R, \underline{\mathrm{SO}}_q) \longrightarrow H^1_{\text{ét}}(R, \underline{\mathrm{O}}_q) \xrightarrow{\det_*} H^1_{\text{ét}}(R, \underline{\mu}_2), \tag{2.2}$$

where $\det_*([\mathrm{Iso}(q,q')]) = [D(q')] - [D(q)]$ in $H^1_{\text{ét}}(R, \underline{\mu}_2)$ (preserving the base point, [15, IV, Prop. 4.3.4]). By the exactness of (2.2), $\mathrm{Iso}(q,q')$ represents a class in $H^1_{\text{ét}}(R, \underline{\mathrm{SO}}_q) = \ker(\det_*)$ if and only if $q'$ is equivalent to $q$ in the étale topology and shares the Arf invariant of $q$.

**Lemma 2.5.** *The map* $\psi : H^1_{\text{ét}}(R, \underline{\mathrm{SO}}_q) \cong \mathfrak{cl}_0(\mathrm{disc}(q)) : [\mathrm{Iso}(q,q')] \mapsto [q']$ *is a bijection of pointed sets having a structure of an abelian group.*

*Proof.* A representative $\mathrm{Iso}(q,q')$ in $H^1_{\text{ét}}(R, \underline{\mathrm{SO}}_q)$ satisfies $[D(q')] = [D(q)]$ in $H^1_{\text{ét}}(R, \underline{\mu}_2)$. The latter is equivalent to $\det(B_{q'}) = a^2 \det(B_q)$ for some $a \in \mathbb{F}^\times$ ([19, III, §3.3]), i.e., to $\mathrm{disc}(q') = \mathrm{disc}(q)$. Identifying these sets of representatives modulo proper isometries by $\psi$, $\mathfrak{cl}_0(\mathrm{disc}(q))$ is identified with $H^1_{\text{ét}}(R, \underline{\mathrm{SO}}_q)$ and inherits its structure of the abelian group, as $\underline{\mathrm{SO}}_q = \underline{\mathrm{N}}$ (Lemma 2.3) is commutative. □

**Example 2.6.** Let $q = (1, 0, x)$ be a quadratic form defined over $R = \mathbb{F}_5[x]$. Then $q' = (2, 0, x)$ cannot represent a class in $H^1_{\text{ét}}(R, \underline{\mathrm{SO}}_q)$ as $\mathrm{disc}(q) \neq \mathrm{disc}(q')$, though representing a class in $H^1_{\text{ét}}(R, \underline{\mathrm{O}}_q)$; fixing $a$ such that $a^2 = 2$, $H = \mathrm{diag}(a, 1)$ is an isometry $q \to q'$ defined over an étale cover of $R$. The form $q'' = (4, 0, x)$, however, being $R$-equivalent to $q$ by $H = \mathrm{diag}(2, 1)$, represents a class in $H^1_{\text{ét}}(R, \underline{\mathrm{SO}}_q)$, but not the one of $q$ as $H$ cannot be proper.

Given a set $\Omega' = \{\omega_1, \omega_2\}$, set the vector $\overline{\Omega'} = \binom{\omega_1}{\omega_2}$ and notice that $q' = q \circ H$ can be written as $\widetilde{q}'(X,Y) = \widetilde{q}((X,Y) \cdot H)$, or, equivalently, as

$$q'((X,Y) \cdot \overline{\Omega}) = q((X,Y) \cdot \overline{\Omega'})$$

where $\overline{\Omega'} = H \cdot \overline{\Omega}$. We denote $\Omega'$ briefly by $H\Omega$.

**Lemma 2.7.** *The map* $\widetilde{i}_*([q \circ H]) = [R\langle H\Omega \rangle]$ *forms an exact sequence of pointed-sets:*

$$1 \longrightarrow R^\times / n(A_\alpha^\times) \longrightarrow \mathfrak{cl}_1(-\alpha(R^\times)^2) \xrightarrow{\widetilde{i}_*} \mathrm{Pic}(A_\alpha) \longrightarrow 1.$$

*Proof.* Applying étale cohomology to the short exact sequence of smooth $R$-groups:

$$1 \longrightarrow \underline{\mathrm{N}} \xrightarrow{i} \underline{\mathrm{R}} \xrightarrow{n} \underline{\mathbb{G}}_m \longrightarrow 1, \tag{2.3}$$

being commutative, gives rise to a short exact sequence of abelian groups:

$$1 \longrightarrow R^\times / n(A_\alpha^\times) \xrightarrow{\delta} H^1_{\text{ét}}(R, \underline{\mathrm{N}}) \xrightarrow{i_*} H^1_{\text{ét}}(R, \underline{\mathrm{R}}), \tag{2.4}$$

in which $H^1_{\text{ét}}(R, \underline{\mathrm{R}})$ is isomorphic as an abelian group by Shapiro's Lemma to $H^1_{\text{ét}}(A_\alpha, \underline{\mathbb{G}}_m) \cong \mathrm{Pic}(A_\alpha)$. A representative $\mathrm{Iso}(q, q \circ H)$ in $H^1_{\text{ét}}(R, \underline{\mathrm{N}} = \underline{\mathrm{SO}}_q)$

(Lemma 2.3) corresponds to the quadratic $R$-module $(R\langle H\Omega\rangle, q\circ H)$ with trivial Arf-invariant. Its class is mapped by $i_*$ to $[\mathrm{Iso}(A_\alpha, R\langle H\Omega\rangle)]$ in $H^1_{\text{ét}}(A_\alpha, \mathbb{G}_m = \mathrm{Aut}(A_\alpha))$ ([15, V, 3.1.1.1]), or, equivalently, to $[R\langle H\Omega\rangle]$ in $\mathrm{Pic}(A_\alpha)$ (forgetting the quadratic form, see the proof of [18, Thm. 3]). By Lemma 2.5 $i_*$ can be replaced by $i_*([q\circ H]) = [R\langle H\Omega\rangle]$ in:

$$(2.5) \qquad 1 \longrightarrow R^\times/n(A_\alpha^\times) \xrightarrow{\psi\circ\delta} \mathfrak{cl}_0(-\alpha(R^\times)^2) \xrightarrow{i_*} \mathrm{Pic}(A_\alpha).$$

The extension $\widetilde{i}_*$ of $i_*$ to $\mathfrak{cl}_1(-\alpha(R^\times)^2)$, including all quadratic *maps* of the discriminant $-\alpha(R^\times)^2$, is surjective; any representative $P$ in $\mathrm{Pic}(A_\alpha)$ corresponds up to isomorphism to a primitive quadratic $R$-map $q_P$ such that the quadratic module $(P, q_P)$ is of type $A_\alpha$ (see Section 1). This $q_P$ which can be taken to be the norm $n_P$ induced by the standard involution on $P$ ([19, III, Prop. 7.3.1]), is locally everywhere equivalent to $n$ ([19, III, Rmk. 7.3.4]), implying that:

$$(2.6) \qquad \exists\, a \in \bigcap_{\mathfrak{p}\in\mathrm{Spec}\,R} \widehat{\mathcal{O}}_{\mathfrak{p}}^\times = R^\times : \det(B_{n_P}) = a^2\det(B_n),$$

thus $\mathrm{disc}(n_P) = \mathrm{disc}(n)$ and so $[n_P] \in \mathfrak{cl}_1(-\alpha(R^\times)^2)$. This amounts in the asserted exact sequence. □

**Remark 2.8.** Each fiber of the surjection $i_* : [(P, q_P)] \to [P]$, forgetting as above the quadratic map $q_P$, bijects with the kernel $R^\times/n(A_\alpha^\times)$, thus $\mathfrak{cl}_1(-\alpha(R^\times)^2)$ can be endowed a-priori with the structure of an abelian group, being $R^\times/n(A_\alpha^\times) \times \mathrm{Pic}(A_\alpha)$.

## 3. Dedekind correspondence: the geometric case

Let $\mathbb{F}(x)$ be the field of rational functions over a finite field $\mathbb{F}$ of odd characteristic. Any finite non-scalar extension $k$ of $\mathbb{F}(x)$ can be viewed as the function field of some projective, smooth and geometrically connected $\mathbb{F}$-curve $C$. Each closed point $\mathfrak{p}$ on $C$ gives rise to a discrete valuation on $k$. Let $\widehat{\mathcal{O}}_{\mathfrak{p}}$ be the ring of integers in the completion $\widehat{k}_{\mathfrak{p}}$ of $k$ with respect to $v_{\mathfrak{p}}$. Throughout, $k$ is assumed *imaginary*, namely, the prime $\infty = \langle 1/x\rangle$ in $\mathbb{F}(x)$ does not split into distinct places in $k$ (cf. [21]). Let $\infty_k$ be the unique prime of $k$ lying above $\infty$, regarded as a closed point on $C$. Then the ring of regular functions on the affine curve $C^{\mathrm{af}} := C - \{\infty_k\}$ is a Dedekind domain:

$$\mathcal{O} := \mathbb{F}[C^{\mathrm{af}}] = \{x \in k : v_{\mathfrak{p}}(x) \geq 0 \ \ \forall\, \mathfrak{p} \neq \infty_k\}.$$

This leads to the geometric analogue of the Dedekind correspondence:

**Theorem 3.1.** *Given a finite field $\mathbb{F}$ of odd characteristic, let $k/\mathbb{F}(x)$ be an imaginary extension and $\mathcal{O}$ the domain of $k$-elements regular everywhere away of the prime $\infty_k$ lying over $\infty = \langle 1/x\rangle$. Let $K/k$ be a geometric imaginary quadratic extension and $\mathcal{O}_K$ the domain of $K$-elements regular* *everywhere away of the prime* $\infty_K|\infty_k$*, with discriminant* $\Delta_K = -\alpha(\mathbb{F}^\times)^2$*,* $\alpha \in \mathcal{O}$*. There is an isomorphism of abelian groups:*

$$\widetilde{i}_* : \mathfrak{cl}_1'(\Delta_K) \xrightarrow{\sim} \mathrm{Pic}(\mathcal{O}_K) : \ [(a,b,c)] \longmapsto [\langle a, b/2 + \sqrt{\alpha}\rangle]\ .$$

*Proof.* First we see that $\mathcal{O}_K = A_\alpha$ for some (non-scalar) $\alpha \in \mathcal{O}$. As a (maximal) order over $\mathcal{O}$, $\mathcal{O}_K$ is a free $\mathcal{O}$-module of rank 2, thus admits a basis $\{1, t\}$ over $\mathcal{O}$, where $t$ is an algebraic integer thus a root of a monic quadratic polynomial over $\mathcal{O}$, i.e., there exist $m, n \in \mathcal{O}$ s.t. $t^2 + mt + n = 0$. Taking $t$ to be the root $\frac{\sqrt{m^2-4n}}{2} - \frac{m}{2}$, we see that $\mathcal{O}_K = A_\alpha$ for $\alpha = m^2 - 4n$.

Consider the exact sequence in Lemma 2.7 for $R = \mathcal{O}$:

$$1 \longrightarrow \mathcal{O}^\times/n(A_\alpha^\times) \xrightarrow{\delta} \mathfrak{cl}_1(\Delta_K) \xrightarrow{\widetilde{i}_*} \mathrm{Pic}(A_\alpha) \longrightarrow 1.$$

Notice that $\mathcal{O}^\times = \mathbb{F}^\times$, and as $K$ is imaginary one has $n(A_\alpha^\times) = (\mathbb{F}^\times)^2$ ([22, Ex. 1]). A representative $\lambda$ in $\mathcal{O}^\times/n(A_\alpha^\times) \cong \mathbb{F}^\times/(\mathbb{F}^\times)^2$ is mapped by $\delta$ to $[\lambda q] \in \mathfrak{cl}_1(\Delta_K)$, hence $\mathfrak{cl}_1(\Delta_K)/\operatorname{Im}(\delta) \cong \mathfrak{cl}_1'(\Delta_K)$ (recall by Remark 2.8 that $\mathfrak{cl}_1(\Delta_K)$ has a group structure).

Explicitly, starting by a general $\mathcal{O}$-form $q_L = (a,b,c)$ of discriminant $\Delta_K = -\alpha(\mathbb{F}^\times)^2$ ($c$ can be taken to be $\frac{b^2/4-\alpha}{a}$), we have $q_L = q \circ H_L$ where $H_L = \frac{1}{\sqrt{a}}\left(\begin{smallmatrix} a & 0 \\ b/2 & 1\end{smallmatrix}\right)$. As $\det(H_L) = 1$, $[q_L] \in \mathfrak{cl}_1'(\Delta_K)$. By Lemma 2.7:

$$\widetilde{i}_*([q_L]) = \left[\mathcal{O}\left\langle H_L\Omega = \frac{1}{\sqrt{a}}\{a, b/2 + \sqrt{\alpha}\}\right\rangle\right] = [\langle a, b/2 + \sqrt{\alpha}\rangle]$$

in $\mathrm{Pic}(\mathcal{O}_K)$ (the two ideals differ by tensoring with a principal one). □

**Remark 3.2.** The exact sequence (2.4) was obtained similarly in [4, (2.3)] for $R = \mathbb{Z}$, only for the flat cohomology, as $\underline{\mathrm{N}}$ may not be smooth at 2 which is not a unit in $\mathbb{Z}$, and the map $i_*$ is surjective there, as the following right term $\mathrm{Pic}(R)$ is trivial for $R = \mathbb{Z}$. In both cases $\ker(\delta)$ is $R^\times/n(A_\alpha^\times)$, but its non-trivial coset differs: while for $R = \mathcal{O}$ it is represented by $\lambda \in \mathbb{F}^\times - (\mathbb{F}^\times)^2$, for $R = \mathbb{Z}$ it is $-1$ (for $K = \mathbb{Q}(\sqrt{d}), d < 0$). This explains in what sense the identification of two definite forms in our $\mathfrak{cl}_1'(\Delta_K)$ in Definition 1.1, is analogous to the one over $\mathbb{Z}$.

**Remark 3.3.** Given a form $q = (a,b,c)$, we call $q^{\mathrm{op}} = (a,-b,c)$ its *opposite form.* By Theorem 3.1 the tensor product in $\mathrm{Pic}(\mathcal{O}_K)$ induces by a group operation in $\mathfrak{cl}_1'(\mathrm{disc}(q))$:

$$[q_{L_1}] \star [q_{L_2}] = \widetilde{i}_*^{-1}([L_1 \otimes L_2]),$$

and $[q]^{-1} = [q^{\mathrm{op}}]$. Indeed, let $L^{\mathrm{op}}$ be the ideal corresponding to $q^{\mathrm{op}}$. Then:

$$\begin{aligned} I = L \otimes L^{\mathrm{op}} &= \langle a, \sqrt{a} + b/2\rangle \otimes \langle a, \sqrt{\alpha} - b/2\rangle \\ &= \langle a^2, a(\sqrt{\alpha} + b/2), a(\sqrt{\alpha} - b/2), b^2/4 - \alpha\rangle. \end{aligned}$$

But $b^2/4 - \alpha = ac$, thus $I \subseteq \langle a \rangle$. On the other hand, both $L$ and $L^{\mathrm{op}}$ are primitive, thus $\langle a \rangle \subseteq I$, whence $I = \langle a \rangle$ is principal.

## 4. Not necessarily proper classification

In this section we study a less narrow classification of all primitive binary quadratic $\mathcal{O}$-maps of a common given discriminant, namely, up to *proper and improper* $\mathcal{O}$-isometries

$$\mathfrak{cl}(\Delta) := \{q : \mathrm{disc}(q) = \Delta\} / \mathrm{GL}_2(\mathcal{O}).$$

Given a smooth $\mathcal{O}$-group $\underline{G}$ and a representative $P$ in $H^1_{\acute{e}t}(\mathcal{O}, \underline{G})$, the quotient of $P \times_{\mathcal{O}} \underline{G}$ by the $\underline{G}$-action, $(p, g) \mapsto (ps^{-1}, sgs^{-1})$, is an affine $\mathcal{O}$-group scheme ${}^P\underline{G}$, being an inner form of $\underline{G}$, called the *twist* of $\underline{G}$ by $P$ (e.g., [24, §2.2]).

**Lemma 4.1.** $\mathfrak{cl}(\Delta) \cong \mathfrak{cl}_1(\Delta)/([q] \sim [q^{\mathrm{op}}])$.

*Proof.* As $B_q = \mathrm{diag}(1, -\alpha)$, the short exact sequence of smooth $\mathcal{O}$-groups of (2.1):

$$1 \longrightarrow \underline{\mathrm{SO}}_q \longrightarrow \underline{\mathrm{O}}_q \xrightarrow{\det} \underline{\mu}_2 \longrightarrow 1$$

splits by the section mapping the non-trivial element in $\underline{\mu}_2$ to $\mathrm{diag}(1, -1)$ in $\underline{\mathrm{O}}_q$, i.e., $\underline{\mathrm{O}}_q$ is isomorphic to $\underline{\mathrm{SO}}_q \rtimes \underline{\mu}_2$. Then according to [13, Lem. 2.6.3] we get:

$$H^1_{\acute{e}t}(\mathcal{O}, \underline{\mathrm{O}}_q) = \coprod_{[P] \in H^1_{\acute{e}t}(\mathcal{O}, \underline{\mu}_2)} H^1_{\acute{e}t}(\mathcal{O}, {}^P\underline{\mathrm{SO}}_q)/\underline{\mu}_2(\mathcal{O}), \tag{4.1}$$

in which $\underline{\mu}_2(\mathcal{O})$ acts on the set of representatives of $H^1_{\acute{e}t}(\mathcal{O}, {}^P\underline{\mathrm{SO}}_q)$ by $\mathrm{diag}(1, \pm 1)$. If $P$ is a trivial $\underline{\mu}_2$-torsor, then $H^1_{\acute{e}t}(\mathcal{O}, {}^P\underline{\mathrm{SO}}_q = \underline{\mathrm{SO}}_q) \cong \mathfrak{cl}_0(\Delta)$ by Lemma 2.5. Otherwise, if $P$ represents a non-trivial $\underline{\mu}_2$-torsor, then the corresponding twisted form has a distinct Arf-invariant than the one of $q$, which thereby does not belong to $H^1_{\acute{e}t}(\mathcal{O}, \underline{\mathrm{SO}}_q)$ (see sequence (2.2)). Consequently, $\mathfrak{cl}(\Delta)$ is identified with the first component in the decomposition (4.1), thus to $\mathfrak{cl}_0(\Delta)$ extended to $\mathfrak{cl}_1(\Delta)$ modulo $\underline{\mu}_2(\mathcal{O})$, such that any quadratic map is identified with its opposite by $\mathrm{diag}(1, -1)$. $\square$

Applying the quotient in Lemma 4.1 to $\mathfrak{cl}'_1(\Delta_K)$ gives by Theorem 3.1:

**Corollary 4.2.** *Let $K/k$ be a geometric quadratic extension of imaginary fields. There is a bijection of pointed sets (compare with* [4, Rmk. 5.20]*):*

$$\mathfrak{cl}'(\Delta_K) \cong \mathrm{Pic}(\mathcal{O}_K)/(x \sim x^{-1});\ [(a, b, c)] \longmapsto [\langle a, \sqrt{\alpha} - b/2 \rangle]$$

*thus $\mathfrak{cl}'(\Delta_K)$ remains a group if and only if* $\exp(\mathrm{Pic}(\mathcal{O}_K)) \le 2$.

## 5. Genera and the principal genus

Let $\underline{G}$ be an affine $\mathcal{O}$-group scheme with generic fiber $G$. The group of $k$-points $G(k)$ is embedded diagonally in the adelic group $\underline{G}(\mathbb{A})$, in which $\underline{G}(\mathbb{A}_\infty) := G(k_\infty) \times \prod_{\mathfrak{p} \neq \infty_k} \underline{G}(\mathcal{O}_\mathfrak{p})$ is also a subgroup. The *class set* of $\underline{G}$ is the finite set of double cosets ([5, Prop. 3.9]):

$$\mathrm{Cl}_\infty(\underline{G}) := \underline{G}(\mathbb{A}_\infty)\backslash \underline{G}(\mathbb{A})/G(k).$$

Given furthermore, that $\underline{G}$ is of finite type and smooth (not necessarily connected), it suits by Y. Nisnevich [23, Thm. I.3.5] into an exact sequence of pointed sets

$$1 \longrightarrow \mathrm{Cl}_\infty(\underline{G}) \longrightarrow H^1_{\text{ét}}(\mathcal{O}, \underline{G}) \xrightarrow{\varphi} H^1(k, G) \times \prod_{\mathfrak{p} \neq \infty_k} H^1_{\text{ét}}(\widehat{\mathcal{O}}_\mathfrak{p}, \underline{G}_\mathfrak{p}). \tag{5.1}$$

Let $[\xi_0] := \varphi([\underline{G}])$. The *principal genus* of $\underline{G}$ is then $\varphi^{-1}([\xi_0])$, i.e., the set of classes of $\underline{G}$-torsors that are generically and locally trivial at all primes of $\mathcal{O}$. More generally, a *genus* of $\underline{G}$ is any fiber $\varphi^{-1}([\xi])$ where $[\xi] \in \mathrm{Im}(\varphi)$. The *set of genera* of $\underline{G}$ is then:

$$\mathrm{gen}(\underline{G}) := \{\varphi^{-1}([\xi]) \ : \ [\xi] \in \mathrm{Im}(\varphi)\},$$

whence $H^1_{\text{ét}}(\mathcal{O}, \underline{G})$ is a disjoint union of its genera. The left exactness of sequence (5.1) reflects the fact that $\mathrm{Cl}_\infty(\underline{G})$ coincides with the principal genus of $\underline{G}$. If there is an embedding

$$\forall\, \mathfrak{p} \neq \infty_k : H^1_{\text{ét}}(\widehat{\mathcal{O}}_\mathfrak{p}, \underline{G}_\mathfrak{p}) \hookrightarrow H^1(\widehat{k}_\mathfrak{p}, G_\mathfrak{p}) \tag{5.2}$$

then as in [23, Cor. I.3.6], the sequence (5.1) simplifies to

$$1 \longrightarrow \mathrm{Cl}_\infty(\underline{G}) \longrightarrow H^1_{\text{ét}}(\mathcal{O}, \underline{G}) \longrightarrow H^1(k, G), \tag{5.3}$$

which indicates that any $\underline{G}$-torsor belongs to the principal genus of $\underline{G}$ if and only if it is $k$-isomorphic to it. More precisely, there is an exact sequence of pointed sets (cf. [14, Cor. A.8])

$$1 \longrightarrow \mathrm{Cl}_\infty(\underline{G}) \longrightarrow H^1_{\text{ét}}(\mathcal{O}, \underline{G}) \longrightarrow B \longrightarrow 1, \tag{5.4}$$

in which

$$B = \left\{ [\gamma] \in H^1(k, G) : \begin{array}{l} \forall\, \mathfrak{p} \neq \infty_k, \\ [\gamma \otimes \widehat{\mathcal{O}}_\mathfrak{p}] \in \mathrm{Im}\big(H^1_{\text{ét}}(\widehat{\mathcal{O}}_\mathfrak{p}, \underline{G}_\mathfrak{p}) \to H^1(\widehat{k}_\mathfrak{p}, G_\mathfrak{p})\big) \end{array} \right\}.$$

Let $K/k$ be a finite Galois extension, $\mathfrak{p}$ be a prime of $k$ and $\mathfrak{P}$ be a prime of $K$ dividing $\mathfrak{p}$. Write $\widehat{k}_\mathfrak{p}$ and $\widehat{K_\mathfrak{P}}$ for the completions of $k$ at $\mathfrak{p}$ and of $K$ at $\mathfrak{P}$, respectively, noting that $\widehat{K_\mathfrak{P}}$ is independent of the choice of $\mathfrak{P}$ up to isomorphism. The norm map $\mathrm{Nr} : K \to k$ extends the above norm $n : \mathcal{O}_K \to \mathcal{O}$ and induces local maps $\mathrm{Nr} : K \otimes_k \widehat{k}_\mathfrak{p} \to \widehat{k}_\mathfrak{p}$; under the isomorphism above this corresponds to the product of the norm maps $\mathrm{Nr}_{K_\mathfrak{P}/k_\mathfrak{p}}$ on the components. Similarly, $\mathcal{O}_K \otimes_\mathcal{O} \widehat{\mathcal{O}}_\mathfrak{p} \simeq \mathcal{O}^r_{\hat{K}_\mathfrak{P}}$. Write $U_\mathfrak{p}$ and

$U_{\mathfrak{P}}$ for $\widehat{\mathcal{O}}_{\mathfrak{p}}^{\times}$ and $\mathcal{O}_{\hat{K}_{\mathfrak{P}}}^{\times}$, respectively. The short exact sequence of smooth $\widehat{\mathcal{O}}_{\mathfrak{p}}$-groups (see Section 2)

$$1 \longrightarrow \underline{\mathrm{N}}_{\mathfrak{p}} \longrightarrow \underline{\mathrm{R}}_{\mathfrak{p}} \longrightarrow (\underline{\mathbb{G}}_m)_{\mathfrak{p}} \longrightarrow 1$$

yields by étale cohomology the exact and functorial sequence

$$1 \longrightarrow \underline{\mathrm{N}}_{\mathfrak{p}}(\widehat{\mathcal{O}}_{\mathfrak{p}}) \longrightarrow \underline{\mathrm{R}}_{\mathfrak{p}}(\widehat{\mathcal{O}}_{\mathfrak{p}}) \cong U_{\mathfrak{P}}^r \xrightarrow{\mathrm{Nr}} U_{\mathfrak{p}} \longrightarrow H^1_{\text{ét}}(\widehat{\mathcal{O}}_{\mathfrak{p}}, \underline{\mathrm{N}}_{\mathfrak{p}}) \longrightarrow 1,$$

since $H^1_{\text{ét}}(\widehat{\mathcal{O}}_{\mathfrak{p}}, \underline{\mathrm{R}}_{\mathfrak{p}})$ is the Picard group of a product of local rings and thus vanishes.

We deduce an isomorphism

$$H^1_{\text{ét}}(\widehat{\mathcal{O}}_{\mathfrak{p}}, \underline{\mathrm{N}}_{\mathfrak{p}}) \cong U_{\mathfrak{p}} / \mathrm{Nr}(U_{\mathfrak{P}}^r) = U_{\mathfrak{p}} / \mathrm{Nr}_{\hat{K}_{\mathfrak{P}}/\hat{k}_{\mathfrak{p}}}(U_{\mathfrak{P}}).$$

Applying Galois cohomology to the short exact sequence of $\widehat{k}_{\mathfrak{p}}$-groups

$$1 \longrightarrow \mathrm{N}_{\mathfrak{p}} \longrightarrow \mathrm{R}_{\mathfrak{p}} \longrightarrow (\mathbb{G}_m)_{\mathfrak{p}} \longrightarrow 1$$

gives rise to the exact sequence of abelian groups

$$1 \longrightarrow \mathrm{N}_{\mathfrak{p}}(\widehat{k}_{\mathfrak{p}}) \longrightarrow \underline{\mathrm{R}}_{\mathfrak{p}}(\widehat{k}_{\mathfrak{p}}) \cong (\widehat{K_{\mathfrak{P}}^{\times}})^r \xrightarrow{\mathrm{Nr}} \widehat{k}_{\mathfrak{p}}^{\times} \longrightarrow H^1(\widehat{k}_{\mathfrak{p}}, \mathrm{N}_{\mathfrak{p}}) \longrightarrow 1,$$

where the rightmost term vanishes by Hilbert's Theorem 90. Hence we may again deduce a functorial isomorphism $H^1(\widehat{k}_{\mathfrak{p}}, \mathrm{N}_{\mathfrak{p}}) \cong \widehat{k}_{\mathfrak{p}}^{\times} / \mathrm{Nr}_{\hat{K}_{\mathfrak{P}}/\hat{k}_{\mathfrak{p}}}(\widehat{K_{\mathfrak{P}}^{\times}})$. Note that $U_{\mathfrak{P}}$ is compact and thus $\mathrm{Nr}_{\hat{K}_{\mathfrak{P}}/k_{\mathfrak{p}}}(U_{\mathfrak{P}})$ is closed in $k_{\mathfrak{p}}^{\times}$. Only units have norms that are units, so we obtain an embedding of groups:

$$\text{(5.5)} \quad H^1_{\text{ét}}(\mathcal{O}_{\mathfrak{p}}, \underline{\mathrm{N}}_{\mathfrak{p}}) \cong U_{\mathfrak{p}} / \mathrm{Nr}_{\hat{K}_{\mathfrak{P}}/\hat{k}_{\mathfrak{p}}}(U_{\mathfrak{P}}) \hookrightarrow \widehat{k}_{\mathfrak{p}}^{\times} / \mathrm{Nr}_{\hat{K}_{\mathfrak{P}}/\hat{k}_{\mathfrak{p}}}(\widehat{K_{\mathfrak{P}}^{\times}}) \cong H^1(\widehat{k}_{\mathfrak{p}}, \mathrm{N}_{\mathfrak{p}}).$$

**Definition 5.1.** Let $S$ be a non-empty finite set of primes of $k$. The *first Tate–Shafarevich set* of $G$ over $k$ relative to $S$ is

$$Ш^1_S(k, G) := \ker \left[ H^1(k, G) \longrightarrow \prod_{\mathfrak{p} \notin S} H^1(\widehat{k}_{\mathfrak{p}}, G_{\mathfrak{p}}) \right].$$

**Proposition 5.2.** *Suppose* $[K : k]$ *is prime and* $\mathrm{Nr}(\underline{\mathrm{R}}(\widehat{\mathcal{O}}_{\mathfrak{p}})) = U_{\mathfrak{p}} \cap \mathrm{Nr}_{\hat{K}_{\mathfrak{P}}/\hat{k}_{\mathfrak{p}}}(\widehat{K_{\mathfrak{P}}^{\times}})$ *for all* $\mathfrak{p}$. *Let* $S_r$ *be the set of primes dividing* $\Delta_k$. *Then there is an exact sequence of abelian groups (compare with formula (5.3) in* [22]*):*

$$1 \longrightarrow \mathrm{Cl}_{\infty}(\underline{\mathrm{N}}) \longrightarrow H^1_{\text{ét}}(\mathcal{O}, \underline{\mathrm{N}}) \longrightarrow Ш^1_{S_r \cup \{\infty_k\}}(k, \mathrm{N}) \longrightarrow 1.$$

*Proof.* As $H^1_{\text{ét}}(\mathcal{O}_{\mathfrak{p}}, \underline{\mathrm{N}}_{\mathfrak{p}})$ embeds into $H^1(\widehat{k}_{\mathfrak{p}}, \mathrm{N}_{\mathfrak{p}})$ for any prime $\mathfrak{p}$ by (5.5), the group $\underline{\mathrm{N}}$ admits the exact sequence (5.4), consisting of abelian groups as $\underline{\mathrm{N}}$ is commutative. The pointed set $\mathrm{Cl}_{\infty}(\underline{\mathrm{N}})$ is in bijection with the first Nisnevich cohomology set $H^1_{\mathrm{Nis}}(\mathcal{O}, \underline{\mathrm{N}})$ (cf. [23, I. Thm. 2.8]), which is a subgroup of $H^1_{\text{ét}}(\mathcal{O},\underline{\mathrm{N}})$ because any Nisnevich cover is flat. Hence the first map is an embedding. Since $K/k$ has prime degree and so is necessarily abelian, at any prime $\mathfrak{p}$ the local Artin reciprocity law implies that

$$n_{\mathfrak{p}} = |\mathrm{Gal}(\widehat{K}_{\mathfrak{P}}/\widehat{k}_{\mathfrak{p}})| = [\widehat{k}_{\mathfrak{p}}^{\times} : \mathrm{Nr}_{\hat{K}_{\mathfrak{P}}/\hat{k}_{\mathfrak{p}}}(\widehat{K}_{\mathfrak{P}}^{\times})] = |H^1(\widehat{k}_{\mathfrak{p}},\mathrm{N}_{\mathfrak{p}})|.$$

Furthermore, since $[K:k]$ is a prime number, any ramified place $\mathfrak{p}$ is totally ramified, which implies that $[U_{\mathfrak{p}} : U_{\mathfrak{p}} \cap \mathrm{Nr}_{\hat{K}_{\mathfrak{P}}/\hat{k}_{\mathfrak{p}}}(U_{\mathfrak{P}})] = n_{\mathfrak{p}}$ [17, Thm. 5.5]. Together with (5.5) this means that $H^1_{\text{ét}}(\widehat{\mathcal{O}}_{\mathfrak{p}},\underline{\mathrm{N}}_{\mathfrak{p}})$ coincides with $H^1(\mathbb{Q}_{\mathfrak{p}},\mathrm{N}_{\mathfrak{p}})$ at ramified primes and vanishes elsewhere. Thus the set $B$ of (5.4) consists of classes $[\gamma] \in H^1(k,\mathrm{N})$ whose fibers vanish at unramified places. This means that $B = \text{Ш}^1_{S_r\cup\{\infty_k\}}(k,\mathrm{N})$, where $S_r$ is the (finite) set of ramified primes of $K/k$. □

**Remark 5.3.** The group $B = \text{Ш}^1_{S_r\cup\{\infty_k\}}(k,\mathrm{N})$ embeds in $H^1(k,\mathrm{N})$ by definition. But $H^1(k,\mathrm{N}) \cong k^\times/\mathrm{Nr}(K^\times)$, which means that $B$ has an exponent dividing $n = [K:k]$.

**Corollary 5.4.** *For any* $[q'] \in \mathfrak{cl}_0(\mathrm{disc}(q))$, $[q' \star q'] \in \mathrm{Cl}_\infty(q) := \mathrm{Cl}_\infty(\underline{\mathrm{SO}}_q)$.

*Proof.* The scheme $\underline{\mathrm{SO}}_q = \underline{\mathrm{N}}$ admits the exact sequence (5.4) (see the proof of Proposition 5.2). Together with (5.3) and Lemma 2.3 the principal genus satisfies

$$\mathrm{Cl}_\infty(\underline{\mathrm{SO}}_q = \underline{\mathrm{N}}) = \ker[H^1_{\text{ét}}(\mathcal{O},\underline{\mathrm{N}}) \longrightarrow H^1(k,\mathrm{N})].$$

The quotient $H^1_{\text{ét}}(\mathcal{O},\underline{\mathrm{N}})/\mathrm{Cl}_\infty(\underline{\mathrm{N}}) = \text{Ш}^1_{S_r\cup\{\infty_k\}}(k,N)$ has exponent 2 by Proposition 5.2 and Remark 5.3. This means that if $[q'] \in H^1_{\text{ét}}(\mathcal{O},\underline{\mathrm{N}} = \underline{\mathrm{SO}}_q)$, the latter pointed-set being bijective to $\mathfrak{cl}_0(\mathrm{disc}(q))$ by Lemma 2.5, then $[q' \star q']$ lies in $\mathrm{Cl}_\infty(q)$. □

## 6. Over elliptic curves

Let $\mathcal{O} = \mathbb{F}[x]$ and so $k = \mathbb{F}(x)$. Let $C = \{Y^2Z = X^3 + aXZ^2 + bZ^3\}$ be an elliptic curve defined over $\mathbb{F}$. Then $K = \mathbb{F}(C)$ is quadratic imaginary over $k$; $K = k(\sqrt{\alpha})$ where $\alpha = x^3 + ax + b \in \mathcal{O}$. As $\mathrm{char}(k)$ is odd $K/k$ is separable and as $\deg(\alpha) = 3$, $\infty_k = \langle 1/x \rangle$ ramifies in $K$ ([20, Thm. 1 (1)(a)]). Suppose $\infty_K = (0:1:0)$ belongs to $C(\mathbb{F})$. Then $\mathcal{O}_K = \mathbb{F}[C^{\mathrm{af}}]$ where $C^{\mathrm{af}}$ is the affine $\mathbb{F}$-curve $C - \{\infty_K\} = \{y^2 = \alpha\}$ and one has $\mathrm{Pic}(\mathcal{O}_K) \cong C(\mathbb{F})$ (e.g., [3, Ex. 4.8]). Let as above $\mathfrak{cl}_1'(\Delta_K)$ be the set of classes of primitive quadratic binary $\mathcal{O}$-forms, being definite, up to proper $\mathcal{O}$-isometries. By Theorem 3.1 one has: $\mathfrak{cl}_1'(\Delta_K) \cong C(\mathbb{F})$. Explicitly,

**Corollary 6.1.** *Let $C = \{Y^2Z = X^3 + aXZ^2 + bZ^3\}$ be an elliptic $\mathbb{F}$-curve such that $\infty_K := (0:1:0) \in C(\mathbb{F})$. Set: $\Delta_K = -(x^3 + ax + b)(\mathbb{F}^\times)^2$. Then there is an isomorphism of abelian groups $C(\mathbb{F}) \cong \mathfrak{cl}'_1(\Delta_K)$ given by:*

$$[(\mathcal{A}:\mathcal{B}:\mathcal{C} \neq 0)] \longmapsto \left[\left(x - \frac{\mathcal{A}}{\mathcal{C}}, -\frac{2\mathcal{B}}{\mathcal{C}}, \frac{\left(\frac{\mathcal{B}}{\mathcal{C}}\right)^2 - \alpha}{x - \frac{\mathcal{A}}{\mathcal{C}}}\right)\right],$$
$$[(0:1:0)] \longmapsto [(1, 0, -\alpha)].$$

*Proof.* Since $\infty_K$ is a closed point on $C$, $\mathbb{F}[C - \{\infty_K\}] = \mathcal{O}[\sqrt{\alpha}]$ where $\alpha = x^3 + ax + b$ is the ring of $\{\infty_K\}$-integers in $K = \mathbb{F}(C)$. The above correspondence is then given by:

$$\begin{aligned} &[(\mathcal{A}:\mathcal{B}:\mathcal{C} \neq 0)] \in C(\mathbb{F}) - \{\infty_K\} \\ &\qquad \longmapsto \left[\left(\frac{\mathcal{A}}{\mathcal{C}}, \frac{\mathcal{B}}{\mathcal{C}}\right)\right] \in C^{\mathrm{af}}(\mathbb{F}) \\ &\qquad \longmapsto \left[\left\langle x - \frac{\mathcal{A}}{\mathcal{C}}, y - \frac{\mathcal{B}}{\mathcal{C}}\right\rangle\right] \in \mathrm{Pic}(\mathcal{O}_K) \\ &\qquad \longmapsto \left[\left(x - \frac{\mathcal{A}}{\mathcal{C}}, -2\frac{\mathcal{B}}{\mathcal{C}}, \frac{\left(\frac{\mathcal{B}}{\mathcal{C}}\right)^2 - \alpha}{x - \frac{\mathcal{A}}{\mathcal{C}}}\right)\right] \in \mathfrak{cl}'_1(\Delta_K) \end{aligned}$$

and $(0:1:0) \mapsto (1, 0, -\alpha)$. □

**Example 6.2.** Let $C = \{Y^2Z = X^3 + XZ^2 + Z^3\}$ defined over $\mathbb{F}_3$. Removing the rational point $\infty_K = (0:1:0)$, we get the affine curve $C^{\mathrm{af}} = \{y^2 = x^3 + x + 1\}$ with $\mathcal{O}_K = \mathbb{F}_3[x,y]/\langle y^2 - x^3 - x - 1\rangle$.
Then we have:

| i | $C(\mathbb{F}_3)$ | affine support | order | $L_i$ | $q_i$ |
|---|---|---|---|---|---|
| 1 | $(1:0:1)$ | $(1,0)$ | 2 | $(x-1, y)$ | $(x-1, 0, 2x^2+2x+1)$ |
| 2 | $(0:1:2)$ | $(0,2)$ | 4 | $(x, y-2)$ | $(x, 2, 2x^2+2)$ |
| 3 | $(0:1:1)$ | $(0,1)$ | 4 | $(x, y-1)$ | $(x, 1, 2x^2+2)$ |
| 4 | $(0:1:0)$ | O | 1 | $\mathcal{O}_K$ | $(1, 0, 2x^3+2x+2)$ |

Here $q_2$ and $q_3$ are opposite $[q_2]\star[q_3] = [q_4]$. Indeed: $\langle x, y-2\rangle \otimes \langle x, y-1\rangle = \langle x\rangle$, thus

$$\mathfrak{cl}'_1(\Delta_K) \cong \mathrm{Pic}(\mathcal{O}_K) \cong \mathbb{Z}/4,$$

while $\mathfrak{cl}'(\Delta_K) = \{[q_1], [q_2], [q_4]\}$ has no group structure.

According to Proposition 5.2 there are 2 genera and by Proposition 5.4 the class $[q_2^2]$ belongs to the principal genus though not being the trivial one. Indeed: $[q_2^2] = [q_1]$ by the group law, and as $y^2 = (x-1)(x^2+x-1)$, $q_1$ is isomorphic to $q_4$ by $\left(1/\sqrt{x-1}, \sqrt{x-1}\right)$ locally at $\mathfrak{p} \neq \langle x-1\rangle$, and by $\mathrm{diag}\left(\sqrt{x^2+x-1}/y, y/\sqrt{x^2+x-1}\right)$ at $\mathfrak{p} = \langle x-1\rangle$.

**Example 6.3.** Let $C = \{Y^2Z = X^3+XZ^2\}$ defined over $\mathbb{F}_5$. Removing the rational point $\infty_K = (0:1:0)$ we get the affine curve $C^{\mathrm{af}} = \{y^2 = x^3+x\}$ with $\mathcal{O}_K = \mathbb{F}_5[x,y]/\langle y^2 - x^3 - x\rangle$. Then:

| i | $C(\mathbb{F}_5)$ | affine support | order | $L_i$ | $q_i$ |
|---|---|---|---|---|---|
| 1 | $(0:0:1)$ | $(0,0)$ | 2 | $(x,y)$ | $(x,0,4x^2+4)$ |
| 2 | $(1:0:2)$ | $(3,0)$ | 2 | $(x-3,y)$ | $(x-3,0,x^2+3x)$ |
| 3 | $(1:0:3)$ | $(2,0)$ | 2 | $(x-2,y)$ | $(x-2,0,x^2+2x)$ |
| 4 | $(0:1:0)$ | O | 1 | $\mathcal{O}_K$ | $(1,0,4x^3+4x)$ |

Here we observe no forms of order greater than 2 and so

$$\mathfrak{cl}'(\Delta_K) = \mathfrak{cl}'_1(\Delta_K) \cong \mathrm{Pic}(\mathcal{O}_K) \cong \mathbb{Z}_2^2.$$

**Acknowledgements.** I thank U. First, P. Gille, B. Kunyavskiĭ, S. Scully and S. Vladuts for valuable discussions concerning the topics of the present article. I also thank the anonymous referee for their constructive remarks.

## References

[1] A. Auel, R. Parimala & V. Suresh, "Quadric surface bundles over surfaces", *Doc. Math.* (2015), p. 31-70, Extra Vol., Alexander S. Merkurjev's Sixtieth Birthday.

[2] O. Biesel, "A norm functor for quadratic algebras", *Beitr. Algebra Geom.* **65** (2024), no. 1, p. 59-83.

[3] R. A. Bitan, "The Hasse principle for bilinear symmetric forms over a ring of integers of a global function field", *J. Number Theory* **168** (2016), p. 346-359.

[4] R. A. Bitan & M. M. Schein, "On the flat cohomology of binary norm forms", *J. Théor. Nombres Bordeaux* **31** (2019), no. 3, p. 527-553.

[5] A. Borel & G. Prasad, "Finiteness theorems for discrete subgroups of bounded covolume in semi-simple groups", *Publ. Math., Inst. Hautes Étud. Sci.* **69** (1989), p. 119-171.

[6] S. Bosch, W. Lütkebohmert & M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge, vol. 21, Springer, 1990.

[7] B. Calmès & J. Fasel, "Groupes Classiques", in *Autour des schémas en groupes. École d'Été "Schémas en groupes ". Volume II*, Panoramas et Synthèses, vol. 46, Société Mathématique de France, 2015, p. 1-133.

[8] B. Conrad, "Math 252. Properties of orthogonal groups", available at `http://math.stanford.edu/~conrad/252Page/handouts/O(q).pdf`.

[9] ———, "Non-split Reductive Groups Over Z", available at `http://math.stanford.edu/~conrad/papers/redgpZsmf.pdf`.

[10] B. Conrad, O. Gabber & G. Prasad, *Pseudo-reductive groups*, 2nd ed., New Mathematical Monographs, vol. 26, Cambridge University Press, 2015, xxiv+665 pages.

[11] A. Fröhlich & M. J. Taylor, *Algebraic Number Theory*, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press, 1990, xiv+355 pages.

[12] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801.

[13] P. Gille, "Sur la classification des schémas en groupes semi-simples", in *Autour des schémas en groupes. École d'Été "Schémas en groupes". Volume III*, Panoramas et Synthèses, vol. 47, Société Mathématique de France, 2015, p. 39-110.

[14] P. Gille & A. Pianzola, "Isotriviality and étale cohomology of Laurent polynomial rings", *J. Pure Appl. Algebra* **212** (2008), no. 4, p. 780-800.

[15] J. Giraud, *Cohomologie non abélienne*, Grundlehren der Mathematischen Wissenschaften, vol. 179, Springer, 1971, ix+467 pages.

[16] A. Grothendieck, "Éléments de géométrie algébrique. IV: Étude locale des schémas et des morphismes de schémas (Seconde partie)", *Publl. Math., Inst. Hautes Étud. Sci.* **24** (1965), p. 5-231, rédigés avec la collaboration de J. Dieudonné.
[17] M. Hazewinkel, "Local class field theory is easy", *Adv. Math.* **18** (1975), p. 148-181.
[18] M. Kneser, "Composition of binary quadratic forms", *J. Number Theory* **15** (1982), p. 406-413.
[19] M.-A. Knus, *Quadratic and hermitian forms over rings*, Grundlehren der Mathematischen Wissenschaften, vol. 294, Springer, 1991, xi+524 pages.
[20] D. Le Brigand, "Real quadratic extensions of the rational function field in characteristic two", in *Arithmetic, geometry and coding theory (AGCT 2003)*, Séminaires et Congrès, vol. 11, Société Mathématique de France, 2005, p. 143-169.
[21] Y. Lee & A. M. Pacelli, "Class Groups of Imaginary Function Fields: The Inert Case", *Proc. Am. Math. Soc.* **133** (2005), no. 10, p. 2883-2889.
[22] M. Morishita, "On *S*-class number relations of algebraic tori in Galois extensions of global fields", *Nagoya Math. J.* **124** (1991), p. 133-144.
[23] Y. Nisnevich, "Étale Cohomology and Arithmetic of Semisimple Groups", PhD Thesis, arvard University, 1982.
[24] A. Skorobogatov, *Torsors and Rational Points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, 2001, viii+187 pages.
[25] M. M. Wood, "Gauss composition over an arbitrary base", *Adv. Math.* **226** (2011), no. 2, p. 1756-1771.

Rony A. Bitan
Afeka, Tel-Aviv Academic College of Engineering
Tel-Aviv, Israel
*E-mail*: ronyb@afeka.ac.il