Journal
de Théorie des Nombres
de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Rony A. BITAN et Michael M. SCHEIN

On the flat cohomology of binary norm forms

Tome 31, n° 3 (2019), p. 527-553.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2019__31_3_527_0>

Journal de Théorie des Nombres
de Bordeaux **31** (2019), 527–553

On the flat cohomology of binary norm forms

par Rony A. BITAN et Michael M. SCHEIN

Résumé. Soit $\mathcal{O}$ un ordre d'indice m dans l'ordre maximal d'un corps de nombres quadratique $k = \mathbb{Q}(\sqrt{d})$. Soit $\underline{\mathrm{O}}_{d,m}$ le $\mathbb{Z}$-groupe orthogonal de la forme norme associée $q_{d,m}$. Nous décrivons la structure de l'ensemble pointé $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_{d,m})$, qui classifie les formes quadratiques isomorphes à $q_{d,m}$ pour la topologie plate. Gauss a classifié les formes quadratiques de discriminant fondamental et montré que la composée d'une $\mathbb{Z}$-forme de discriminant Δ_k avec elle-même est dans le genre principal. En utilisant le langage cohomologique, nous étendons ces résultats aux formes de certains discriminants non fondamentaux.

Abstract. Let $\mathcal{O}$ be an order of index m in the maximal order of a quadratic number field $k = \mathbb{Q}(\sqrt{d})$. Let $\underline{\mathrm{O}}_{d,m}$ be the orthogonal $\mathbb{Z}$-group of the associated norm form $q_{d,m}$. We describe the structure of the pointed set $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_{d,m})$, which classifies quadratic forms isomorphic (properly or improperly) to $q_{d,m}$ in the flat topology. Gauss classified quadratic forms of fundamental discriminant and showed that the composition of any binary $\mathbb{Z}$-form of discriminant Δ_k with itself belongs to the principal genus. Using cohomological language, we extend these results to forms of certain non-fundamental discriminants.

1. Introduction

Let q be an integral binary quadratic form, namely a map $q : \mathbb{Z}^2 \to \mathbb{Z}$ represented by a symmetric matrix B_q satisfying $q(x,y) = (x,y)B_q(x,y)^t = ax^2+bxy+cy^2$, where $a,b,c \in \mathbb{Z}$. For brevity we write $q = (a,b,c)$. Schemes defined over $\operatorname{Spec}\mathbb{Z}$ are underlined, whereas the underline is omitted for their generic fibers. Any change of variables by $A \in \underline{\mathrm{GL}}_2(\mathbb{Z})$ gives rise to an isomorphic form $q' = q \circ A$ represented by the congruent matrix $B_{q'} = AB_qA^t$. In particular, if $q = q \circ A$, then A is called an *isometry* of q. It is called *proper* if $A \in \underline{\mathrm{SL}}_2(\mathbb{Z})$. The *discriminant* of q is the integer $\Delta(q) = b^2 - 4ac = -4\det(B_q)$; it is independent of the choice of the basis of $\mathbb{Z}^2$ since $\det(A) = \pm 1$ for any $A \in \underline{\mathrm{GL}}_2(\mathbb{Z})$. Given an integer $n \in \mathbb{Z}$,

Manuscrit reçu le 3 novembre 2016, révisé le 24 juin 2019, accepté le 28 septembre 2019.
2010 *Mathematics Subject Classification.* 11E41, 11E72, 11E12.
Mots-clefs. flat cohomology, quadratic forms, quadratic orders.
This work was supported by grant 1246/2014 from the Germany-Israel Foundation. The first author was also supported by a Chateaubriand Fellowship of the Embassy of France in Israel, 2016.

a natural and very classical problem is to describe the set of equivalence classes

$$\mathfrak{cl}^+(n) := \{q : \Delta(q) = n\}/\underline{\mathrm{SL}}_2(\mathbb{Z}). \tag{1.1}$$

Consider the quadratic number field $k = \mathbb{Q}(\sqrt{d})$, where $d \notin \{0,1\}$ is a square-free integer. Denote its discriminant by Δ_k and the norm map by $\mathrm{Nr} : k^\times \to \mathbb{Q}^\times$. Fixing an integral basis $\{1,\omega\}$ of the ring of integers $\mathcal{O}_k$, associate to k the *norm $\mathbb{Z}$-form* $q_d(x,y) := \mathrm{Nr}(x+y\omega)$. Then $\Delta(q_d) = \Delta_k$ is a fundamental discriminant. As $\mathcal{O}_k$ is a Dedekind domain, its narrow ideal class group I_k/P_k^+ coincides with its (narrow) Picard group $\mathrm{Pic}^+(\mathcal{O}_k)$. If $d < 0$, write $\mathfrak{cl}^+(\Delta(q_d))'$ for the restriction of $\mathfrak{cl}^+(\Delta(q_d))$ to only *positive* definite forms, namely those for which $a, c > 0$. If $d > 0$, define $\mathfrak{cl}^+(\Delta(q_d))' = \mathfrak{cl}^+(\Delta(q_d))$. Gauss, in his *Disquisitiones Arithmeticae* [18], proved that there is a bijection $\mathfrak{cl}^+(\Delta(q_d))' \cong \mathrm{Pic}^+(\mathcal{O}_k)$ of pointed sets given explicitly by

$$[(a,b,c)] \mapsto \left[\left\langle a, \frac{b - F\sqrt{d}}{2}\right\rangle\right], \text{ where } F = \begin{cases} 2 & d \equiv 2,3 \pmod 4 \\ 1 & d \equiv 1 \pmod 4). \end{cases} \tag{1.2}$$

The main aim of this paper is to describe the sets

$$\mathfrak{cl}(n) := \{q : \Delta(q) = n\}/\underline{\mathrm{GL}}_2(\mathbb{Z}),$$

in terms of geometric invariants of orders in quadratic number fields. This extends the question considered by Gauss in three ways: we consider all quadratic forms, and not only the positive definite ones; we consider all isometries, and not only proper ones; we consider discriminants n that are not fundamental.

A modern perspective on these classical ideas, used in the 1980's by Ono [30] for number fields and extended by Morishita [28] to general global fields, identifies $\mathfrak{cl}^+(\Delta(q_d))$ with $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_d^+)$, where $\underline{\mathrm{O}}_d^+$ is the *special orthogonal group* of q_d. This flat cohomology, which *a priori* is a pointed set but is an abelian group since $\underline{\mathrm{O}}_d^+$ is commutative, classifies all integral binary forms that are isomorphic to q_d in the flat (i.e. fppf) topology modulo proper isometries. Analogously, the first Nisnevich cohomology set classifies forms in the principal genus of q_d. Recall that two integral binary forms are said to be isomorphic in the flat topology if for every prime p they are isomorphic over some finite flat extension of $\mathbb{Z}_p$. We extend this approach to arbitrary quadratic orders $\mathcal{O} \subseteq \mathcal{O}_k$ and obtain a classification, in terms of the Picard group $\mathrm{Pic}\,\mathcal{O}$, of isomorphism classes (not just proper isomorphism classes) of integral forms that are isomorphic in the flat topology to the norm form associated with $\mathcal{O}$.

1.1. Organization of the paper. We briefly describe the structure of the paper and point out its main results. Sections 2 and 3 recall the basic notions we will use, most notably a $\mathbb{Z}$-model $\underline{N}$ of a norm $\mathbb{Q}$-torus associated to an order. Section 4 defines the orthogonal and special orthogonal groups $\underline{\mathrm{O}}_q$ and $\underline{\mathrm{O}}_q^+$ associated to a quadratic form q. If q is degenerate over $\mathbb{Z}$, the orthogonal group $\underline{\mathrm{O}}_q$ need not be flat over $\mathbb{Z}$. Thus we work instead with $\widetilde{\underline{\mathrm{O}}}_q$, the schematic closure in $\underline{\mathrm{O}}_q$ of the generic fiber. We obtain an identification (Lemma 4.5) of the special orthogonal group of a norm form of an order $\mathcal{O}$ (with respect to a fixed $\mathbb{Z}$-basis of $\mathcal{O}$) with $\underline{N}$. Finally, we let $\mathcal{O}_{d,m}$ denote the unique order of index m in the maximal order of $k = \mathbb{Q}(\sqrt{d})$ and fix $\mathbb{Z}$-bases of the orders $\mathcal{O}_{d,m}$. There is a natural bifurcation into two cases: either the norm form $q_{d,m} := q_{\mathcal{O}_{d,m}}$ is diagonal for a suitable choice of basis (Case (II)) or not (Case (I)). Case (I) holds when $d \equiv 1 \bmod 4$ and m is odd, whereas Case (II) covers all other instances.

Section 5, the heart of the paper, starts by determining (Proposition 5.1) the structure of the quotient $\widetilde{\underline{\mathrm{O}}}_{q_{d,m}}/\underline{\mathrm{O}}^+_{q_{d,m}}$, which is always a finite flat group scheme of order two. The proof is short and relies on the theory of finite flat group schemes. For comparison, in an appendix to the paper we provide a more classical proof that writes down defining polynomials of $\widetilde{\underline{\mathrm{O}}}_{q_{d,m}}$ and $\underline{\mathrm{O}}^+_{q_{d,m}}$. We then turn to studying the pointed set $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_{q_{d,m}}) = H^1_{\mathrm{fl}}(\mathbb{Z}, \widetilde{\underline{\mathrm{O}}}_{q_{d,m}})$. In Case (I) it is canonically identified with $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}^+_{q_{d,m}})$, whereas in Case (II) it also contains classes of forms of discriminant $-\Delta(q_{d,m})$. This is shown in Proposition 5.5 and Lemma 5.6, respectively. From this we can study the sets $\mathfrak{cl}(n)$ for many discriminants n. The following is the content of Propositions 5.17 and 5.18:

Proposition 1.1. *Let $D \in \mathbb{Z}$ be an integer such that $D \equiv 0 \bmod 4$ or $D \equiv 1 \bmod 4$. Suppose further that D is not a perfect square and not of the form $D = -3 \cdot 4^m$ for some $m \geq \mathbb{N}_0$. Then*

$$\mathfrak{cl}(D) = \begin{cases} \mathfrak{cl}^+(D) = H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q^+) & : D \equiv 1 \bmod 4 \\ \mathfrak{cl}^+(D)/\sim\, = H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q^+)/\sim & : D \equiv 0 \bmod 4, \end{cases}$$

where the explicit quadratic form q is the norm form of a quadratic order with respect to one of our explicit bases, and the equivalence relation $\sim$ is given by $[ax^2 + bxy + cy^2] \sim [ax^2 - bxy + cy^2]$.

The relation stated here between quadratic forms and flat cohomology fails for discriminants of the form $-3 \cdot 4^m$; see Remark 5.16. Along the way we study a number of explicit examples. For any square-free $d \neq 0, 1$ we show in Theorem 5.19 that

$$\mathfrak{cl}^+(\Delta_{\mathbb{Q}(\sqrt{d})}) \cong \{\pm 1\}^{\mu(d)} \times \mathrm{Pic}^+(\mathcal{O}_k), \text{ where } \mu(d) = \begin{cases} 1 & d < 0 \\ 0 & d > 0. \end{cases}$$

This is a straightforward extension of Gauss' proper classification to all forms, not just the positive definite ones. More generally, our analysis of Case (II) leads to an extension of the classification to many cases in which

$4D$ is not a fundamental discriminant. Theorem 5.21, another classical theorem that we prove with new methods, states that if D is any integer that is not a perfect square and not of the form $D = -3 \cdot 4^m$, then

$$\mathfrak{cl}^+(4D) \cong \{\pm 1\}^{\tilde{\varepsilon}(D)} \times \mathrm{Pic}(\mathbb{Z}[\sqrt{D}]),$$

where

$$\tilde{\varepsilon}(D) = \begin{cases} 0 & D > 0 \text{ and } \mathrm{Nr}(\mathbb{Z}[\sqrt{D}]^\times) = \{\pm 1\} \\ 1 & \text{otherwise.} \end{cases}$$

Note that $\mathbb{Z}[\sqrt{D}]$ is not in general a Dedekind domain. Theorem 5.21 remains true for discriminants of the form $-3 \cdot 4^m$, but our proof does not work in that case. Recall that $k = \mathbb{Q}(\sqrt{d})$. In Proposition 5.22, we express the cardinality $|H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_{q_{\mathcal{O}_k}})|$ in terms of the narrow class numbers of $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-d})$. Finally, we show in Corollary 5.24 under some hypotheses on the form $q_{d,m}$, that any $\underline{\mathrm{O}}^+_{q_{d,m}}$-torsor, tensored with itself, belongs to the principal genus of $q_{d,m}$. This may be viewed as an extension, in the language of cohomology, of another classical theorem of Gauss.

Acknowledgements. The authors would like to thank J. Bernstein, B. Conrad, P. Gille, B. Kunyavskiĭ, and B. Moroz for valuable discussions concerning the topics of the present article. They are grateful to the anonymous referee for a very careful reading of the paper and helpful comments that have clarified the exposition.

2. Preliminaries

Let $k/\mathbb{Q}$ be a finite Galois extension with Galois group $\Gamma = \mathrm{Gal}(k/\mathbb{Q})$ and degree $n = [k : \mathbb{Q}]$. Let $\underline{\mathbb{G}}_m$ and $\underline{\mathrm{GL}}_n$ denote the multiplicative and general linear $\mathbb{Z}$-groups, respectively. Recall that an *order* in $\mathcal{O}_k$ is a subring that has the maximal rank n as a $\mathbb{Z}$-lattice. Fix a $\mathbb{Z}$-basis $\Omega = \{\omega_1, \dots, \omega_n\}$ for an *order* $\mathcal{O}_\Omega \subseteq \mathcal{O}_k$. The Weil restriction of scalars $\underline{R}_\Omega = \mathrm{Res}_{\mathcal{O}_\Omega/\mathbb{Z}}(\underline{\mathbb{G}}_m)$ is an n-dimensional $\mathbb{Z}$-group that admits an isomorphism $\rho : \underline{R}_\Omega(\mathbb{Z}) \simeq \mathcal{O}_\Omega^\times$ [5, §7.6]. The natural action of $\rho(\underline{R}_\Omega(\mathbb{Z}))$ on $\mathcal{O}_\Omega$ yields a canonical embedding of $\underline{R}_\Omega$ in $\mathrm{Aut}(\mathcal{O}_\Omega) = \underline{\mathrm{GL}}(\mathcal{O}_\Omega)$, depending only on the order $\mathcal{O}_\Omega$ and not on the $\mathbb{Z}$-basis Ω. The choice of Ω provides an embedding $\iota : \underline{R}_\Omega \hookrightarrow \underline{\mathrm{GL}}_n$. The composition of ι with the determinant gives a map $\underline{R}_\Omega \to \underline{\mathbb{G}}_m$ that we abusively denote[1] det. Then $\mathrm{Nr}(\alpha) = \det(\iota(\rho^{-1}(\alpha)))$ for all $\alpha \in \mathcal{O}_\Omega^\times$, where $\mathrm{Nr} : k^\times \to \mathbb{Q}^\times$ is the usual norm map; see Exercise 9 (c) of [6, §II.5].

[1] Note that the map det depends only on the order $\mathcal{O}_\Omega$ and not on the choice of basis Ω. Indeed, the constructions of this and the following two sections, up to the explicit matrix realizations of (4.2) and (4.4), are independent of the choice of Ω.

We get a short exact sequence of commutative $\mathbb{Z}$-group schemes where the quotient map is faithfully flat in the sense of [22, 0.6.7.8]:

$$1 \to \underline{N}_\Omega \to \underline{R}_\Omega \xrightarrow{\det} \underline{\mathbb{G}}_m \to 1. \tag{2.1}$$

The generic fibers of the elements of this sequence are the norm torus $N = \mathrm{Res}^{(1)}_{k/\mathbb{Q}}(\mathbb{G}_m)$, the Weil torus $R = \mathrm{Res}_{k/\mathbb{Q}}(\mathbb{G}_m)$, and the multiplicative $\mathbb{Q}$-group $\mathbb{G}_m$, respectively. Their fibers at any prime p are denoted by $(\underline{N}_\Omega)_p$, $(\underline{R}_\Omega)_p$ and $(\underline{\mathbb{G}}_m)_p$, respectively, while their reductions are overlined. We omit the subscript Ω when $\mathcal{O}_\Omega$ is the maximal order $\mathcal{O}_k$.

While $\underline{\mathbb{G}}_m$ and $\underline{R}_\Omega$ are smooth over $\operatorname{Spec}\mathbb{Z}$, the kernel $\underline{N}_\Omega$ need not be smooth, in that it may have a non-reduced reduction at some prime. However, $\underline{N}_\Omega$ is flat over $\operatorname{Spec}\mathbb{Z}$. Indeed, $\underline{R}_\Omega$ and $\underline{\mathbb{G}}_m$ are smooth and hence regular and Cohen-Macaulay. By the Miracle Flatness Theorem [27, Theorem 23.1], it suffices to check that all geometric fibers of $\underline{N}_\Omega = \ker[\underline{R}_\Omega \xrightarrow{\det} \underline{\mathbb{G}}_m]$ have dimension $[k : \mathbb{Q}] - 1$. The map $(\overline{R}_\Omega)_p \xrightarrow{\det_p} (\overline{\mathbb{G}}_m)_p$ induced by det in the reduction of (2.1) is surjective for all p. Thus $\underline{N}_\Omega$ is flat over $\operatorname{Spec}\mathbb{Z}$, and instead of using étale cohomology we restrict ourselves to flat cohomology.

Applying flat cohomology to (2.1) gives rise to a long exact sequence of pointed sets; see [21, III, Prop. 3.3.1 (i)]:

$$\begin{aligned} 1 \to \underline{N}_\Omega(\mathbb{Z}) \to \underline{R}_\Omega(\mathbb{Z}) \cong \mathcal{O}_\Omega^\times \xrightarrow{\mathrm{Nr}} \{\pm 1\} \to H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_\Omega) \\ \to H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{R}_\Omega) \to H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathbb{G}}_m) = \operatorname{Pic}\mathbb{Z} = 0. \end{aligned} \tag{2.2}$$

Now $\mathcal{O}_\Omega$ is finite and torsion-free over $\mathbb{Z}$, hence flat. By Shapiro's Lemma [16, XXIV, Prop. 8.2], we have $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{R}_\Omega) \cong H^1_{\mathrm{fl}}(\mathcal{O}_\Omega, \underline{\mathbb{G}}_{m,\mathcal{O}_\Omega}) = \operatorname{Pic}\mathcal{O}_\Omega$. Thus (2.2) can be rewritten as

$$1 \to \{\pm 1\}/\operatorname{Nr}(\mathcal{O}_\Omega^\times) \to H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_\Omega) \to \operatorname{Pic}(\mathcal{O}_\Omega) \to 1. \tag{2.3}$$

The maximal order $\mathcal{O}_k$ is a Dedekind domain whose Picard group coincides with the ideal class group of k. The set $\{\pm 1\}/\operatorname{Nr}(\mathcal{O}_k^\times)$ is equal to the zero-Tate cohomology set $H^0_T(\Gamma, \mathcal{O}_k^\times)$ [30, Ex. 1]. Thus, in the case $\mathcal{O}_\Omega = \mathcal{O}_k$, we deduce an isomorphism of finite groups

$$H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N})/H^0_T(\Gamma, \mathcal{O}_k^\times) \cong \operatorname{Pic}\mathcal{O}_k. \tag{2.4}$$

If n is odd, then $\operatorname{Nr}(-1) = (-1)^n = -1$. Therefore $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}) \cong \operatorname{Pic}\mathcal{O}_k$ and it follows that

$$h_k = |H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N})|. \tag{2.5}$$

In the quadratic case $n = 2$, we have $k = \mathbb{Q}(\sqrt{d})$ for some square-free integer $d \notin \{0, 1\}$. If $\mathcal{O}_\Omega$ is the maximal order $\mathcal{O}_k$, we set h_d and $\underline{N}_d$ to be the class number h_k and the $\mathbb{Z}$-group $\underline{N}$, respectively. Then (2.3) implies that

$$|H^1_{\text{fl}}(\mathbb{Z},\underline{N}_d)| = h_d \cdot 2^{\varepsilon(d)}, \tag{2.6}$$

where [30, §5, Ex. 2]:

$$\varepsilon(d) = \begin{cases} 0 & d>0 \text{ and } \mathrm{Nr}(\mathcal{O}_k^\times) = \{\pm 1\} \\ 1 & \text{otherwise.} \end{cases} \tag{2.7}$$

Let $\mathrm{Pic}^+(\mathcal{O}_k)$ be the narrow class group of k and let h_d^+ denote its cardinality. Then $h_d^+ = h_d$ unless $d>0$ and $\mathrm{Nr}(\mathcal{O}_k^\times) = \{1\}$, in which case $h_d^+ = 2h_d$. Now (2.6) implies

$$|H^1_{\text{fl}}(\mathbb{Z},\underline{N}_d)| = h_d^+ \cdot 2^{\mu(d)}, \quad \mu(d) := \begin{cases} 1 & d<0 \\ 0 & d>0. \end{cases} \tag{2.8}$$

Hence computing the narrow class number h_d^+ is equivalent to determining $|H^1_{\text{fl}}(\mathbb{Z},\underline{N}_d)|$.

3. The class set of the norm torus

Let $\underline{G}$ be an affine flat group scheme defined over $\mathrm{Spec}\,\mathbb{Z}$ with generic fiber G. We denote by $\underline{G}_p$ the $\mathbb{Z}_p$-scheme obtained from $\underline{G}$ by the base change $\mathrm{Spec}\,\mathbb{Z}_p \to \mathrm{Spec}\,\mathbb{Z}$. For a global field F, recall that the adelic group $\underline{G}(\mathbb{A}_F)$ is the restricted product of the groups $G(F_v)$, where F_v is the completion of F at a place v. We write $\underline{G}(\mathbb{A})$ for $\underline{G}(\mathbb{A}_\mathbb{Q})$. As in [4, §1.2], consider its subgroup $\underline{G}(\mathbb{A}_\infty) = G(\mathbb{R}) \times \prod_p \underline{G}(\mathbb{Z}_p)$.

Definition 3.1. The *class set* of $\underline{G}$ is the set of double cosets $\mathrm{Cl}_\infty(\underline{G}) := \underline{G}(\mathbb{A}_\infty)\backslash\underline{G}(\mathbb{A})/G(\mathbb{Q})$. This set is finite ([4, Thm. 5.1]) and its cardinality, denoted $h(\underline{G})$, is called the *class number* of $\underline{G}$.

Definition 3.2. Let S be a finite set of places in $\mathbb{Q}$. The *first Tate–Shafarevich set* of G over $\mathbb{Q}$ relative to S is

$$Ш^1_S(\mathbb{Q},G) := \ker\left[H^1(\mathbb{Q},G) \to \prod_{v\notin S} H^1(\mathbb{Q}_v,G_v)\right].$$

When $S=\varnothing$, we simply write $Ш^1(\mathbb{Q},G)$.

As $\underline{G}$ is affine, flat and of finite type, Y. Nisnevich has shown [29, Thm. I.3.5] that it admits an exact sequence of pointed sets

$$1 \to \mathrm{Cl}_\infty(\underline{G}) \to H^1_{\text{fl}}(\mathbb{Z},\underline{G}) \to H^1(\mathbb{Q},G) \times \prod_p H^1_{\text{fl}}(\mathbb{Z}_p,\underline{G}_p) \tag{3.1}$$

whose left exactness reflects the fact that $\mathrm{Cl}_\infty(\underline{G})$ is the set of $\mathbb{Z}$-forms of $\underline{G}$ that are isomorphic to $\underline{G}$ over $\mathbb{Q}$ and over $\mathbb{Z}_p$ for all p. If $H^1_{\text{fl}}(\mathbb{Z}_p,\underline{G}_p)$ injects into $H^1(\mathbb{Q}_p, G_p)$ for all p, then, as in [29, Cor. I.3.6], the sequence (3.1) simplifies to

$$1 \to \mathrm{Cl}_\infty(\underline{G}) \to H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{G}) \to H^1(\mathbb{Q}, G). \tag{3.2}$$

More precisely, there is an exact sequence of pointed sets (cf. [20, Cor. A.8])

$$1 \to \mathrm{Cl}_\infty(\underline{G}) \to H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{G}) \to B \to 1 \tag{3.3}$$

in which

$$B = \Big\{ [\gamma] \in H^1(\mathbb{Q}, G) : \forall\, p, [\gamma \otimes \mathbb{Z}_p] \in \mathrm{Im}\,\Big(H^1_{\mathrm{fl}}(\mathbb{Z}_p, \underline{G}_p) \to H^1(\mathbb{Q}_p, G_p) \Big) \Big\}.$$

Let $k/\mathbb{Q}$ be a finite Galois extension as in the previous section. Let p be a rational prime, and let P be a prime of k dividing p. Write $\mathbb{Q}_p$ and k_P for the localizations of $\mathbb{Q}$ at p and of k at P, respectively, noting that k_P is independent of the choice of P, up to isomorphism. Observe that $k \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong k_P^r$, where r is the number of primes of k dividing p. The norm map $\mathrm{Nr} : k \to \mathbb{Q}$ induces a map $\mathrm{Nr} : k \otimes_{\mathbb{Q}} \mathbb{Q}_p \to \mathbb{Q}_p$; under the isomorphism above this corresponds to the product of the norm maps $\mathrm{N}_{k_P/\mathbb{Q}_p}$ on the components. Similarly, $\mathcal{O}_k \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \mathcal{O}_{k_P}^r$. Write U_P for $\mathcal{O}_{k_P}^\times$.

Fix a $\mathbb{Z}$-basis Ω of an order $\mathcal{O}_\Omega$ as in the previous section, and assume that $\mathrm{Nr}((\underline{R}_\Omega)_p(\mathbb{Z}_p)) = \mathbb{Z}_p^\times \cap \mathrm{N}_{k_P/\mathbb{Q}_p}(k_P^\times)$ for all p. Note that the assumption always holds if $\mathcal{O}_\Omega$ is the maximal order of k, since then $(\underline{R}_\Omega)_p(\mathbb{Z}_p) = U_P^r$. See Example 5.25 for another case where it holds. Applying flat cohomology to the short exact sequence of flat $\mathbb{Z}_p$-groups

$$1 \to (\underline{N}_\Omega)_p \to (\underline{R}_\Omega)_p \to (\underline{\mathbb{G}}_m)_p \to 1$$

yields the exact and functorial sequence

$$1 \to (\underline{N}_\Omega)_p(\mathbb{Z}_p) \to (\underline{R}_\Omega)_p(\mathbb{Z}_p) \xrightarrow{\mathrm{Nr}} \mathbb{Z}_p^\times \to H^1_{\mathrm{fl}}(\mathbb{Z}_p, (\underline{N}_\Omega)_p) \to 1,$$

since $H^1_{\mathrm{fl}}(\mathbb{Z}_p, (\underline{R}_\Omega)_p)$ is the Picard group of a product of local rings and thus vanishes. We deduce an isomorphism $H^1_{\mathrm{fl}}(\mathbb{Z}_p, (\underline{N}_\Omega)_p) \cong \mathbb{Z}_p^\times / \mathrm{Nr}((\underline{R}_\Omega)_p(\mathbb{Z}_p))$. Applying Galois cohomology to the short exact sequence of $\mathbb{Q}_p$-groups

$$1 \to N_p \to R_p \to (\mathbb{G}_m)_p \to 1$$

gives rise to the exact sequence of abelian groups

$$1 \to N_p(\mathbb{Q}_p) \to R_p(\mathbb{Q}_p) \cong (k_P^\times)^r \xrightarrow{\mathrm{Nr}} \mathbb{Q}_p^\times \to H^1(\mathbb{Q}_p, N_p) \to 1,$$

where the rightmost term vanishes by Hilbert's Theorem 90. Hence we may again deduce a functorial isomorphism $H^1(\mathbb{Q}_p, N_p) \cong \mathbb{Q}_p^\times / \mathrm{N}_{k_P/\mathbb{Q}_p}(k_P^\times)$. Note that U_P is compact and thus $\mathrm{N}_{k_P/\mathbb{Q}_p}(U_P)$ is closed in $\mathbb{Q}_p^\times$. By our assumption on $\mathcal{O}_\Omega$:

$$H^1_{\mathrm{fl}}(\mathbb{Z}_p, \underline{N}_p) \cong \mathbb{Z}_p^\times / \mathrm{Nr}((\underline{R}_\Omega)_p(\mathbb{Z}_p)) \hookrightarrow \mathbb{Q}_p^\times / \mathrm{N}_{k_P/\mathbb{Q}_p}(k_P^\times) \cong H^1(\mathbb{Q}_p, N_p). \tag{3.4}$$

Proposition 3.3. *Suppose that* $[k:\mathbb{Q}]$ *is prime and that* $\mathrm{Nr}((\underline{R}_\Omega)_p(\mathbb{Z}_p)) = \mathbb{Z}_p^\times \cap \mathrm{N}_{k_P/\mathbb{Q}_p}(k_P^\times)$ *for all* p. *Let* S_r *be the set of primes dividing* Δ_k. *Then there is an exact sequence of abelian groups (compare with formula (5.3) in* [28]*):*

$$1 \to \mathrm{Cl}_\infty(\underline{N}_\Omega) \to H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_\Omega) \to \text{Ш}^1_{S_r \cup \{\infty\}}(\mathbb{Q}, N) \to 1.$$

Proof. Since $H^1_{\mathrm{fl}}(\mathbb{Z}_p, (\underline{N}_\Omega)_p)$ embeds into $H^1(\mathbb{Q}_p, N_p)$ for any prime p by (3.4), the $\mathbb{Z}$-group scheme $\underline{N}_\Omega$ admits the exact sequence (3.3), in which the terms are abelian groups as $\underline{N}_\Omega$ is commutative. The pointed set $\mathrm{Cl}_\infty(\underline{N}_\Omega)$ is in bijection with the first Nisnevich cohomology set $H^1_{\mathrm{Nis}}(\mathbb{Z}, \underline{N}_\Omega)$ (cf. [29, I, Thm. 2.8]), which is a subgroup of $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_\Omega)$ because any Nisnevich cover is flat. Hence the first map is an embedding. Since $k/\mathbb{Q}$ has prime degree and so is necessarily abelian, at any prime p the local Artin reciprocity law implies that

$$n_p = |\mathrm{Gal}(k_P/\mathbb{Q}_p)| = [\mathbb{Q}_p^\times : \mathrm{N}_{k_P/\mathbb{Q}_p}(k_P^\times)] = |H^1(\mathbb{Q}_p, N_p)|.$$

Furthermore, since $[k:\mathbb{Q}]$ is prime, any ramified place p is totally ramified, so $[\mathbb{Z}_p^\times : \mathbb{Z}_p^\times \cap \mathrm{N}_{k_p/\mathbb{Q}_p}(U_P)] = n_p$ [24, Thm. 5.5]. Together with (3.4) this means that $H^1_{\mathrm{fl}}(\mathbb{Z}_p, \underline{N}_p)$ coincides with $H^1(\mathbb{Q}_p, N_p)$ at ramified primes and vanishes elsewhere. Thus the set B of (3.3) consists of classes $[\gamma] \in H^1(\mathbb{Q}, N)$ whose fibers vanish at unramified places. This means that $B = \text{Ш}^1_{S_r \cup \{\infty\}}(\mathbb{Q}, N)$, where S_r is the set of ramified primes of $k/\mathbb{Q}$. □

Remark 3.4. The group $B = \text{Ш}^1_{S_r \cup \{\infty\}}(\mathbb{Q}, N)$ embeds in the group $H^1(\mathbb{Q}, N)$ by definition. But $H^1(\mathbb{Q}, N) \cong \mathbb{Q}^\times / \mathrm{Nr}(k^\times)$, so B has exponent dividing n.

4. Norm forms of orders in quadratic number fields

4.1. Orthogonal groups. Throughout the rest of this article we will assume that k is a quadratic number field, so that $k = \mathbb{Q}(\sqrt{d})$, where $d \notin \{0,1\}$ is a square-free integer. Recall that a *binary integral quadratic form* is a homogeneous polynomial of order two in two variables with coefficients in $\mathbb{Z}$:

$$q : \mathbb{Z}^2 \to \mathbb{Z};\ q(x,y) = ax^2 + bxy + cy^2,\ a,b,c \in \mathbb{Z}.$$

The form q is represented by the symmetric 2×2 matrix $B_q = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ satisfying $q(x,y) = (x,y)B_q(x,y)^t$. We denote q by the triple (a,b,c) and set $\Delta(q) = b^2 - 4ac$. Consider the symmetric bilinear form

$$\widetilde{B_q}(u,v) = q(u+v) - q(u) - q(v),$$

for $u, v \in \mathbb{Z}^2$. Set $\mathrm{disc}(q)$ to be the determinant of the matrix

$$\widetilde{B_q}(e_i, e_j)_{1 \le i,j \le 2},$$

where $e_1 = (1,0)$ and $e_2 = (0,1)$. We say that q is *non-degenerate* over a $\mathbb{Z}$-algebra R if $\operatorname{disc}(q)$ is invertible in R. In particular, q is non-degenerate over $\mathbb{Z}$ when $\operatorname{disc}(q) = \pm 1$ (cf. [13, §2]). It is easily checked that this matrix is $2B_q$, thus $\Delta(q) = -4\det(B_q) = -\operatorname{disc}(q)$. We assume $\Delta(q) \neq 0$, so q is non-degenerate over $\mathbb{Q}$. Observe that q is degenerate over $\mathbb{Z}$ unless $q(x,y) = \pm xy$. Two integral forms q and q' are said to be *isomorphic* over a $\mathbb{Z}$-algebra R if there exists an *R-isometry* from one form to the other, namely a matrix $A \in \underline{\mathrm{GL}}_2(R)$ such that $q \circ A = q'$. If $\det A = 1$, then we say that A gives a *proper isomorphism* over R between q and q'.

Definition 4.1 ([13, p. 303])**.** Let V be a free $\mathbb{Z}$-module of rank two and $q : V \to \mathbb{Z}$ a quadratic form with $\operatorname{disc}(q) \neq 0$. The *orthogonal group* of the quadratic lattice (V,q) is the affine $\mathbb{Z}$-group

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

Since (V,q) is not assumed to be non-degenerate over $\mathbb{Z}$, we note that $\underline{\mathrm{O}}_q$ may fail to be $\mathbb{Z}$-flat for fiber-jumping reasons [14, §2]. We are thus led to restrict our attention to the closed subscheme $\widetilde{\underline{\mathrm{O}}}_q \subset \underline{\mathrm{O}}_q$ defined as the schematic closure in $\underline{\mathrm{O}}_q$ of the generic fiber. Since (V,q) is non-degenerate over $\mathbb{Q}$, and the characteristic of $\mathbb{Q}$ is not 2, we may define the special orthogonal subgroup of the generic fiber $\mathrm{O}_q = \underline{\mathrm{O}}_q \otimes_{\mathbb{Z}} \mathbb{Q}$ naively as

$$\mathrm{O}_q^+ = \ker[\mathrm{O}_q \xrightarrow{\det} \mu_2].$$

The analogous definition over $\mathbb{Z}$ is more subtle but is not limited to the non-degenerate case.

Definition 4.2 ([14, Def. 2.8])**.** The *special orthogonal group* $\underline{\mathrm{O}}_q^+$ of a quadratic lattice (V,q) is the schematic closure of O_q^+ inside $\underline{\mathrm{O}}_q$ (or, equivalently, inside $\widetilde{\underline{\mathrm{O}}}_q$). As $\mathbb{Z}$ is Dedekind it is flat. Indeed, the coordinate ring of the schematic closure, in a $\mathbb{Z}$-scheme, of an affine subscheme of the generic fiber is clearly torsion-free, hence flat over $\mathbb{Z}$.

Remark 4.3. The $\mathbb{Q}$-group O_q is smooth. Its open subgroup O_q^+ is smooth and connected [12, Thm. 1.7 (1)] and is the unique such subgroup [12, Prop. 3.2]. By the correspondence between flat closed subschemes of $\underline{\mathrm{O}}_q$ and closed subschemes of O_q [23, Prop. 2.8.1], $\underline{\mathrm{O}}_q^+$ is the unique flat and closed subgroup of $\underline{\mathrm{O}}_q$ whose generic fiber is O_q^+.

Definition 4.4. Let $\Omega = \{\omega_1, \omega_2\} \subset \mathcal{O}_k$ be a basis of a quadratic order $\mathcal{O}_\Omega \subseteq \mathcal{O}_k$. The *norm form* associated to Ω is the integral quadratic form

$$q_\Omega(x,y) := \mathrm{Nr}(x\omega_1 + y\omega_2).$$

Let $\underline{\mathrm{O}}_\Omega$ denote the orthogonal group of q_Ω. The choice of the basis Ω specifies an isomorphism of $\mathbb{Z}$-modules $r : \mathbb{Z}^2 \xrightarrow{\sim} \mathcal{O}_\Omega$ given by $r(x,y) =$

$x\omega_1 + y\omega_2$. In turn, as we observed at the beginning of Section 2, the map r induces an embedding $\iota : \underline{R}_\Omega \hookrightarrow \underline{\mathrm{GL}}_2$.

Lemma 4.5. *Let Ω be a basis of the quadratic order $\mathcal{O}_\Omega \subseteq \mathcal{O}_k$. Then $\underline{\mathrm{O}}_\Omega^+ = \underline{N}_\Omega$ as subgroup schemes of $\underline{\mathrm{GL}}(\mathcal{O}_\Omega)$.*

Proof. Over $\mathbb{Q}$, consider the map $q_\Omega = \mathrm{Nr} \circ r : \mathbb{Q}^2 \to \mathbb{Q}$. For any $b \in R_\Omega$ and $(x, y) \in \mathbb{Z}^2$ one has

$$\iota(b) \cdot \begin{pmatrix} x \\ y \end{pmatrix} = r^{-1} \left(b \cdot r \begin{pmatrix} x \\ y \end{pmatrix} \right).$$

If $b \in N_\Omega = \ker(\mathrm{Nr} : R_\Omega \to \mathbb{G}_{m,\mathbb{Q}})$ and we also use b to denote multiplication by b in $\mathcal{O}_\Omega$, then $\mathrm{Nr} \circ b = \mathrm{Nr}$. We obtain an inclusion of $\mathbb{Q}$-groups:

$$\begin{aligned} \mathrm{O}_\Omega^+ &= \{A \in \mathrm{SL}_2 : q_\Omega \circ A = q_\Omega\} \\ &\supseteq \{b \in N_\Omega : q_\Omega \circ \iota(b) = q_\Omega\} = \{b \in N_\Omega : q_\Omega \circ r^{-1} \circ b \cdot r = q_\Omega\} \\ &= \{b \in N_\Omega : \mathrm{Nr} \circ b \cdot r = \mathrm{Nr} \circ r\} = \{b \in N_\Omega : \mathrm{Nr} \circ b = \mathrm{Nr}\} = N_\Omega. \end{aligned}$$

Since O_Ω^+ and N_Ω are both one-dimensional tori, the inclusion is an equality. Hence $\underline{\mathrm{O}}_\Omega^+$ and $\underline{N}_\Omega$ are $\mathbb{Z}$-flat closed subgroups of $\underline{\mathrm{O}}_\Omega$ with the same generic fiber $\mathrm{O}_\Omega^+ = N_\Omega$. Such an object is unique by Remark 4.3, so $\underline{\mathrm{O}}_\Omega^+ = \underline{N}_\Omega$. □

Remark 4.6. Since the norm subgroup $\underline{N}_\Omega$ is clearly normal in $\underline{\mathrm{GL}}(\mathcal{O}_\Omega)$, an immediate consequence of Lemma 4.5 is that $\underline{\mathrm{O}}_\Omega^+$ is a normal subgroup scheme of $\underline{\mathrm{O}}_\Omega$.

We note that for the particular bases Ω used in the sequel, Lemma 4.5 can be checked explicitly; see Remark A.3.

4.2. Orders in quadratic fields. Recall that $k = \mathbb{Q}(\sqrt{d})$. For every $m \in \mathbb{N}$, the maximal order $\mathcal{O}_k$ contains a unique order $\mathcal{O}_{d,m}$ of index m. If $\{1, \omega\}$ is any $\mathbb{Z}$-basis of $\mathcal{O}_k$, then $\mathcal{O}_{d,m}$ is spanned by $\{1, m\omega\}$. We fix the convenient $\mathbb{Z}$-basis $\Omega_{d,m} = \{1, \omega_{d,m}\}$ of $\mathcal{O}_{d,m}$, where

$$\omega_{d,m} = \begin{cases} \frac{1+m\sqrt{d}}{2} & : d \equiv 1 \bmod 4,\ m \,\mathrm{odd} \\ \frac{m}{2}\sqrt{d} & : d \equiv 1 \bmod 4,\ m \,\mathrm{even} \\ m\sqrt{d} & : d \equiv 2, 3 \bmod 4. \end{cases}$$

Henceforth we denote by $q_{d,m}$ the associated norm form $q_{\Omega_{d,m}}$. We also set $q_d = q_{d,1}$. Define

$$c_{d,m} = \begin{cases} \frac{1-m^2 d}{4} & : d \equiv 1 \bmod 4,\ m \,\mathrm{odd} \\ \frac{m^2 d}{4} & : d \equiv 1 \bmod 4,\ m \,\mathrm{even} \\ m^2 d & : d \equiv 2, 3 \bmod 4 \end{cases} \tag{4.1}$$

and note that $c_{d,m}$ is always an integer. For simplicity in long expressions, we will sometimes drop the subscripts and write c for $c_{d,m}$; this should cause no confusion. We also write $\underline{\mathrm{O}}_{d,m}$ for $\underline{\mathrm{O}}_{q_{d,m}}$, $\widetilde{\underline{\mathrm{O}}}_{d,m}$ for $\widetilde{\underline{\mathrm{O}}}_{d,m}$, etc. We say that we are in

Case (I) if $d \equiv 1 \bmod 4$ and m is odd, and in

Case (II) otherwise.

Then

$$(4.2)\quad q_{d,m} = \begin{cases} (1,1,c_{d,m}) & : \text{Case (I)} \\ (1,0,-c_{d,m}) & : \text{Case (II)}. \end{cases}$$

$$\text{and}\quad B_{q_{d,m}} = \begin{cases} \begin{pmatrix} 1 & 1/2 \\ 1/2 & c_{d,m} \end{pmatrix} & : \text{Case (I)} \\ \begin{pmatrix} 1 & 0 \\ 0 & -c_{d,m} \end{pmatrix} & : \text{Case (II)}. \end{cases}$$

Hence

$$(4.3)\ \underline{N}_{d,m} := \underline{N}_{\Omega_{d,m}} = \begin{cases} \operatorname{Spec} \mathbb{Z}[x,y]/(x^2+xy+c_{d,m}y^2-1) & : \text{Case (I)} \\ \operatorname{Spec} \mathbb{Z}[x,y]/(x^2-c_{d,m}y^2-1) & : \text{Case (II)}. \end{cases}$$

The integral matrix realization $\iota(\underline{N}_{d,m}(\mathbb{Z}))$ is given by

$$(4.4)\qquad A_d = \begin{cases} \begin{pmatrix} x & y \\ -c_{d,m}y & x+y \end{pmatrix}, \ \det = 1 & : \text{Case (I)} \\ \begin{pmatrix} x & y \\ c_{d,m}y & x \end{pmatrix}, \ \det = 1 & : \text{Case (II)}. \end{cases}$$

For any pair (d,m), the integral model $\underline{N}_{d,m}$ has the generic fiber

$$N_{d,m} = \underline{N}_{d,m} \otimes_{\mathbb{Z}} \mathbb{Q} = \operatorname{Spec} \mathbb{Q}[x,y]/(x^2-dy^2-1).$$

Note that $N_{d,m}$ is independent of m.

5. The flat cohomology of the orthogonal group of a norm form

5.1. A quotient map. The special orthogonal subgroup $\underline{\mathrm{O}}^{+}_{d,m}$ is a flat closed normal subgroup of $\underline{\mathrm{O}}_{d,m}$ by Remarks 4.3 and 4.6. Since $\operatorname{Spec}\mathbb{Z}$ is one-dimensional, the fppf quotient $\underline{\mathrm{O}}_{d,m}/\underline{\mathrm{O}}^{+}_{d,m}$ is representable by [1, Thm. 4.C] and thus has the structure of an affine $\mathbb{Z}$-group scheme. However, this quotient is not flat. Instead, we consider the quotient $\underline{Q}_{d,m} = \widetilde{\underline{\mathrm{O}}}_{d,m}/\underline{\mathrm{O}}^{+}_{d,m}$, which is flat over $\mathbb{Z}$ because $\widetilde{\underline{\mathrm{O}}}_{d,m}$ is. Our first goal in this section is to determine the structure of $\underline{Q}_{d,m}$, for which we will use the theory of finite flat group schemes. An alternative proof, by means of explicitly writing out defining equations, is presented in an appendix at the end of the paper.

Recall that there are only two finite $\mathbb{Z}$-groups of order two, up to isomorphism, namely $\underline{\mathbb{Z}/2} = \operatorname{Spec}\mathbb{Z}[t]/(t^2-t)$ and $\underline{\mu}_2 = \operatorname{Spec}\mathbb{Z}[t]/(t^2-1)$; see, for instance, the Corollary on p. 21 of [32] for a proof of this fact. These two $\mathbb{Z}$-groups are locally isomorphic everywhere except at (2), in which case $\underline{\mu}_2 \otimes_{\mathbb{Z}} \mathbb{F}_2$ contains one nilpotent point while $\underline{\mathbb{Z}/2} \otimes_{\mathbb{Z}} \mathbb{F}_2$ is reduced and contains two points.

Proposition 5.1. *Let $d \neq 0, 1$ be square-free and $m \in \mathbb{N}$. Then, as $\mathbb{Z}$-group schemes,*

$$\widetilde{\underline{\mathrm{O}}}_{d,m}/\underline{\mathrm{O}}^{+}_{d,m} \simeq \begin{cases} \underline{\mathbb{Z}/2} & : \text{Case (I)} \\ \underline{\mu}_2 & : \text{Case (II)}. \end{cases}$$

Proof. Recall from Definition 4.1 that for any quadratic form q, an isometry $A \in \underline{\mathrm{O}}_q$ satisfies $q \circ A = q$ and hence $AB_qA^t = B_q$. Taking determinants of both sides, we find that $(\det B_q)((\det A)^2 - 1) = 0$. In particular, if q is non-degenerate over $\mathbb{Q}$, then any $A \in \widetilde{\underline{\mathrm{O}}}_q$ satisfies $(\det A)^2 - 1 = 0$. Hence the determinant induces a morphism of group schemes $\det : \widetilde{\underline{\mathrm{O}}}_q \to \underline{\mu}_2$.

Since $\widetilde{\underline{\mathrm{O}}}_{d,m}$ is a $\mathbb{Z}$-scheme defined by the polynomial $(\det A - 1)(\det A + 1)$, among others, it is the scheme-theoretic union of the closed $\mathbb{Z}$-subschemes of matrices of determinant 1 and -1. The former of these is $\underline{\mathrm{O}}^{+}_{d,m}$, and we denote the latter by $\underline{\mathrm{O}}^{-}_{d,m}$. The left translation action on $\widetilde{\underline{\mathrm{O}}}_{d,m}$ of $\left(\begin{smallmatrix} 1 & 0 \\ 1 & -1 \end{smallmatrix}\right)$ in Case (I) and of $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ in Case (II) interchanges the subschemes $\underline{\mathrm{O}}^{+}_{d,m}$ and $\underline{\mathrm{O}}^{-}_{d,m}$. Hence all fibers of $\underline{Q}_{d,m}$ have rank two, and we conclude that $\underline{Q}_{d,m}$ is a finite flat affine $\mathbb{Z}$-group scheme of order two. Thus it is isomorphic either to $\underline{\mathbb{Z}/2}$ or to $\underline{\mu}_2$. To distinguish between the two possibilities, it suffices to determine $\underline{Q}_{d,m} \otimes_{\mathbb{Z}} \mathbb{F}_2$. Since the reduction of $\mathrm{diag}(1, -1)$ modulo 2 is the same as that of the identity matrix, we see that $\underline{Q}_{d,m} \otimes_{\mathbb{Z}} \mathbb{F}_2$ contains only one point in Case (II). In Case (I), on the other hand, it is apparent from (4.4) and Lemma 4.5 that the reduction modulo 2 of the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 1 & -1 \end{smallmatrix}\right)$ does not lie in that of $\underline{N}_{d,m}(\mathbb{Z}) = \underline{\mathrm{O}}^{+}_{d,m}(\mathbb{Z})$. Thus $\underline{Q}_{d,m} \otimes_{\mathbb{Z}} \mathbb{F}_2$ has two points in this case. We conclude that $\underline{Q}_{d,m} = \underline{\mathbb{Z}/2}$ in Case (I) and $\underline{Q}_{d,m} = \underline{\mu}_2$ in Case (II), as claimed. □

5.2. Twisted forms. In this section we briefly recall the construction of a twisted form (in the fppf topology) of a flat group scheme $\underline{G}$ defined over $\operatorname{Spec} R$, where R is a unital commutative ring. From now on, we refer to the fppf topology as the flat topology. A representative P of a class in $H^1_{\mathrm{fl}}(R, \underline{G})$, i.e. a $\underline{G}$-torsor, gives rise to the affine R-group scheme ${}^{P}\underline{G}$ given by the quotient of $P \times_R \underline{G}$ by the $\underline{G}$-action $s \cdot (p, g) = (ps^{-1}, sgs^{-1})$. This is an inner form of $\underline{G}$, called the *twist* of $\underline{G}$ by P. It is isomorphic to $\underline{G}$ in the flat topology, and the map $Q \mapsto {}^{P}Q$ where Q is any $\underline{G}$-torsor, defines a bijection of pointed sets $\theta_P : H^1_{\mathrm{fl}}(R, \underline{G}) \to H^1_{\mathrm{fl}}(R, {}^{P}\underline{G})$; see [31, §2.2, Lem. 2.2.3, and the nearby Ex. 1 and 2].

Remark 5.2. Fix a quadratic $\mathbb{Z}$-form q of arbitrary rank with automorphism group $\mathrm{Aut}(q) := \underline{\mathrm{O}}_q$ defined over $\operatorname{Spec} \mathbb{Z}$. Any $\underline{\mathrm{O}}_q$-torsor, for the flat topology, is of the form $P = \mathrm{Iso}(q, q')$, where q' is a quadratic $\mathbb{Z}$-form isomorphic to q in the flat topology. This is a special case of a general framework due to Giraud; see [8, Prop. 2.2.4.5] for details. It follows that

$\underline{\mathrm{O}}_{q'}$ is an inner form of $\underline{\mathrm{O}}_q$, namely its twist by P. In terms of the classification of $\underline{\mathrm{O}}_q$-torsors by cohomology classes, this corresponds to changing the distinguished base point of $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q)$.

Remark 5.3. For any flat, i.e. torsion-free, $\mathbb{Z}$-algebra R the inclusion $\widetilde{\underline{\mathrm{O}}}_q(R) \subseteq \underline{\mathrm{O}}_q(R)$ of R-points is an equality. This implies a canonical isomorphism of pointed sets $H^1_{\mathrm{fl}}(\mathbb{Z}, \widetilde{\underline{\mathrm{O}}}_q) = H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q)$. In the sequel we identify these sets without further comment.

Lemma 5.4. *Let ${}^P\underline{\mathrm{O}}_q$ be the twisted form of $\underline{\mathrm{O}}_q$ by an $\underline{\mathrm{O}}_q^+$-torsor P and let $\underline{Q} := \widetilde{\underline{\mathrm{O}}}_q/\underline{\mathrm{O}}_q^+$. Then the following are equivalent:*

1. *The push-forward map $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q^+) \xrightarrow{i_*} H^1_{\mathrm{fl}}(\mathbb{Z}, \widetilde{\underline{\mathrm{O}}}_q)$ is injective.*
2. *The quotient map ${}^P\widetilde{\underline{\mathrm{O}}}_q(\mathbb{Z}) \xrightarrow{\pi} \underline{Q}(\mathbb{Z})$ is surjective for any $[P] \in H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q^+)$.*
3. *The $\underline{Q}(\mathbb{Z})$-action on $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q^+)$ is trivial.*

Proof. By the correspondence discussed above between quadratic $\mathbb{Z}$-forms and $\underline{\mathrm{O}}_q$-torsors, the inner form ${}^P\underline{\mathrm{O}}_q$ of $\underline{\mathrm{O}}_q$ is the orthogonal group of some quadratic $\mathbb{Z}$-form q'. Consider the commutative diagram with exact rows (cf. [21, Lem. III.3.3.4])

$$\begin{tikzcd}
\widetilde{\underline{\mathrm{O}}}_q(\mathbb{Z}) \arrow[r, "\pi"] & \underline{Q}(\mathbb{Z}) \arrow[r] & H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q^+) \arrow[r, "i_*"] \arrow[d, "\theta_P", "\cong"'] & H^1_{\mathrm{fl}}(\mathbb{Z}, \widetilde{\underline{\mathrm{O}}}_q) \arrow[d, "\theta_P", "\cong"'] \\
{}^P\widetilde{\underline{\mathrm{O}}}_q(\mathbb{Z}) \arrow[r, "{}^P\pi"] & \underline{Q}(\mathbb{Z}) \arrow[r] & H^1_{\mathrm{fl}}(\mathbb{Z}, {}^P\underline{\mathrm{O}}_q^+) \arrow[r, "i'_*"] & H^1_{\mathrm{fl}}(\mathbb{Z}, {}^P\widetilde{\underline{\mathrm{O}}}_q),
\end{tikzcd}$$

where the top row arises by applying flat cohomology to the sequence $1 \to \underline{\mathrm{O}}_q^+ \to \widetilde{\underline{\mathrm{O}}_q} \to \underline{Q} \to 1$, whereas the bottom row comes from the analogous sequence for q' and the maps θ_P are the induced twisting bijections defined above.

$(1) \Leftrightarrow (2)$. The map i_* is injective if any class $[P]$ of $\underline{\mathrm{O}}_q^+$-torsors is the unique pre-image of $i_*([P]) \in H^1_{\mathrm{fl}}(\mathbb{Z}, \widetilde{\underline{\mathrm{O}}}_q) = H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q)$. By commutativity of the diagram, this is equivalent to the distinguished point in $H^1_{\mathrm{fl}}(\mathbb{Z}, {}^P\underline{\mathrm{O}}_q^+)$ being the unique pre-image of its image, for any choice of a twisted form ${}^P\underline{\mathrm{O}}_q^+$ of $\underline{\mathrm{O}}_q^+$, i.e. to the triviality of $\ker(i'_*)$ for any $\underline{\mathrm{O}}_q^+$-torsor P. By exactness of the rows, this is condition (2).

$(1) \Leftrightarrow (3)$. By [21, Prop. III.3.3.3 (iv)], i_* induces an injection of $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q^+)/\underline{Q}(\mathbb{Z})$ into $H^1_{\mathrm{fl}}(\mathbb{Z}, \widetilde{\underline{\mathrm{O}}}_q)$. Thus $i_* : H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q^+) \to H^1_{\mathrm{fl}}(\mathbb{Z}, \widetilde{\underline{\mathrm{O}}}_q)$ is injective if and only if $\underline{Q}(\mathbb{Z})$ acts on $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q^+)$ trivially. □

5.3. Case (I)**.** Recall that Case (I) means that $d \equiv 1 \bmod 4$ and m is odd. In this case the quotient $\underline{\widetilde{\mathrm{O}}}_{d,m}/\underline{\mathrm{O}}^+_{d,m}$ is $\underline{\mathbb{Z}/2}$ by Proposition 5.1, the quotient map being the Dickson morphism $D_{q_{d,m}}$.

Proposition 5.5. *In Case* (I)*, there is an equality of abelian groups* $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_{d,m}) = H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_{d,m})$.

Proof. Applying flat cohomology to the short exact sequence of flat $\mathbb{Z}$-schemes

$$1 \to \underline{\mathrm{O}}^+_{d,m} \to \underline{\widetilde{\mathrm{O}}}_{d,m} \to \underline{Q}_{d,m} \to 1$$

gives rise to a long exact sequence of pointed sets

$$(5.1)\quad \underline{\widetilde{\mathrm{O}}}_{d,m}(\mathbb{Z}) \to \underline{Q}_{d,m}(\mathbb{Z}) \to H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}^+_{d,m}) \xrightarrow{i_*} H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_{d,m}) \xrightarrow{\delta} H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{Q}_{d,m}).$$

We will show that i_* is an isomorphism; the claim then follows by Lemma 4.5. Since $\underline{\mathbb{Z}/2}$ is smooth, the rightmost term in (5.1) coincides with $H^1_{\text{ét}}(\mathbb{Z}, \underline{\mathbb{Z}/2})$ by [2, Corollaire VIII.2.3], which classifies étale quadratic covers of $\mathbb{Z}$ (cf. [26, Chap. III, Prop. 4.1.4]). As no such non-trivial cover exists, δ is trivial, and i_* is surjective.

To prove that i_* is injective, it suffices by Lemma 5.4 to show that the map ${}^P\underline{\widetilde{\mathrm{O}}}_{d,m}(\mathbb{Z}) \to \underline{\mathbb{Z}/2}(\mathbb{Z})$ is surjective for all $[P] \in H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}^+_{d,m})$. This is true when $[P]$ is the distinguished class, since we verified explicitly in the course of the proof of Proposition 5.1 that $D_{q_{d,m}} : \underline{\widetilde{\mathrm{O}}}_{d,m}(\mathbb{Z}) \to \underline{\mathbb{Z}/2}(\mathbb{Z})$ is surjective. In fact, this implies that the determinant map $\underline{\widetilde{\mathrm{O}}}_{d,m}(\mathbb{Z}) \to \underline{\mu}_2(\mathbb{Z}) = \{\pm 1\}$ is surjective on $\mathbb{Z}$-points. In general, ${}^P\underline{\mathrm{O}}^+_{d,m}$ is an inner form of $\underline{\mathrm{O}}^+_{d,m}$ by Remark 5.2, and thus it is a conjugate of $\underline{\mathrm{O}}^+_{d,m}$ by some $M \in \mathrm{GL}_2(R)$ for a finite flat extension $R/\mathbb{Z}$. But ${}^P\underline{\mathrm{O}}^+_{d,m}$ is the special orthogonal group of a quadratic $\mathbb{Z}$-form q and $\underline{\mathrm{O}}_q = M\underline{\mathrm{O}}_{d,m}M^{-1}$. Conjugation preserves the determinant, so $\underline{\widetilde{\mathrm{O}}}_q(\mathbb{Z}) \overset{\det}{\to} \underline{\mu}_2(\mathbb{Z})$ is surjective, and hence so is $D_q : \underline{\widetilde{\mathrm{O}}}_q(\mathbb{Z}) \to \underline{\mathbb{Z}/2}(\mathbb{Z})$. □

5.4. Case (II)**.** In this case, we know from Proposition 5.1 that the determinant map induces an isomorphism $\underline{\widetilde{\mathrm{O}}}_{d,m}/\underline{\mathrm{O}}^+_{d,m} \simeq \underline{\mu}_2$. The relevant bit of the long exact sequence (5.1) is:

$$H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}^+_{d,m}) \xrightarrow{i_*} H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_{d,m}) \overset{\mathrm{disc}}{\twoheadrightarrow} H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mu}_2) \cong \{\pm 1\}.$$

Here disc, which assigns to any class $[q] \in H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_{d,m})$ the sign of the discriminant of q, is surjective because $[(1, 0, c_{d,m})], [(1, 0, -c_{d,m})] \in H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_{d,m})$; observe that $(1, 0, c_{d,m})$ becomes isomorphic to $(1, 0, -c_{d,m})$ over $\mathbb{Z}[\sqrt{-1}]$ by the isometry $A = \mathrm{diag}(1, \sqrt{-1})$.

Lemma 5.6. *Suppose that Case* (II) *holds, so* $q = (1, 0, -c_{d,m})$, *i.e.* $q(x, y) = x^2 - c_{d,m}y^2$. *Then*

$$H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_{d,m}) = H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}^+_{d,m})/\underline{\mu}_2(\mathbb{Z}) \coprod H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}^+_{(1,0,c_{d,m})})/\underline{\mu}_2(\mathbb{Z}), \tag{5.2}$$

where the non-trivial element of $\underline{\mu}_2(\mathbb{Z})$ *maps* $[(a, b, c)]$ *to* $[(a, -b, c)]$.

Proof. The action of the non-trivial element of $\underline{\mu}_2(\mathbb{Z}) = \{\pm 1\}$ on $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}^+_{d,m})$ is described by [21, Rmq. III.3.3.2]. The pre-image of -1 under $\det : \widetilde{\underline{\mathrm{O}}}_{q,m} \to \underline{\mu_2}$ is $\underline{\mathrm{O}}^-_{d,m} := \mathrm{diag}(1, -1)\underline{\mathrm{O}}^+_{d,m}$. A twisted form of $\underline{\mathrm{O}}^+_{d,m}$ by some $\underline{\mathrm{O}}^+_{d,m}$-torsor is $\underline{\mathrm{O}}^+_{q'}$ where q' is of discriminant $4c_{d,m}$. Then the action of -1 on $\underline{\mathrm{O}}^+_{q'}$ is a twist by $\underline{\mathrm{O}}^-_{d,m}$, which is equivalent to the twist of $q' = (a, b, c)$ by $\mathrm{diag}(1, -1)$ to $(a, -b, c)$:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^t = \begin{pmatrix} a & -b/2 \\ -b/2 & c \end{pmatrix}.$$

Observe that $\widetilde{\underline{\mathrm{O}}}_{d,m}$ may be realized as a semi-direct product $\underline{\mathrm{O}}^+_{d,m} \rtimes \underline{\mu}_2$ by means of the section $x \mapsto \mathrm{diag}(1, x)$ of the quotient map $\widetilde{\underline{\mathrm{O}}}_{d,m} \overset{\det}{\to} \underline{\mu}_2$. By [19, Lem. 2.6.3], this implies the claimed decomposition

$$\begin{aligned} H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_{d,m}) &= H^1_{\mathrm{fl}}(\mathbb{Z}, \widetilde{\underline{\mathrm{O}}}_{d,m}) \\ &= H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}^+_{(1,0,c_{d,m})})/\underline{\mu}_2(\mathbb{Z}) \coprod H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}^+_{(1,0,-c_{d,m})})/\underline{\mu}_2(\mathbb{Z}), \end{aligned} \tag{5.3}$$

where the quotients are taken modulo the equivalence relation given by the action of $\underline{\mu}_2(\mathbb{Z})$ on each group as above. Indeed, the twisted form $(1, 0, c_{d,m})$ of discriminant $-4c_{d,m}$ corresponds to the non-trivial $\underline{\mu}_2$-torsor represented by $\{t^2 = -1\}$, which splits over $\mathbb{Z}[\sqrt{-1}]$ and is represented by

$$\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -c_{d,m} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{-1} \end{pmatrix}^t = \begin{pmatrix} 1 & 0 \\ 0 & c_{d,m} \end{pmatrix}. \qquad \square$$

Corollary 5.7. *Each of the groups* $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}^+_{d,m})$ *and* $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}^+_{(1,0,c_{d,m})})$ *is entirely embedded in* $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_{d,m})$ *if and only if it satisfies one (hence all) of the conditions of Lemma 5.4.*

Remark 5.8. Although the groups $\widetilde{\underline{\mathrm{O}}}_{d,m}$ and $\widetilde{\underline{\mathrm{O}}}_{(1,0,c_{d,m})}$ are not isomorphic, Lemma 5.6 provides the same decomposition of $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_{d,m})$ as of $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_{(1,0,c_{d,m})})$. Hence these two pointed sets are in bijection with each other. Observe that

$$\widetilde{\underline{\mathrm{O}}}_{(1,0,c_{d,m})} = \begin{cases} \widetilde{\underline{\mathrm{O}}}_{-d,m/2} & : d \equiv 1 \bmod 4,\ m \text{ even} \\ \widetilde{\underline{\mathrm{O}}}_{-d,m} & : d \equiv 2 \bmod 4 \\ \widetilde{\underline{\mathrm{O}}}_{-d,2m} & : d \equiv 3 \bmod 4. \end{cases}$$

Example 5.9. In this and the subsequent examples in this section, we set $\underline{N}'_d = \underline{N}_{d,2}$ for brevity. The set $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_{11})$ contains $2h_{11} = 2$ classes $\{[\pm(1, 0, -11)]\}$; see Lemma 5.19 below. Each of these classes is a separate $\underline{\mu}_2(\mathbb{Z})$-orbit. However, $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}'_{-11})$ contains six classes by [7, p. 20]; see the table in Example 5.13 below. Precisely, we have $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}'_{-11}) = \{[\pm(1, 0, 11)], [\pm(3, \pm 2, 4)]\}$. The pairs $(3, \pm 2, 4)$ and $(-3, \pm 2, -4)$ coincide in $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_{11})$. Thus $|H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_{11})| = 2 + 4 = 6$.

Our next aim is to use Lemma 5.6 to study $\mathrm{Pic}\,\mathbb{Z}[\sqrt{d}]$ even in cases where $\mathbb{Z}[\sqrt{d}]$ is not the maximal order of a number field and thus need not be a Dedekind domain. As a preliminary, we record the following exercise in algebraic number theory.

Lemma 5.10. *Let d be any integer. The ring $\mathbb{Z}[\sqrt{d}]$ has a unique prime ideal containing 2.*

Proof. The case $d \in \{0, 1\}$ is obvious, so we assume that it does not hold. We may assume without loss of generality that d is square-free. If $d \equiv 2, 3 \pmod 4$, then $\mathbb{Z}[\sqrt{d}] = \mathcal{O}_d$ is a Dedekind domain and 2 ramifies in $\mathbb{Q}(\sqrt{d})$, so that $2\mathcal{O}_d = \mathfrak{p}^2$, where $\mathfrak{p}$ is the unique prime ideal of $\mathcal{O}_d$ dividing (2). Now suppose that $d \equiv 1 \pmod 4$. Then $\mathcal{O}_d/\mathbb{Z}[\sqrt{d}]$ is an integral extension of rings, so by [27, Thm. 9.3] any prime ideal of $\mathbb{Z}[\sqrt{d}]$ has the form $\mathbb{Z}[\sqrt{d}] \cap \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_d$. If $d \equiv 5 \pmod 8$, then 2 is inert in $\mathbb{Q}(\sqrt{d})$. Thus $2\mathcal{O}_d$ is prime and is the unique prime ideal of $\mathcal{O}_d$ containing 2; this implies our claim by the previous observation. If $d \equiv 1 \pmod 8$, then $2\mathcal{O}_d = \mathfrak{p}_1\mathfrak{p}_2 = \mathfrak{p}_1 \cap \mathfrak{p}_2$ for distinct prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of $\mathcal{O}_d$. Hence $\mathbb{Z}[\sqrt{d}] \cap \mathfrak{p}_1$ and $\mathbb{Z}[\sqrt{d}] \cap \mathfrak{p}_2$ each contain $I = \mathbb{Z}[\sqrt{d}] \cap 2\mathcal{O}_d = \{a + b\sqrt{d} : a \equiv b \pmod 2\}$. Since I has index 2 in the ring $\mathbb{Z}[\sqrt{d}]$ and thus is a maximal ideal, it is the unique prime ideal of $\mathbb{Z}[\sqrt{d}]$ containing 2. □

Proposition 5.11. *Let $d \equiv 3 \pmod{4}$. Set $\eta(d) = 1$ if $d \equiv 3 \pmod{8}$ and one of the following two conditions holds:*

- *$d > 3$*
- *$d < 0$ and $\mathcal{O}^{\times}_{-d} \subset \mathbb{Z}[\sqrt{-d}]$.*

Otherwise, set $\eta(d) = 0$. Then $|\mathrm{Pic}\,\mathbb{Z}[\sqrt{-d}]| = 3^{\eta(d)} h_{-d}$.

Proof. Observe that $-d \equiv 1 \bmod 4$, and thus $\mathbb{Z}[\sqrt{-d}] = \mathcal{O}_{-d,2}$. We write Ω for $\Omega_{-d,2} = \{1, \sqrt{-d}\}$.

The claim is clear if $d = -1$, so suppose that $d \equiv 3 \pmod 4$ and $d \neq -1$. By Lemma 4.5, the special orthogonal group $\underline{N}_{-d,2}$ is equal to $\underline{\mathrm{O}}^+_\Omega$. Set $k' = \mathbb{Q}(\sqrt{-d})$. We relate the Picard groups of $\mathcal{O}_\Omega = \mathbb{Z}[\sqrt{-d}]$ and $\mathcal{O}_{-d,1} = \mathcal{O}_{k'} = \mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$ by studying their localizations. For any prime ideal $\mathfrak{p}$ of

$\mathcal{O}_\Omega$, let $\mathcal{O}_\mathfrak{p}$ be the localization of $\mathcal{O}_\Omega$ at $\mathfrak{p}$, and let $(\mathcal{O}_{k'})_\mathfrak{p}$ be the integral closure of $\mathcal{O}_\mathfrak{p}$ in $\mathcal{O}_{k'}$. Then [25, Thm. 5.6] provides an exact sequence of abelian groups

$$1 \to \mathcal{O}_\Omega^\times \xrightarrow{\varphi} \mathcal{O}_{k'}^\times \to \bigoplus_{\mathfrak{p}} (\mathcal{O}_{k'})_\mathfrak{p}^\times / \mathcal{O}_\mathfrak{p}^\times \to \operatorname{Pic} \mathcal{O}_\Omega \to \operatorname{Pic} \mathcal{O}_{k'} \to 1. \tag{5.4}$$

Here the direct sum in the middle runs over the prime ideals of $\mathcal{O}_\Omega$. Let $\mathcal{F}$ denote the conductor of $\mathcal{O}_{k'}/\mathcal{O}_\Omega$. By [25, Prop. 6.2] we have the following isomorphism for any $\mathfrak{p}$:

$$(\mathcal{O}_{k'})_\mathfrak{p}^\times / \mathcal{O}_\mathfrak{p}^\times \cong ((\mathcal{O}_{k'})_\mathfrak{p} / \mathcal{F} \cdot (\mathcal{O}_{k'})_\mathfrak{p})^\times \Big/ (\mathcal{O}_\mathfrak{p}/\mathcal{F}\mathcal{O}_\mathfrak{p})^\times. \tag{5.5}$$

Since $\mathcal{O}_\Omega = \mathbb{Z} + 2\mathcal{O}_{k'}$, the conductor is $\mathcal{F} = 2\mathcal{O}_{k'}$. It is a maximal ideal of $\mathcal{O}_\Omega$; since localization at any prime commutes with factorization modulo $\mathcal{F}$, we have $(\mathcal{O}_\mathfrak{p}/\mathcal{F}\mathcal{O}_\mathfrak{p})^\times = (\mathcal{O}_\Omega/\mathcal{F}\mathcal{O}_\Omega)_\mathfrak{p}^\times = \mathbb{F}_2^\times = 1$. Moreover, we see that $(\mathcal{O}_{k'})_\mathfrak{p}^\times \cong \mathcal{O}_\mathfrak{p}^\times$ if $2 \notin \mathfrak{p}$, so such places make no contribution to the direct sum in (5.4). It remains therefore to compute $(\overline{\mathcal{O}}_{k'})_\mathfrak{q}^\times$ for the unique (by Lemma 5.10) place $\mathfrak{q}$ containing 2, where $\overline{\mathcal{O}}_{k'}$ denotes the reduction of $\mathcal{O}_{k'}$ modulo $\mathcal{F}$. Note that $\mathcal{O}_\Omega/\mathcal{F} \simeq \mathbb{F}_2$ and that $c = \frac{1+d}{4}$ is odd if $d \equiv 3 \pmod 8$ and even if $d \equiv 7 \pmod 8$. If $\bar{c} \in \mathbb{F}_2$ is the image of c, then it follows from (4.4) that

$$\begin{aligned}(\overline{\mathcal{O}}_{k'})_\mathfrak{q}^\times &\cong (\overline{R}_{-d}(\mathbb{F}_2))_\mathfrak{q} = \left\{ (\overline{A}_{-d})_\mathfrak{q} = \left(\begin{smallmatrix} a & \bar{c}b \\ b & a+b \end{smallmatrix}\right) : a, b \in \mathbb{F}_2,\ \det(\overline{A}_{-d}) \neq 0 \right\} \\ &\cong \begin{cases} \mathbb{Z}/3 & d \equiv 3 \pmod 8 \\ 1 & d \equiv 7 \pmod 8. \end{cases}\end{aligned}$$

This holds also when $d = -1$. We deduce from (5.4) that if $d \equiv 7 \pmod 8$, then $\operatorname{Pic} \mathcal{O}_\Omega \simeq \operatorname{Pic} \mathcal{O}_{-d}$. If $d \equiv 3 \pmod 8$, then (5.4) implies that

$$\frac{|\operatorname{Pic}(\mathcal{O}_\Omega)|}{h_{-d}} = \frac{3}{|\operatorname{coker}(\varphi)|}. \tag{5.6}$$

If $d \neq 3$, the unit groups $\mathcal{O}_\Omega^\times$ and $\mathcal{O}_{k'}^\times$ contain the same roots of unity. Moreover, if $d > 0$, these groups have no free part, hence $|\operatorname{coker}(\varphi)| = 1$. If $d = 3$, then clearly $|\operatorname{coker}(\varphi)| = 3$. If $d < 0$, then the free parts of both $\mathcal{O}_\Omega^\times$ and $\mathcal{O}_{k'}^\times$ have rank 1, and $\operatorname{coker}(\varphi) = [\langle\varepsilon\rangle : \langle\varepsilon^m\rangle] = m$, where ε is a fundamental unit of k' and ε^m is a generator of $\mathcal{O}_\Omega^\times$. Note that $m|3$ by (5.4), so that $m = 3$ or $m = 1$. Both cases do arise. The case $m = 1$ occurs, for instance, when $d = -37$ and $d = -101$; see sequence A108160 in the *On-Line Encyclopedia of Integer Sequences*. Hence, recalling the definition of $\eta(d)$ from the statement of this claim, we may rewrite (5.6) as

$$\frac{|\operatorname{Pic}(\mathcal{O}_\Omega)|}{h_{-d}} = 3^{\eta(d)}. \qquad \square$$

Remark 5.12. If the norm map Nr attains the value -1 for an element of $\mathcal{O}_{\Omega}^{\times}$, it does so for a generator of its free part. As m is odd, this implies that $\mathrm{Nr}(\mathcal{O}_{k'}^{\times}) = \mathrm{Nr}(\mathcal{O}_{\Omega}^{\times})$. Recalling that $\underline{N}'_d = \underline{N}_{d,2}$, we conclude by (2.3) and Corollary 5.11 that

$$\frac{|H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}'_{-d})|}{|H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_{-d})|} = \frac{|\operatorname{Pic}\mathbb{Z}[\sqrt{-d}]|}{h_{-d}} = 3^{\eta(d)}. \tag{5.7}$$

Example 5.13. We tabulate the following data from [7]: see p. 19 for the second and fourth columns and p. 20 for the third, noting that, as the forms obtained are definite, the number of total classes is twice the number of positive classes by Proposition 5.21 below.

$0 < d \equiv 3\,(\mathrm{mod} 4)$	h_{-d}	$\lvert H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}'_{-d})\rvert$	$\lvert H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_{-d})\rvert$	$c_{-d,1} = \frac{1+d}{4}$
3	1	2	2	1
7	1	2	2	2
11	1	6	2	3
15	2	4	4	4
19	1	6	2	5
23	3	6	6	6

Example 5.14. Let $d = -5$. Then $(\overline{\mathcal{O}}_{k'})^{\times}_{(2)}/\overline{\mathcal{O}}^{\times}_{(2)} \cong \mathbb{Z}/3$ by the argument preceding (5.6). A generator of the free part of $\mathcal{O}_{k'}^{\times}$ is $\varepsilon = \omega = \frac{1+\sqrt{5}}{2}$. Let $\Omega = \{1, \sqrt{5}\}$. The embedding $\varphi : \mathcal{O}_{\Omega} \to \mathcal{O}_{k'}$ induces the embedding of $\underline{N}_{\Omega}(\mathbb{Z})$ in $\underline{N}_5(\mathbb{Z})$ given by the integral matrix realization of (4.4), namely the group homomorphism

$$\varphi : \begin{pmatrix} x & 5y \\ y & x \end{pmatrix} \mapsto \begin{pmatrix} x-y & 2y \\ 2y & x+y \end{pmatrix}.$$

Since $\mathrm{Nr}(\varepsilon) = -1$, a generator of the free part of $\underline{N}_5(\mathbb{Z})$ is $u = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right)$, corresponding to $\varepsilon^2 = 1 + \omega$, while a generator of $\underline{N}'_5(\mathbb{Z})$ is $z = \left(\begin{smallmatrix} 9 & 20 \\ 4 & 9 \end{smallmatrix}\right)$, corresponding to $\varepsilon^6 = 9 + 4\sqrt{5}$. Hence

$$\varphi(z) = \begin{pmatrix} 5 & 8 \\ 8 & 13 \end{pmatrix} = u^3,$$

so that $|\mathrm{coker}(\varphi)| = 3$. This means that $\eta(d) = 0$ in Proposition 5.11, and $|\mathrm{Pic}(\mathbb{Z}[\sqrt{5}])| = h_5$.

Recall from (1.1) that the set $\mathfrak{cl}^+(n)$ classifies quadratic forms of discriminant n up to proper isometry. The next lemma relates $\mathfrak{cl}^+(n)$ to the flat cohomology of special orthogonal groups.

Lemma 5.15. *Let d be any integer that is not a perfect square and not of the form $d = -3 \cdot 4^m$ for any $m \in \mathbb{N}_0$, and set $q(x, y) = x^2 - dy^2$. Then $\mathfrak{cl}^+(4d) = H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q^+)$.*

Proof. Note that $\Delta(q) = 4d$ need not be a fundamental discriminant. The equivalence relations in $\mathfrak{cl}^+(4d)$ and in $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q^+)$ are defined similarly, so we only need to show that the two sets of representatives coincide. Indeed, those in $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q^+)$ are obtained by (local) proper isometries of q, resulting in the same discriminant $\Delta(q)$. Conversely, we claim that any quadratic $\mathbb{Z}$-form q' of rank 2 with $\Delta(q') = \Delta(q)$ is diagonalizable over $\mathbb{Z}_p$ for any prime p, thus is isomorphic to q in the fppf topology. This is true for all odd primes p by [9, Thm. 8.3.1]. If $p = 2$, then by the explicit form of the Jordan Decomposition Theorem [9, Lem. 8.4.1] q' is isomorphic over $\mathbb{Z}_2$ to a direct product of forms of rank at most 2, where the possible components of rank 2 are of the form $2^e xy$ or $2^e(x^2 + xy + y^2)$ for $e \in \mathbb{N}_0$; note that [9] uses the classical definition of integral forms, requiring that b be even. None of these has discriminant $4d$ for an integer d satisfying our hypotheses. Hence q' is diagonalizable over $\mathbb{Z}_2$. Moreover, by Lemma 5.6 a local isometry between q and q' can be taken to be proper, as they share the same discriminant. So any $\mathbb{Z}$-form with discriminant $\Delta(q)$ is properly isomorphic to q in the flat topology. This completes the proof. □

Remark 5.16. We justify the exclusion of discriminants of the form $-3 \cdot 4^m$, for $m \geq 1$, in the hypotheses of Lemma 5.15 by noting that the lemma is false in those cases. Indeed, the form $(2^m, 2^{m-1}, 2^m)$ has discriminant $-3 \cdot 4^m$, but one readily checks that it is not isometric to $(1, 0, 3 \cdot 4^{m-1})$ over any finite flat extension of $\mathbb{Z}_2$. Thus the class $[(2^m, 2^{m-1}, 2^m)]$ appears in $\mathfrak{cl}^+(-3 \cdot 4^m)$ but not in $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}^+_{(1,0,3\cdot 4^{m-1})})$. Indeed, $\operatorname{Pic} \mathbb{Z}[\sqrt{-3}]$ is trivial; see, for instance, [15, Exercise 7.9]. It follows from (2.3) and Lemma 4.5 that $|H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}^+_{(1,0,3)})| = 2$; alternatively, see the data of Example 5.13. Thus $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}^+_{(1,0,3)}) = \{[\pm(1, 0, 3)]\}$.

5.5. Applications to the classification of binary quadratic forms.

Having studied Cases (I) and (II) separately, we gather together our results. First we determine the structure of $\mathfrak{cl}(D)$ for many integers D.

Proposition 5.17. *Let $D \neq -3$ be an integer such that $D \equiv 1 \bmod 4$ and D is not a perfect square. Set $q(x, y) = x^2 + xy + ((1 - D)/4)y^2$. Then $\mathfrak{cl}(D) = \mathfrak{cl}^+(D) = H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q^+)$.*

Proof. The same argument as in the proof of Lemma 5.15 shows that $\mathfrak{cl}^+(D) = H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q^+)$. Write $D = dm^2$, where $d \equiv 1 \bmod 4$ is square-free and m is odd. Then $q = q_{d,m}$. Moreover, by Lemma 4.5 and Proposition 5.5 we have $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q^+) = H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_{d,m}) = H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_{d,m})$. Thus any quadratic form that is improperly isomorphic to q is also properly isomorphic to q, hence $\mathfrak{cl}(D) = \mathfrak{cl}^+(D)$. □

Proposition 5.18. *Let D be any integer that is not a perfect square and not of the form $D = -3 \cdot 4^\ell$ for any $\ell \in \mathbb{N}_0$. Set $q(x, y) = x^2 - Dy^2$. Then $\mathfrak{cl}(4D) = H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q^+)/\underline{\mu}_2(\mathbb{Z})$, where the non-trivial element of $\underline{\mu}_2(\mathbb{Z})$ maps $[(a, b, c)]$ to $[(a, -b, c)]$.*

Proof. We have $\mathfrak{cl}^+(4D) = H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q^+)$ by Lemma 5.15. The description of the structure of $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_q)$ provided by Lemma 5.6 shows that the only proper isomorphism classes of forms *of discriminant* $4D$ that are improperly isomorphic to each other are those in the same orbit of the $\underline{\mu}_2(\mathbb{Z})$-action. □

Recall that $k = \mathbb{Q}(\sqrt{d})$. As noted in the introduction, Gauss proved in his *Disquisitiones Arithmeticae* [18] that the elements of $\mathfrak{cl}^+(\Delta(q_d))$, namely proper isomorphism classes of forms of discriminant Δ_k, are parametrized by $\mathrm{Pic}^+(\mathcal{O}_k)$. See, for instance, [17, Thm. 58] for an exposition of this result.

If $d < 0$, Gauss' classification of forms of discriminant $\Delta_{\mathbb{Q}(\sqrt{d})}$ treats only the positive definite forms, namely those for which $a, c > 0$. The following claim completes the proper classification.

Theorem 5.19. *If $d \notin \{0, 1\}$ is a square-free integer, then*

$$\mathfrak{cl}^+(\Delta(q_d)) = H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_d^+) \cong \{\pm 1\}^{\mu(d)} \times \mathrm{Pic}^+(\mathcal{O}_k), \ \text{where } \mu(d) = \begin{cases} 1 & d < 0 \\ 0 & d > 0. \end{cases}$$

Proof. By Lemma 4.5 we have $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_d) = H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_d^+)$, and the latter properly classifies the integral quadratic forms that are isomorphic to q_d for the flat topology, thus of discriminant Δ_k. So if $d > 0$, then $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_d)$ injects into $\mathfrak{cl}^+(\Delta_k) = \mathfrak{cl}^+(\Delta(q_d))$, which is in bijection with $\mathrm{Pic}^+(\mathcal{O}_k)$ by the classical theorem of Gauss mentioned above. Since $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_d)$ and $\mathrm{Pic}^+(\mathcal{O}_k)$ have the same cardinality by (2.8), we have obtained a natural bijection between them.

If $d < 0$, however, then $\mathrm{Pic}^+(\mathcal{O}_k)$ classifies only the positive definite forms; see the proof of [17, Thm. 58]. The subset $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_d)^+$ of classes of positive forms injects into $\mathrm{Pic}^+(\mathcal{O}_k) = \mathrm{Pic}\,\mathcal{O}_k$ as above. If $[q] \in H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_d)$, then the isometry $\mathrm{diag}(\sqrt{-1}, \sqrt{-1})$ shows that $[-q]$ belongs to $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_d)$. Thus if $d \equiv 1 \pmod 4$, then $[-q] \in H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_d)$ by Proposition 5.5. This remains true also in the case $d \equiv 2, 3 \pmod 4$ by the decomposition of Lemma 5.6, since $\mathrm{disc}(-q) = \Delta_k$. Furthermore, since q realizes only non-negative values and $-q$ realizes non-positive values, the two forms q and $-q$ cannot be $\mathbb{Z}$-equivalent. Since every definite form is positive or negative, we have $\{\pm 1\} \times H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_d)^+ = H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_d)$, and we have just shown that this injects into $\{\pm 1\} \times \mathrm{Pic}^+(\mathcal{O}_k) = \mathfrak{cl}^+(\Delta(q_d))$. Again by (2.8), these sets have the same cardinality, so our injection is a bijection. □

Remark 5.20. Let $D \equiv 2, 3 \bmod 4$ be square-free, and consider a form $q = (a, b, c)$ of discriminant $4D$. We show by a simple calculation that the composition of q with its opposite form $(a,-b,c)$ lies in the trivial class of $\mathfrak{cl}^+(4D)$. It suffices, via the bijection of (1.2), to show that the product of the corresponding ideal classes in $\operatorname{Pic}^+(\mathcal{O}_{\mathbb{Q}(\sqrt{D})})$ is principal. The following ideal I is a representative of this product:

$$\begin{aligned} I &= \left(a, \frac{b}{2} - \sqrt{D}\right)\left(a, \frac{b}{2} + \sqrt{D}\right) \\ &= \left(a^2, a\left(\frac{b}{2} + \sqrt{D}\right), a\left(\frac{b}{2} - \sqrt{D}\right), \frac{b^2}{4} - D\right). \end{aligned}$$

Since $4D = \operatorname{disc}(q) = b^2 - 4ac$, we have $\frac{b^2}{4} - D = ac$, which shows that $I \subseteq (a)$. On the other hand, since $4D$ is a fundamental discriminant, it is easy to see that $\gcd(a,b,c) = 1$ (i.e. q is primitive). This implies that a is an integral linear combination of $a^2, ab, ac \in I$. It follows that $(a) \subseteq I$, and hence $I = (a)$ is principal. Thus opposite forms represent inverse classes in $\operatorname{Pic}^+(\mathcal{O}_{\mathbb{Q}(\sqrt{D})})$. By Lemma 5.15, Proposition 5.18, and Theorem 5.19 we conclude that

$$\mathfrak{cl}(4D) \cong \{\pm 1\}^{\mu(D)} \times \operatorname{Pic}^+(\mathcal{O}_{\mathbb{Q}(\sqrt{D})})/(x \sim x^{-1})$$

and we deduce that $\mathfrak{cl}(4D)$ inherits an abelian group structure from $\operatorname{Pic}^+(\mathcal{O}_{\mathbb{Q}(\sqrt{D})})$ if and only if $\exp(\operatorname{Pic}^+(\mathcal{O}_{\mathbb{Q}(\sqrt{D})})) \leq 2$.

The following statement generalizes the result of Gauss mentioned above to cases in which $4d$ is not a fundamental discriminant, and, when $d < 0$, to forms that need not be positive definite. It is also classical; see, for instance, [15, Exercise 7.23]. We prove it by modern methods, at the price of ruling out discriminants of the form $-3 \cdot 4^\ell$. The theorem remains true in this case, but Remark 5.16 shows that our cohomological argument must be modified in order to treat it. If D is an integer that is not a perfect square, then define

$$\tilde{\varepsilon}(D) = \begin{cases} 0 & D > 0 \text{ and } \operatorname{Nr}(\mathbb{Z}[\sqrt{D}]^\times) = \{\pm 1\} \\ 1 & \text{otherwise.} \end{cases} \tag{5.8}$$

Theorem 5.21. *For any integer D that is not a perfect square and not of the form $D = -3 \cdot 4^\ell$ for any $\ell \in \mathbb{N}_0$, there is a bijection*

$$\mathfrak{cl}^+(4D) \cong \{\pm 1\}^{\tilde{\varepsilon}(D)} \times \operatorname{Pic}(\mathbb{Z}[\sqrt{D}]).$$

Moreover, if $d \notin \{0, 1, -3\}$ is square-free, then

$$\mathfrak{cl}^+(4d) \cong \{\pm 1\}^{\varepsilon(d)} \times \operatorname{Pic}(\mathbb{Z}[\sqrt{d}]).$$

Proof. Since D is not a perfect square, it may be written uniquely in the form $D = d(m')^2$, where $d \neq 0, 1$ is square-free and $m' \in \mathbb{N}$. Set $m = 2m'$

if $d \equiv 1 \bmod 4$ and $m = m'$ otherwise. Observe that $\mathbb{Z}[\sqrt{D}] = \mathcal{O}_{d,m}$ and $q_{d,m} = (1, 0, -D)$. Consider the exact sequence (2.3) for the basis $\Omega_{d,m}$:

$$1 \to \{\pm 1\} / \operatorname{Nr}(\mathcal{O}_{d,m}^{\times}) \to H^1_{\text{fl}}(\mathbb{Z}, \underline{N}_{d,m}) \to \operatorname{Pic} \mathbb{Z}[\sqrt{D}] \to 1.$$

The group $H^1_{\text{fl}}(\mathbb{Z}, \underline{N}_{d,m})$ is equal to $H^1_{\text{fl}}(\mathbb{Z}, \mathrm{O}^+_{d,m})$ by Lemma 4.5, and hence is identified with $\mathfrak{cl}^+(4D)$ by Lemma 5.15. The first part of our claim is immediate. For the second part, there is nothing further to prove if $d \equiv 2, 3 \bmod 4$; in this case, $\varepsilon(d) = \tilde{\varepsilon}(d)$ by definition. If $d \equiv 1 \bmod 4$ is square-free, then we observed in Remark 5.12 that $\operatorname{Nr}(\mathbb{Z}[\sqrt{D}]^{\times}) = \operatorname{Nr}(\mathcal{O}_d^{\times})$, so again $\varepsilon(d) = \tilde{\varepsilon}(d)$. This concludes the proof. □

Proposition 5.22. *For a square-free integer $d \notin \{0, 1\}$ let m_d be the number of pairs $[(a, \pm b, c)]$ which are distinct in $\mathfrak{cl}^+(\Delta(q_d))$, and let l_d be the number of such pairs in $\mathfrak{cl}^+(-\Delta(q_d))$. Let h_d^+ be the narrow class number of $\mathbb{Q}(\sqrt{d})$. Then*

$$|H^1_{\text{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_d)| = \begin{cases} 2^{\mu(d)} h_d^+ & d \equiv 1 \pmod 4 \\ 2^{\mu(d)} h_d^+ + 2^{\mu(-d)} h_{-d}^+ - m_d - l_d & d \equiv 2 \pmod 4 \\ 2^{\mu(d)} h_d^+ + 2^{\mu(-d)} \cdot 3^{\eta(d)} h_{-d}^+ - m_d - l_d & d \equiv 3 \pmod 4. \end{cases}$$

Proof. If $d \equiv 1 \pmod 4$ then $|H^1_{\text{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_d)| = |H^1_{\text{fl}}(\mathbb{Z}, \underline{N}_d)| = h_d^+ \cdot 2^{\mu(d)}$, where the first equality is Proposition 5.5 and the second comes from (2.8). Otherwise, use Lemma 5.6 and notice that if $d \equiv 2 \pmod 4$, then $-d \equiv 2 \pmod 4$ as well, so $\underline{N}'_{-d} = \underline{N}_{-d}$. On the other hand, if $d \equiv 3 \pmod 4$, then $-d \equiv 1 \pmod 4$, and the claim follows. □

Remark 5.23. Let $d \equiv 2 \bmod 4$ be square-free. Then $|H^1_{\text{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_d)| = |H^1_{\text{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_{-d})|$ by Lemma 5.6. However, we see from Proposition 5.22 that this observation does not readily imply any relation between the class numbers h_d and h_{-d}. Indeed, the class numbers of real and imaginary quadratic fields behave very differently. For instance, it is well known that only nine imaginary quadratic fields have class number one, but the Cohen–Lenstra heuristics [11] suggest that this should be true of infinitely many real quadratic fields.

5.6. On the principal genus theorem. Theorem 5.19 also implies another classical result of Gauss: the principal genus theorem. Recall that $k = \mathbb{Q}(\sqrt{d})$, with $d \notin \{0, 1\}$ square-free. Then for any binary quadratic form of discriminant Δ_k, the composition of q with itself belongs to the principal genus, namely the genus of the norm form q_d. Under the identification of Lemma 5.15, composition of quadratic forms corresponds to multiplication in the abelian group $H^1_{\text{fl}}(\mathbb{Z}, \underline{\mathrm{O}}_d^+)$; we refer the reader to the discussion in [26, §V.7.3] for details.

Corollary 5.24. *Let $d \notin \{0,1\}$ be square-free and $m \geq 0$. Suppose that $H^1_{\mathrm{fl}}(\mathbb{Z}_p, (\underline{\mathrm{O}}^+_{d,m})_p)$ embeds in $H^1(\mathbb{Q}_p, (\mathrm{O}^+_{d,m})_p)$ for any prime p. For any class $[q] \in H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{\mathrm{O}}^+_{d,m})$, the class $[q \otimes q]$ belongs to the principal genus.*

Proof. To alleviate the notation, we write $\underline{N}$ for $\underline{N}_{d,m}$. Since $H^1_{\mathrm{fl}}(\mathbb{Z}_p, \underline{N}_p)$ injects into $H^1(\mathbb{Q}_p, N_p)$ for any p by assumption, by (3.2) and Lemma 4.5 we obtain

$$\mathrm{Cl}_\infty(\underline{\mathrm{O}}^+_{d,m}) = \mathrm{Cl}_\infty(\underline{N}) = \ker[H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}) \to H^1(\mathbb{Q}, N)],$$

showing that $\mathrm{Cl}_\infty(\underline{\mathrm{O}}^+_{d,m})$ is the principal genus of q. Moreover, the quotient $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N})/\,\mathrm{Cl}_\infty(\underline{N}) = \text{Ш}^1_{S_r \cup \{\infty\}}(\mathbb{Q}, N)$ has exponent 2 by Proposition 3.3 and Remark 3.4 whose hypotheses are satisfied thanks to our assumptions. Recall that $\underline{N}$ is commutative, so that $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N})$ is an abelian group. Thus for any class $[q] \in H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_d)$, the class of the tensor product $q \otimes q$ lies in $\mathrm{Cl}_\infty(\underline{N}) = \mathrm{Cl}_\infty(\underline{\mathrm{O}}^+_{d,m})$. □

Example 5.25. The hypotheses of Corollary 5.24 were shown to hold for all $\underline{\mathrm{O}}^+_{d,1}$ in (3.4). They also hold in the case of $\underline{\mathrm{O}}^+_{d,2}$ where $d \equiv 1 \pmod 4$, i.e. for the norm form $q_{d,2} = (1, 0, -d)$ corresponding to the order $\mathbb{Z}[\sqrt{d}]$. Indeed, if $p \mid d$ then the embedding follows from $q_{d,2}$ being of simple degeneration and multiplicity one (cf. [3, Cor. 3.8]). If $p \nmid d$ and p is odd, it follows from $(\underline{\mathrm{O}}^+_{d,2})_p$ being reductive (see the proof of [10, Prop. 3.14]). If $p = 2$, then $(\underline{\mathrm{O}}^+_{d,2})_p$ is not smooth, yet the embedding holds since all forms in $H^1_{\mathrm{fl}}(\mathbb{Z}_2, (\underline{\mathrm{O}}^+_{d,2})_2)$ are diagonalizable as in the proof of Proposition 5.15. Hence $[q \otimes q] \in \mathrm{Cl}_\infty(\underline{\mathrm{O}}^+_{d,2})$.

Remark 5.26. Proposition 3.3 shows that $\mathrm{Cl}_\infty(\underline{N}_{d,m})$ is embedded as a subgroup of $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_{d,m})$. If $d \neq -3$, then the latter group is a disjoint union of classes of integral quadratic binary forms of discriminant $\Delta(q_{d,m})$ of all genera. This embedding holds for any twisted form of $q_{d,m}$, hence, under the hypotheses of Corollary 5.24, the quotient $H^1_{\mathrm{fl}}(\mathbb{Z}, \underline{N}_{d,m})/\,\mathrm{Cl}_\infty(\underline{N}_{d,m}) \simeq \text{Ш}^1_{S_r \cup \{\infty\}}(\mathbb{Q}, N_{d,m})$ is in bijection with the set of proper genera of $q_{d,m}$. Thus there are $2^{|S_r|-1}$ such proper genera, as was initially proved by Gauss; see also [30, §5, Example 2] and [33, Cor. 16].

Appendix A. Some explicit presentations of group schemes

In this section we will write down equations cutting out the algebraic groups $\widetilde{\underline{\mathrm{O}}}_{d,m}$ and $\underline{\mathrm{O}}^+_{d,m}$ and use them to provide an explicit proof of Proposition 5.1, which describes their quotient.

Lemma A.1. *Let $d \neq 0, 1$ be square-free and $m \in \mathbb{N}$, and define the ideal $\mathcal{I}_{d,m} \subset \mathbb{Z}[\alpha, \beta, \gamma, \delta, t]$ of a polynomial ring in five variables as follows. In*

Case (I)*, set*

$$\mathcal{I}_{d,m} = (\alpha^2 + \alpha\beta + c_{d,m}\beta^2 - 1, 2\alpha\gamma + \alpha\delta + \beta\gamma + 2c_{d,m}\beta\delta - 1,$$
$$\gamma^2 + \gamma\delta + c_{d,m}\delta^2 - c_{d,m}, (\alpha\delta - \beta\gamma)t - 1, u^2 - u),$$

where $c_{d,m}$ *was defined in* (4.1) *and* $u = 1 - \alpha\gamma - \beta\gamma - c_{d,m}\beta\delta$*.*

In Case (II)*, define* $\mathcal{I}_{d,m} = (\alpha^2 - c_{d,m}\beta^2 - 1, \alpha\gamma - c_{d,m}\beta\delta, \gamma^2 - c_{d,m}\delta^2 + c_{d,m}, (\alpha\delta - \beta\gamma)t - 1, t^2 - 1)$.

Then $\widetilde{\underline{\mathrm{O}}}_{d,m} = \operatorname{Spec}\mathbb{Z}[\alpha, \beta, \gamma, \delta, t]/\mathcal{I}_{d,m}$*.*

Proof. We first treat Case (II), in which $q_{d,m}(x, y) = x^2 - cy^2$; we write c for $c_{d,m}$ for brevity. Consider the matrix

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

The identity $q_{d,m} \circ A = q_{d,m}$ amounts to

$$q_{d,m} = (\alpha x+\gamma y)^2-c(\beta x+\delta y)^2 = (\alpha^2-c\beta^2)x^2+(2\alpha\gamma-2c\beta\delta)xy+(\gamma^2-c\delta^2)y^2.$$

Equating the coefficients of x^2, xy, and y^2, and noting that A must be invertible, we obtain

$$\underline{\mathrm{O}}_{d,m} = \operatorname{Spec}\mathbb{Z}[\alpha, \beta, \gamma, \delta, t]/(\alpha^2-c\beta^2-1, \alpha\gamma-c\beta\delta, \gamma^2-c\delta^2+c, (\alpha\delta-\beta\gamma)t-1).$$

Observe that the identity $c((\alpha\delta-\beta\gamma)^2-1) = 0$ is satisfied in $\underline{\mathrm{O}}_{d,m}$. This can be seen by taking determinants in the matrix equation $AB_{q_{d,m}}A^t = B_{q_{d,m}}$ corresponding to the condition $q_{d,m} \circ A = q_{d,m}$; alternatively, we leave it as an exercise for the reader to deduce this identity from the equations cutting out $\underline{\mathrm{O}}_{d,m}$. Therefore, $(\alpha\delta - \beta\gamma)^2 - 1 = 0$ (or, equivalently, $t^2 - 1 = 0$), in $\widetilde{\underline{\mathrm{O}}}_{d,m}$. One now checks explicitly that the ring $\mathbb{Z}[\alpha, \beta, \gamma, \delta, t]/(\alpha^2 - c\beta^2 - 1, \alpha\gamma - c\beta\delta, \gamma^2 - c\delta^2 + c, (\alpha\delta - \beta\gamma)t - 1, t^2 - 1)$ is torsion-free, and this implies the claim in Case (II).

Now suppose that we are in Case (I), i.e. that $d \equiv 1 \bmod 4$ and m is odd. Then $q_{d,m} = x^2 + xy + cy^2$. In this case, the condition $q_{d,m} \circ A = q_{d,m}$ gives

$$q_{d,m} = (\alpha x + \gamma y)^2 + (\alpha x + \gamma y)(\beta x + \delta y) + c(\beta x + \delta y)^2$$
$$= (\alpha^2 + \alpha\beta + c\beta^2)x^2 + (2\alpha\gamma + \alpha\delta + \beta\gamma + 2c\beta\delta)xy + (\gamma^2 + \gamma\delta + c\delta^2)y^2.$$

Hence we obtain

$$\underline{\mathrm{O}}_{d,m} = \operatorname{Spec}\mathbb{Z}[\alpha, \beta, \gamma, \delta, t]/(\alpha^2 + \alpha\beta + c\beta^2 - 1,$$
$$2\alpha\gamma + \alpha\delta + \beta\gamma + 2c\beta\delta - 1, \gamma^2 + \gamma\delta + c\delta^2 - c, (\alpha\delta - \beta\gamma)t - 1).$$

By similar considerations to the previous case, the identity $c((\alpha\delta - \beta\gamma)^2 - 1) = 0$ holds in $\underline{\mathrm{O}}_{d,m}$. Set $u = 1 - \alpha\gamma - \beta\gamma - c\beta\delta$. Then one of the equations cutting out $\underline{\mathrm{O}}_{d,m}$ may be written as $2u = \alpha\delta-\beta\gamma+1$. Hence $c((2u-1)^2-1) =$

$4c(u^2 - u) = 0$ in $\underline{\mathrm{O}}_{d,m}$, and thus $u^2 - u = 0$ in $\underline{\widetilde{\mathrm{O}}}_{d,m}$. Since the ring $\mathbb{Z}[\alpha, \beta, \gamma, \delta, t]/\mathcal{I}_{d,m}$ is torsion-free, the claim follows. □

Corollary A.2. *Let $d \neq 0, 1$ be square-free and $m \in \mathbb{N}$. Maintaining the notation of Lemma A.1, we have*

$$\underline{\mathrm{O}}^{+}_{d,m} = \begin{cases} \operatorname{Spec} \mathbb{Z}[\alpha, \beta, \gamma, \delta, t]/(\mathcal{I}_d, u - 1) & : \text{Case (I)} \\ \operatorname{Spec} \mathbb{Z}[\alpha, \beta, \gamma, \delta, t]/(\mathcal{I}_d, t - 1) & : \text{Case (II)}. \end{cases}$$

Proof. In all cases, the identity $t = 1$ is immediate from the definition of $\underline{\mathrm{O}}^{+}_{d,m}$. In Case (I), this implies that the identity $2u - 1 = 1$ holds in $\underline{\mathrm{O}}^{+}_{d,m}$, and hence so does $u = 1$. We leave the verification that these rings are torsion-free to the reader. □

Remark A.3. It is an instructive exercise to verify Lemma 4.5 for the bases $\Omega_{d,m}$ by showing that the map $x \mapsto \alpha, y \mapsto \beta$ is an explicit isomorphism of commutative rings between the coordinate ring of $\underline{N}_{d,m}$ and that of $\underline{\mathrm{O}}^{+}_{d,m}$.

With the previous results in hand, we can give an explicit proof of Proposition 5.1.

Proposition. *Let $d \neq 0, 1$ be square-free and $m \in \mathbb{N}$. Then*

$$\underline{\widetilde{\mathrm{O}}}_{d,m}/\underline{\mathrm{O}}^{+}_{d,m} \simeq \begin{cases} \underline{\mathbb{Z}/2} & : \text{Case (I)} \\ \underline{\mu}_2 & : \text{Case (II)}. \end{cases}$$

Proof. The claim follows straightforwardly from the explicit presentations obtained in Lemma A.1 and Corollary A.2. In the course of the proofs of those statements, we showed that the relation $(\alpha\delta - \beta\gamma)^2 - 1 = 0$ always holds in $\underline{\widetilde{\mathrm{O}}}_{d,m}$. Hence the determinant induces a map $\det : \underline{\widetilde{\mathrm{O}}}_{d,m} \to \underline{\mu_2}$ corresponding to the ring homomorphism $\mathbb{Z}[t]/(t^2 - 1) \to \mathbb{Z}[\alpha, \beta, \gamma, \delta, t]/\mathcal{I}_{d,m}$ sending t to $\alpha\delta - \beta\gamma$.

Now suppose we are in Case (II). If R is a $\mathbb{Z}$-algebra, then the sequence of groups

$$1 \to \underline{\mathrm{O}}^{+}_{d,m}(R) \to \underline{\widetilde{\mathrm{O}}}_{d,m}(R) \overset{\det}{\to} \underline{\mu}_2(R) \to 1$$

is exact. Indeed, the only part of this statement not immediate from Lemma A.1 is the surjectivity of the determinant, obtained by observing that if $x \in \underline{\mu}_2(R)$, then $\operatorname{diag}(x, 1) \in \underline{\widetilde{\mathrm{O}}}_{d,m}(R)$.

In Case (I), on the other hand, the determinant need not be surjective. To see this, recall from the proof of Lemma A.1 that if $A \in \underline{\widetilde{\mathrm{O}}}_{d,m}(R)$, then $\det A = 2u - 1$ for $u = 1 - \alpha\gamma - \beta\gamma - c_{d,m}\beta\delta \in R$, following our usual notation for matrix elements. Now consider the $\mathbb{Z}$-algebra $R = \mathbb{Z}[t]/(t^2 - 1)$; it is, in fact, faithfully flat over $\mathbb{Z}$ of finite presentation. Observe that $t \in \underline{\mu}_2(R)$, but there is no $u \in R$ such that $2u - 1 = t$. Thus the determinant map $\underline{\widetilde{\mathrm{O}}}_{d,m}(R) \to \underline{\mu}_2(R)$ is not surjective.

Instead, consider the map $D : \widetilde{\underline{\mathrm{O}}}_{d,m} \to \underline{\mathbb{Z}/2}$ corresponding to the ring homomorphism $\mathbb{Z}[t]/(t^2 - t) \to \mathbb{Z}[\alpha, \beta, \gamma, \delta, t]/\mathcal{I}_{d,m}$ sending t to $1 - \alpha\gamma - \beta\gamma - c_{d,m}\beta\delta$. This notation reflects that D is the Dickson morphism $D_{q_{d,m}}$; cf. [13, (C.2.2)]. We claim that

$$1 \to \underline{\mathrm{O}}^+_{d,m}(R) \to \widetilde{\underline{\mathrm{O}}}_{d,m}(R) \overset{D}{\to} \underline{\mathbb{Z}/2}(R) \to 1$$

is an exact sequence of groups for any $\mathbb{Z}$-algebra R. Indeed, if $x \in \underline{\mathbb{Z}/2}(R)$, then

$$A_x = \begin{pmatrix} 1 & 0 \\ 1 - x & 2x - 1 \end{pmatrix} \in \widetilde{\underline{\mathrm{O}}}_{d,m}(R)$$

satisfies $D(A_x) = x$, so ψ is surjective. It follows from Corollary A.2 that $\ker D = \underline{\mathrm{O}}^+_{d,m}(R)$. □

References

[1] S. Anantharaman, "Schémas en groupes, espaces homogènes et espaces algébriques sur une base de dimension 1", *Bull. Soc. Math. Fr.* **33** (1973), p. 5-79.

[2] M. Artin, A. Grothendieck & J.-L. Verdier (eds.), *Théorie des Topos et Cohomologie Étale des Schémas (SGA 4)*, Lecture Notes in Mathematics, Springer, 19721973.

[3] A. Auel, R. Parimala & V. Suresh, "Quadric surface bundles over surfaces", *Doc. Math.* **Extra vol.** (2015), p. 31-70.

[4] A. Borel, "Some finiteness properties of adele groups over number fields", *Publ. Math., Inst. Hautes Étud. Sci.* **16** (1963), p. 5-30.

[5] S. Bosch, W. Lütkebohmert & M. Raynaud, *Néron Models*, Springer, 1990.

[6] N. Bourbaki, *Éléments de mathématique, Algèbre commutative*, Hermann, 1972.

[7] D. A. Buell, *Binary Quadratic Forms, Classical Theory and Modern Computations*, Springer, 1989.

[8] B. Calmès & J. Fasel, "Groupes Classiques", in *Autour des schémas en groupes. Vol. II*, Panoramas et Synthèses, vol. 46, Société Mathématique de France, 2015, p. 1-133.

[9] J. W. S. Cassels, *Rational Quadratic Forms*, London Mathematical Society Monographs, vol. 13, Academic Press Inc., 1978.

[10] V. Chernousov, P. Gille & A. Pianzola, "A classification of torsors over Laurent polynomial rings", *Comment. Math. Helv.* **92** (2017), no. 1, p. 37-55.

[11] H. Cohen & H. W. Lenstra, "Heuristics on class groups of number fields", in *Number theory (Noordwijkerhout 1983)*, Lecture Notes in Mathematics, vol. 1068, Springer, 1983, p. 33-62.

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

[13] ———, "Reductive group schemes", in *Autour des schémas en groupes. Vol. I*, Panoramas et Synthèses, vol. 42-43, Société Mathématique de France, 2014, p. 93-444.

[14] ———, "Non-split reductive groups over $\mathbb{Z}$", in *Autour des schémas en groupes. Vol. II*, Panoramas et Synthèses, vol. 46, Société Mathématique de France, 2015, p. 193-253.

[15] D. A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory, and complex multiplication*, Pure and Applied Mathematics, John Wiley & Sons, 2013.

[16] M. Demazure & A. Grothendieck (eds.), *Séminaire de géométrie algébrique du Bois Marie 1962–64. Schémas en groupes (SGA 3). Tome I: Propriétés générales des schémas en groupes*, 2nd ed., Documents Mathématiques, vol. 7, Société Mathématique de France, 2011.

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

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

[19] P. Gille, “Sur la classification des schémas en groupes semi-simples”, in *Autour des schémas en groupes. Vol. III*, Panoramas et Synthèses, vol. 47, Société Mathématique de France, 2015, p. 39-110.

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

[21] J. Giraud, *Cohomologie non abélienne*, Grundlehren der Mathematischen Wissenschaften, vol. 179, Springer, 1971.

[22] A. Grothendieck, “Éléments de géométrie algébrique: I. Le langage des schémas”, *Publ. Math., Inst. Hautes Étud. Sci.* **4** (1960), p. 5-228.

[23] ———, “Éléments de géométrie algébrique : IV. Étude locale des schémas et des morphismes de schémas, Seconde partie”, *Publ. Math., Inst. Hautes Étud. Sci.* **24** (1965), p. 5-231, rédigés avec la collaboration de J. Dieudonné.

[24] M. Hazewinkel, “Local class field theory is easy”, *Adv. Math.* **18** (1975), p. 148-181.

[25] J. Klüners & S. Pauli, “Computing residue class rings and Picard groups of orders”, *J. Algebra* **292** (2005), no. 1, p. 47-64.

[26] M.-A. Knus, *Quadratic and Hermitian Forms over Rings*, Grundlehren der Mathematischen Wissenschaften, vol. 294, Springer, 1991.

[27] H. Matsumura, *Commutative Ring Theory*, Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, 1989.

[28] M. Morishita, “On S-class number relations of algebraic tori in Galois extensions of global fields”, *Nagoya Math. J.* **124** (1991), p. 133-144.

[29] Y. Nisnevich, “Étale Cohomology and Arithmetic of Semisimple Groups”, PhD Thesis, Harvard University (USA), 1982.

[30] T. Ono, “On some class number relations for Galois extensions”, *Nagoya Math. J.* **107** (1987), p. 121-133.

[31] A. N. Skorobogatov, *Torsors and Rational Points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, 2001.

[32] J. Tate & F. Oort, “Group schemes of prime order”, *Ann. Sci. Éc. Norm. Supér.* **3** (1970), p. 1-21.

[33] W. C. Waterhouse, “Composition of norm-type forms”, *J. Reine Angew. Math.* **353** (1984), p. 85-97.

Rony A. Bitan
Afeka, Tel Aviv Academic College of Engineering
Tel Aviv 6910717, Israel
E-mail: `ronyb@afeka.ac.il`

Michael M. Schein
Department of Mathematics
Bar-Ilan University
Ramat Gan 5290002, Israel
E-mail: `mschein@math.biu.ac.il`