Quadratic forms as fppf-torsors

The, Jorre

Jorre Thé

Quadratic forms as fppf-torsors

Supervisor: prof. dr. J.B. Vonk

August 7, 2025

Master thesis, Mathematisch Instituut, Leiden University

Contents

1 Introduction

One of the most remarkable achievements in Gauss's 1801 *Disquisitiones Arithmeticae* [Gau1801] was his theory of binary quadratic forms

$$Q(x, y) = ax^2 + bxy + cy^2 \tag{1.1}$$

with integer coefficients[1]. Historically, the study of these forms and which integers they represent was central to number theory. Early examples include Fermat's theorem on the sum of two squares and subsequent work on primes of the form $x^2 + ny^2$ [Cox89, §1.2]. It became clear that a general theory was needed to settle many open problems at the time. This led Gauss to develop his theory of equivalence and composition of quadratic forms.

The primary goal of this thesis is to reframe the work of Gauss in the context of algebraic geometry. More specifically, we detail a correspondence between integral binary quadratic forms of discriminant Δ and the fppf-torsors of a certain group scheme R^1_Δ over $\mathrm{Spec}(\mathbb{Z})$. Gauss composition then arises naturally as the group law on its first cohomology group. This geometric viewpoint suggests a generalization, replacing R^1_Δ by the norm 1 group scheme $R^1_{Y/X}(\mathbb{G}_{m,Y})$ associated to a finite locally free morphism of schemes $Y \to X$. We interpret its first cohomology group as a certain *norm class group*, recovering the narrow class group when $Y \to X = \operatorname{Spec} \mathbb{Z}$ is a quadratic extension. For a quadratic extension of a global field of class number one, we determine the 4-torsion of this norm class group using a spectral sequence.

1.1 The work of Gauss

The form (1.1) is *primitive* when $\gcd(a, b, c) = 1$ and its *discriminant* is b^2-4ac. Denote by $\mathcal{F}_\Delta$ the set of primitive integral binary quadratic forms of discriminant Δ. Gauss defined forms $Q_1, Q_2 \in \mathcal{F}_\Delta$ to be *equivalent* when there exist integers $p, q, r, s \in \mathbb{Z}$ satisfying

$$Q_1(x, y) = Q_2(px + qy, rx + sy) \quad \text{and} \quad ps - qr = 1.$$

That is, the equivalence classes are exactly the orbits of $\mathcal{F}_\Delta$ under the natural right action of $\mathrm{SL}_2(\mathbb{Z})$. Next, Gauss introduced the following composition law.

Definition 1.1. For $Q_1, Q_2 \in \mathcal{F}_\Delta$, a form $Q_3 \in \mathcal{F}_\Delta$ is called their *composition* if there exist bilinear forms

$$B_i(x, y, z, w) = a_i xz + b_i xw + c_i yz + d_i yw \in \mathbb{Z}[x, y, z, w] \quad \text{for} \quad i = 1, 2$$

satisfying

$$Q_1(x, y)Q_2(z, w) = Q_3(B_1(x, y, z, w), B_2(x, y, z, w)) \tag{1.2}$$

and[2]

$$a_1b_2 - a_2b_1 = Q_1(1, 0) \qquad \text{and} \qquad a_1c_2 - a_2c_1 = Q_2(1, 0). \tag{1.3}$$

One example of this stems from antiquity: Brahmagupta's identity

$$(x^2 - ny^2)(z^2 - nw^2) = (xz + nyw)^2 - n(xw + yz)^2$$

shows that $x^2 - ny^2$ is a composition of itself with itself. A form $Q_0 \in \mathcal{F}_\Delta$ with this property exists for every discriminant Δ. Gauss proved the following theorem.

[1] Actually, Gauss only considered forms whose second coefficient b was even, but nowadays we prefer not to make this restriction.

[2] Given (1.2), one always has $a_1b_2 - a_2b_1 = \pm Q_1(1, 0)$ and $a_1c_2 - a_2c_1 = \pm Q_2(1, 0)$, see Lemma 2.2.

Theorem 1.2 (Gauss)**.** *Let $\Delta \equiv 0, 1 \mod 4$ be a non-zero integer. Gauss composition is a well-defined binary operation on $\mathcal{F}_\Delta/\mathrm{SL}_2(\mathbb{Z})$ which makes it into a finite abelian group.*

The class of Q_0 is the identity element of this group. The definition of composition was made more constructive by Dirichlet [Dir1894, §146], though it long retained some mystery. A new interpretation was given using Bhargava cubes [Bha04], which also extends to new composition laws, including a composition law on the cubes themselves.

1.2 Interpretation in terms of torsors

Fix a discriminant Δ, i.e. $\Delta \neq 0$ and $\Delta \equiv 0, 1 \mod 4$. For $Q \in \mathcal{F}_\Delta$ we define the scheme

$$T_Q \coloneqq \operatorname{Spec}\left(\frac{\mathbb{Z}[x,y]}{(Q(x,y)-1)}\right).$$

Suppose that $Q_1, Q_2, Q_3 \in \mathcal{F}_\Delta$ and $B_1, B_2 \in \mathbb{Z}[x,y,z,w]$ satisfy Definition 1.1. Then (1.2) implies that we have a ring homomorphism

$$\begin{aligned} \frac{\mathbb{Z}[b_1,b_2]}{(Q_3(b_1,b_2)-1)} &\longrightarrow \frac{\mathbb{Z}[x,y]}{(Q_1(x,y)-1)} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}[z,w]}{(Q_2(z,w)-1)} \\ b_i &\longmapsto B_i(x\otimes 1, y\otimes 1, 1\otimes z, 1\otimes w) \end{aligned}$$

and therefore a morphism of schemes

$$T_{Q_1} \times T_{Q_2} \longrightarrow T_{Q_3}.$$

We will call such a morphism a *Gauss composition*. Together with its canonical section over $\operatorname{Spec}\mathbb{Z}$, such a morphism $T_{Q_0} \times T_{Q_0} \to T_{Q_0}$ makes T_{Q_0} into a group scheme, which we denote by R^1_Δ.

Now, for every $Q \in \mathcal{F}_\Delta$, there is a canonical Gauss composition $T_Q \times R^1_\Delta \to T_Q$. We prove that this makes T_Q into an R^1_Δ-torsor, and that $Q_1, Q_2 \in \mathcal{F}_\Delta$ are $\mathrm{SL}_2(\mathbb{Z})$-equivalent precisely when T_{Q_1} and T_{Q_2} are isomorphic as R^1_Δ-torsors. As the set of isomorphism classes of G-torsors can be identified with $H^1(X_{fppf}, G)$ for a flat finite-type group scheme G over X [Mil80, Prop. III.4.6], this culminates in the following theorem.

Theorem A. *For a discriminant Δ, associating to a form $Q \in \mathcal{F}_\Delta$ the R^1_Δ-torsor T_Q induces an isomorphism*

$$\mathcal{F}_\Delta/\mathrm{SL}_2(\mathbb{Z}) \xrightarrow{\sim} H^1(\operatorname{Spec}\mathbb{Z}_{fppf}, R^1_\Delta).$$

Chapter 2 presents a proof of Theorem A that is independent of the results of Gauss, thereby providing an alternate proof of Theorem 1.2. We will forego explicit computations by relying on algebro-geometric tools like torsors and faithfully flat descent.

1.3 The norm class group

The group scheme R^1_Δ is an instance of the more general construction of the norm 1 group scheme $R^1_{Y/X}(\mathbb{G}_{m,Y})$ associated to any finite locally free morphism of schemes $Y \to X$, defined in §3.1. Even in this generality, there is a concrete interpretation of $H^1(X, R^1_{Y/X}(\mathbb{G}_{m,Y}))$. To an invertible $\mathcal{O}_Y$-module, one can associate an invertible $\mathcal{O}_X$-module $N(\mathcal{L})$, called its *norm* [EGAII, §6.5]. We introduce the *norm class group*, which is the group $\operatorname{NormCl}(Y/X)$ of invertible $\mathcal{O}_Y$-modules $\mathcal{L}$ of trivial norm, together with a choice of isomorphism $N(\mathcal{L}) \xrightarrow{\sim} \mathcal{O}_X$. Chapter 3 will prove the following theorem.

Theorem B. *For a finite locally free morphism $Y \to X$, there is a canonical isomorphism*

$$\mathrm{NormCl}\,(Y/X) \xrightarrow{\sim} H^1(X_{fppf}, R^1_{Y/X}(\mathbb{G}_{m,Y})).$$

The norm class group $\mathrm{NormCl}\,(\mathcal{O}/\mathbb{Z})$ of an order $\mathcal{O}$ in a number field K is closely related to the narrow class group $\mathrm{Cl}^+(\mathcal{O})$. If K has $r \leq 2$ real embeddings, we even have

$$\mathrm{NormCl}(\mathcal{O}/\mathbb{Z}) \cong \begin{cases} \mathrm{Cl}^+(\mathcal{O}), & \text{if } r = 1, 2 \\ \mathrm{Cl}^+(\mathcal{O}) \oplus \{\pm 1\}, & \text{if } r = 0. \end{cases}$$

despite the fact that $\mathrm{NormCl}\,(\mathcal{O}/\mathbb{Z})$ is defined without separate treatment of the infinite places. When $\mathcal{O}$ is quadratic of discriminant Δ over $\mathbb{Z}$, we have $R^1_{\mathcal{O}/\mathbb{Z}}(\mathbb{G}_{m,O}) = R^1_\Delta$ and Theorems A and B together recover the classical correspondence between binary quadratic forms and the narrow class group.

Chapter 4 features an application of the norm class group to describing the 4-torsion of class groups of global fields. The 2-torsion part of the narrow class group of a quadratic number field is determined by Gauss's genus theory. The 4-torsion was described in [Réd34] as the rank of the Rédei matrix, which has as entries the local Artin symbols of primes at ramified places. This has been generalized to quadratic extensions of $\mathbb{F}_q(t)$ with q odd [Wit09, Thm 1.1] and to quadratic extensions of number fields of odd class number [Qin09]. We will see that for a quadratic extension of global fields, such a theory arises naturally for norm class groups from the Hochschild–Serre spectral sequence. Denoting the 2- and 4-rank of the norm class group of a quadratic extension of rings B/A by

$$r_2(B/A) = \dim_{\mathbb{F}_2} \mathrm{NormCl}\,(B/A)[2]$$
$$r_4(B/A) = \dim_{\mathbb{F}_2} \mathrm{NormCl}\,(B/A)[4]/\mathrm{NormCl}\,(B/A)[2]$$

we prove the following theorem.

Theorem C. *Let L/K be a quadratic extension of global fields with $\mathrm{char}(K) \neq 2$. Let $A \subseteq K$ be a PID with field of fractions K and $B \subseteq L$ the integral closure of A in L. Write $\widetilde{A} = A[\frac{1}{p_1}, \ldots, \frac{1}{p_t}]$ where $p_1, \ldots, p_t \in A$ are generators of the prime ideals of A at which B/A is ramified. Suppose $v_1, \ldots, v_s$ are the places of K not corresponding to a point in $\mathrm{Spec}\,\widetilde{A}$ and $\epsilon_1, \ldots, \epsilon_s$ is a basis for $\widetilde{A}^\times/(\widetilde{A}^\times)^2$. Define the matrix*

$$R_4 = (\theta_{v_i}(\epsilon_j))_{i,j}$$

where θ_{v_i} is the local Artin symbol of L/K at v_i. Then we have

$$r_4(B/A) = r_2(B/A) - \mathrm{rk}\, R_4.$$

The Galois cohomological argument for genus theory in [Lan80, Lem. 13.4.1] can be applied in this case to find the 2-rank:

$$r_2(B/A) = s - \dim_{\mathbb{F}_2} \left(B^{\mathrm{Norm}=1}/(B^{\mathrm{Norm}=1})^2\right).$$

The information about the norm class group can be related back to the wide class group via the short exact sequence

$$0 \longrightarrow A^\times/N_{L/K}\,(B^\times) \longrightarrow \mathrm{NormCl}\,(B/A) \longrightarrow \mathrm{Cl}(B) \longrightarrow 0$$

which holds whenever A is a PID. We will end with an example of this.

2 Torsors from quadratic forms

Fix a non-zero integer $\Delta \equiv 0, 1 \mod 4$. This chapter establishes the connection between quadratic forms and R^1_Δ-torsors. The goal is to construct the isomorphism

$$\mathcal{F}_\Delta/\mathrm{SL}_2(\mathbb{Z}) \xrightarrow{\sim} H^1(\operatorname{Spec}\mathbb{Z}_{fppf}, R^1_\Delta) \tag{2.1}$$

of Theorem A, thus providing a geometric proof of Theorem 1.2 on Gauss composition.

The proof can be broken down into three steps. The first step introduces the concept of $\mathrm{SL}_2(U)$-equivalences $(T_{Q_1})_U \xrightarrow{\sim} (T_{Q_2})_U$ and shows that equivalence of forms, composition and the group scheme structure of R^1_Δ can be phrased in terms of such isomorphisms. This is done in §2.1 and will be the only step that requires direct calculations with quadratic forms. Next, the proof that (2.1) is well-defined, injective and a homomorphism follows from the geometric theory of torsors. This is discussed in §2.2. The final step is to prove surjectivity, which will be done with faithfully flat descent in §2.3.

The last two steps resemble results in [CF15, §4.1] about other group schemes. It can be viewed as an instance of a more general method [Gir71, Thm. 2.5.1], recently referred to as the "yoga of forms" [Gil24, Rmk. 3.2]. However, the theory presented here will be self-contained, relying only on standard algebraic geometry, for example as in [Mil80].

2.1 Geometric Gauss composition

To speak about the theory of Gauss in geometric parlance, we establish the following dictionary.

For a form $Q \in \mathcal{F}_\Delta$, we define the scheme

$$T_Q \coloneqq \operatorname{Spec}\left(\frac{\mathbb{Z}[x,y]}{(Q(x,y)-1)}\right).$$

It represents the functor $\mathbf{Sch}^{\mathrm{op}} \to \mathbf{Sets}$ given by

$$U \longmapsto \{(x,y) \in \mathcal{O}_U(U)^2 : Q(x,y) = 1\}.$$

Using the fact that Q is primitive and [Mil80, I.2.5 and I.2.7], we see that T_Q is faithfully flat over $\operatorname{Spec}\mathbb{Z}$. For a scheme U over $\mathbb{Z}$, we denote the base change of T_Q to U by $(T_Q)_U$.

Definition 2.1. Let $Q_1, Q_2, Q_3 \in \mathcal{F}_\Delta$. A morphism of schemes $T_{Q_1} \times T_{Q_2} \to T_{Q_3}$ is called a *Gauss composition* if the corresponding ring homomorphism

$$\frac{\mathbb{Z}[b_1,b_2]}{(Q_3(b_1,b_2)-1)} \longrightarrow \frac{\mathbb{Z}[x,y,z,w]}{(Q_1(x,y)-1, Q_2(z,w)-1)}$$

sends b_i to a bilinear form $B_i(x,y,z,w) = a_ixz + b_ixw + c_iyz + d_iyw \in \mathbb{Z}[x,y,z,w]$ for $i = 1,2$ satisfying (1.2) and (1.3). For an affine scheme $U = \operatorname{Spec} A$, an isomorphism $(T_{Q_1})_U \xrightarrow{\sim} (T_{Q_2})_U$ is called an $\mathrm{SL}_2(U)$-*equivalence* if the corresponding ring isomorphism

$$\frac{A[x,y]}{(Q_2(x,y)-1)} \xrightarrow{\sim} \frac{A[x,y]}{(Q_1(x,y)-1)}$$

is given by $(x,y) \mapsto \gamma(x,y)$ for some matrix $\gamma \in \mathrm{SL}_2(A)$.

Clearly, $Q_3 \in \mathcal{F}_3$ is a composition of $Q_1, Q_2 \in \mathcal{F}_\Delta$ if and only if there exists a Gauss composition $T_{Q_1} \times T_{Q_2} \to T_{Q_3}$ and two forms $Q_1, Q_2 \in \mathcal{F}_\Delta$ are $\mathrm{SL}_2(\mathbb{Z})$-equivalent if and only if there exists an $\mathrm{SL}_2(\mathbb{Z})$-equivalence $T_{Q_1} \xrightarrow{\sim} T_{Q_2}$. For an affine scheme U, the composition of two $\mathrm{SL}_2(U)$-equivalences is again an $\mathrm{SL}_2(U)$-equivalence and for any affine $U' \to U$, the base change of an $\mathrm{SL}_2(U)$-equivalence to U' is an $\mathrm{SL}_2(U')$-equivalence.

The concept of $\mathrm{SL}_2(U)$-equivalences will be central to our discussion. An important example of this is the following characterization of Gauss compositions in terms of such isomorphisms, which also provides context for condition (1.3).

Lemma 2.2. *For $Q_1, Q_2, Q_3 \in \mathcal{F}_\Delta$, a morphism $T_{Q_1} \times T_{Q_2} \to T_{Q_3}$ is a Gauss composition if and only if the induced morphisms*

$$(T_{Q_2})_{T_{Q_1}} \longrightarrow (T_{Q_3})_{T_{Q_1}} \qquad \text{and} \qquad (T_{Q_1})_{T_{Q_2}} \longrightarrow (T_{Q_3})_{T_{Q_2}}$$

are respectively an $\mathrm{SL}_2(T_{Q_1})$-equivalence and an $\mathrm{SL}_2(T_{Q_2})$-equivalence.

Proof. First, we claim that for bilinear forms $B_i(x, y, z, w) = a_i xz + b_i xw + c_i yz + d_i yw$ satisfying (1.2) we have

$$\det \begin{pmatrix} a_1x + c_1y & b_1x + d_1y \\ a_2x + c_2y & b_2x + d_2y \end{pmatrix} = \pm Q_1(x, y) \text{ and } \det \begin{pmatrix} a_1z + b_1w & c_1z + d_1w \\ a_2z + b_2w & c_2z + d_2w \end{pmatrix} = \pm Q_2(z, w)$$

and both signs are + if and only if (1.3) holds. Indeed, for the matrix

$$M = \begin{pmatrix} a_1x + c_1y & b_1x + d_1y \\ a_2x + c_2y & b_2x + d_2y \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}[x, y])$$

we have $Q_3(M(z, w)) = Q_1(x, y)Q_2(z, w)$ and the discriminant of the left hand side is $(\det M)^2\Delta$ while the discriminant of the right hand side is $Q_1(x, y)^2\Delta$. Therefore, we must have $\det M = \pm Q(x, y)$ and evaluating in $(x, y) = (1, 0)$ tells us that the sign is + if and only if $a_1b_2 - a_2b_1 = Q_1(1, 0)$. The other half of the claim follows symmetrically.

Now, for a Gauss composition $T_{Q_1} \times T_{Q_2} \to T_{Q_3}$ it is immediate from the claim that the induced morphisms $(T_{Q_2})_{T_{Q_1}} \to (T_{Q_3})_{T_{Q_1}}$ and $(T_{Q_1})_{T_{Q_2}} \to (T_{Q_3})_{T_{Q_2}}$ are $\mathrm{SL}_2(T_{Q_1})$- and $\mathrm{SL}_2(T_{Q_2})$-equivalences respectively. Conversely, any morphism $T_{Q_1} \times T_{Q_2} \to T_{Q_3}$ satisfying the latter condition must clearly be given by bilinear forms $B_1, B_2 \in \mathbb{Z}[x, y, z, w]$ satisfying (1.2) and it follows from the claim that they must also satisfy (1.3). □

Let $\varepsilon \in \{0, 1\}$ such that $\Delta \equiv \varepsilon \mod 4$. The *principal form* $Q_0 \in \mathcal{F}_\Delta$ is defined as

$$Q_0(x, y) \coloneqq x^2 + \varepsilon xy - \frac{\Delta - \varepsilon}{4} y^2$$

and we set $R^1_\Delta \coloneqq T_{Q_0}$. This has two crucial properties. First, there is a section

$$e : \operatorname{Spec} \mathbb{Z} \longrightarrow R^1_\Delta$$

corresponding to the solution $(x, y) = (1, 0)$ of $Q_0(x, y) = 1$. Second, any form in $\mathcal{F}_\Delta$ is a composition of itself with Q_0. In fact, in Lemma 2.4 we will see that for every $Q \in \mathcal{F}_\Delta$ there is a canonical choice (with respect to e) of Gauss composition $T_Q \times R^1_\Delta \to T_Q$, namely the unique Gauss composition for which the composite

$$T_Q \xrightarrow{\mathrm{id}_{T_Q} \times e} T_Q \times R^1_\Delta \longrightarrow T_Q$$

is the identity. It is not hard to find explicitly: for $Q(x,y) = ax^2 + bxy + cy^2$ we have

$$Q\left(xz - \frac{b-\varepsilon}{2}yz - cyw, xw + ayz + \frac{b+\varepsilon}{2}yw\right) = Q_0(x,y)Q(z,w) \tag{2.2}$$

where $b \equiv \varepsilon \mod 2$ follows from $b^2 \equiv \Delta \equiv \varepsilon \mod 4$. It is readily verified that this defines a Gauss composition $T_Q \times R^1_\Delta \to T_Q$ with the desired property.

In particular, for $Q = Q_0$, the expression (2.2) yields a Gauss composition

$$\begin{aligned} R^1_\Delta \times R^1_\Delta &\longrightarrow R^1_\Delta. \\ ((x,y),(z,w)) &\longmapsto \left(xz + \frac{\Delta-\varepsilon}{4}yw,\ xw + yz + \varepsilon yw\right) \end{aligned} \tag{2.3}$$

Together with the section e and the inversion morphism $R^1_\Delta \to R^1_\Delta,\ (x,y) \mapsto (x+\varepsilon y, -y)$, it makes R^1_Δ into a commutative group scheme. The group scheme axioms are readily verified, but they will also follow from §3.3. From either (2.3) or Lemma 2.2, we see that multiplication by $g \in R^1_\Delta(U)$ is an $\mathrm{SL}_2(U)$-equivalence $(R^1_\Delta)_U \xrightarrow{\sim} (R^1_\Delta)_U$ for every affine scheme U. When U is flat over $\operatorname{Spec}\mathbb{Z}$, the converse holds as well.

Lemma 2.3. *For U affine and flat over $\mathbb{Z}$, a morphism of U-schemes $(R^1_\Delta)_U \to (R^1_\Delta)_U$ is an $\mathrm{SL}_2(U)$-equivalence if and only if it is multiplication by some $g \in R^1_\Delta(U)$.*

Proof. We have to show that an $\mathrm{SL}_2(U)$-equivalence $(R^1_\Delta)_U \xrightarrow{\sim} (R^1_\Delta)_U$ is multiplication by some $g \in R^1_\Delta(U)$. The desired $g \in R^1_\Delta(U)$ must be the image of 1 under this isomorphism. By multiplying by g^{-1}, we reduce to proving that an $\mathrm{SL}_2(U)$-equivalence $(R^1_\Delta)_U \xrightarrow{\sim} (R^1_\Delta)_U$ that fixes 1 is the identity. Such a matrix must be of the form $\left(\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right)$ for some $r \in \mathcal{O}_U(U)$ satisfying $Q_0(x+ry, y) = Q_0(x,y)$. But the coefficient of xy in $Q_0(x+ry,y)$ is $2r+\varepsilon$ while in $Q_0(x,y)$ it is ε. We obtain $2r = 0$, which implies $r = 0$ since U is flat. □

This lemma will be the key to proving Theorem A, since it connects equivalence and Gauss composition to the group scheme structure of R^1_Δ. This allows us to reason abstractly about the theory of binary quadratic forms without the need for explicit computations. This is best illustrated by an example, in the form of the following proof.

Lemma 2.4. *For every $Q \in \mathcal{F}_\Delta$, there is a unique Gauss composition $T_Q \times R^1_\Delta \to T_Q$ for which the composite*

$$T_Q \xrightarrow{\mathrm{id}\times e} T_Q \times R^1_\Delta \longrightarrow T_Q$$

is the identity on T_Q.

Proof. The desired morphism is given by (2.2). If there are two such Gauss compositions $T_Q \times R^1_\Delta \to T_Q$ they are uniquely determined by the induced isomorphisms $\alpha, \beta : (R^1_\Delta)_{T_Q} \xrightarrow{\sim} (T_Q)_{T_Q}$. These are $\mathrm{SL}_2(T_Q)$-equivalences by Lemma 2.2 and hence $\alpha^{-1} \circ \beta : (R^1_\Delta)_{T_Q} \xrightarrow{\sim} (R^1_\Delta)_{T_Q}$ is also an $\mathrm{SL}_2(T_Q)$-equivalence. It fixes e by assumption, which means that $\alpha^{-1} \circ \beta$ is the identity on $(R^1_\Delta)_{T_Q}$ by Lemma 2.3. Thus, $\alpha = \beta$. □

The proofs in the next section will all be of this nature.

2.2 Torsors

Before we proceed to the proof of Theorem A, we briefly summarize the information on torsors that we will be using. It is a slight adaptation of [Mil80, §III.4].

Throughout, we work in the fppf topology, i.e. a cover is a jointly surjective family of flat morphisms that are locally of finite type. Let G be a flat group scheme over X. A *G-torsor* is an X-scheme T that is faithfully flat and locally of finite type over X, together with a G-action $T \times_X G \to T$ such that the map

$$T \times_X G \longrightarrow T \times_X T,\ (s, g) \longmapsto (s, sg)$$

is an isomorphism. Equivalently, T is a scheme over X with a G-action $T \times_X G \to T$ and there exists a cover $(U_i)_i$ of X such that T_{U_i} is isomorphic with its G_{U_i}-action to G_{U_i} for every i. A *morphism of G-torsors* is a morphism of schemes respecting the G-action, and this is automatically an isomorphism.

A G-torsor T defines a class in the Čech cohomology group $\check{H}^1(X, G)$ as follows. Let $(U_i)_i$ be a cover of X that trivializes T, so that we may choose a section $s_i \in T(U_i)$ for every i. For all i, j, there is a unique $g_{ij} \in G(U_i \times U_j)$ such that $s_i|_{U_i \times U_j} g_{ij} = s_j|_{U_i \times U_j}$, and this gives a 1-cocycle $(g_{ij})_{i,j}$ in $\check{C}((U_i)_i/X, G)$. A different choice of the s_i yields a cohomologous cocycle, hence T defines a class in $\check{H}^1(X, G)$. This gives a bijection between the set of isomorphism classes of G-torsors and $\check{H}^1(X, G)$. We also have a canonical isomorphism $\check{H}^1(X, G) \cong H^1(X, G)$ by [Mil80, Cor. III.2.10]. From now on, we will identify the set of isomorphism classes of G-torsors with $H^1(X, G)$. Under this identification, G-torsors T_1, T_2 and T_3 satisfy $[T_1] + [T_2] = [T_3]$ in $H^1(X, G)$ if and only if there exists a morphism of schemes $m : T_1 \times_X T_2 \to T_3$ such that for every $U \to X$ and $s_1 \in T_1(U)$ and $s_2 \in T_2(U)$ and $g \in G(U)$ we have

$$m(s_1, s_2 g) \ = \ m(s_1 g, s_2) \ = \ m(s_1, s_2) g. \tag{2.4}$$

We can now give a more precise formulation of Theorem A.

Theorem 2.5. *Let $\Delta \equiv 0, 1 \mod 4$ be a non-zero integer. For $Q \in \mathcal{F}_\Delta$, the canonical Gauss composition $T_Q \times R^1_\Delta \to T_Q$ makes T_Q into an R^1_Δ-torsor. This gives a bijection*

$$\begin{aligned} \mathcal{F}_\Delta/\mathrm{SL}_2(\mathbb{Z}) &\xrightarrow{\sim} H^1(\operatorname{Spec} \mathbb{Z}, R^1_\Delta). \\ [Q] &\longmapsto [T_Q] \end{aligned} \tag{2.5}$$

For $Q_1, Q_2, Q_3 \in \mathcal{F}_\Delta$ we have $[T_{Q_1}] + [T_{Q_2}] = [T_{Q_3}]$ if and only if Q_3 is a composition of Q_1 and Q_2.

It is clear that Theorem 1.2 on Gauss composition will follow from this theorem, except for finiteness, which we will get back to. For now, we will prove that (2.5) is well-defined and injective and that $Q_1, Q_2, Q_3 \in \mathcal{F}_\Delta$ satisfy $[T_{Q_1}] + [T_{Q_2}] = [T_{Q_3}]$ if and only if Q_3 is a composition of Q_1 and Q_2. This is the content of the following lemma.

Lemma 2.6. *Let $Q, Q_1, Q_2, Q_3 \in \mathcal{F}_\Delta$.*

(a) The canonical Gauss composition $T_Q \times R^1_\Delta \to T_Q$ makes T_Q into an R^1_Δ-torsor.

(b) For U affine and flat over $\operatorname{Spec}\mathbb{Z}$, an isomorphism of U-schemes $(T_{Q_1})_U \xrightarrow{\sim} (T_{Q_2})_U$ is an isomorphism of $(R^1_\Delta)_U$-torsors if and only if it is an $\mathrm{SL}_2(U)$-equivalence.

(c) We have $[T_{Q_1}] + [T_{Q_2}] = [T_{Q_3}]$ in $H^1(\operatorname{Spec}\mathbb{Z}, R^1_\Delta)$ if and only if there exists a Gauss composition $T_{Q_1} \times T_{Q_2} \to T_{Q_3}$.

Proof. (a) We already noted that T_Q is faithfully flat, and it is clearly of finite type. Denote the Gauss composition $T_Q \times R^1_\Delta \to T_Q$ from Lemma 2.4 by $(s, g) \mapsto s \cdot g$. Recall that $- \cdot e : T_Q \to T_Q$ is the identity morphism. Write $U = T_Q \times R^1_\Delta$ and let $s \in T_Q(U)$ and $g \in R^1_\Delta(U)$ be the natural sections. Then the morphisms $s \cdot - : (R^1_\Delta)_U \to (T_Q)_U$ and $- \cdot g : (T_Q)_U \to (T_Q)_U$ are $\mathrm{SL}_2(U)$-equivalences by Lemma 2.2. The isomorphism $(R^1_\Delta)_U \xrightarrow{\sim} (R^1_\Delta)_U$ fitting into the diagram

$$\begin{array}{ccc} (R^1_\Delta)_U & \xrightarrow{\sim} & (R^1_\Delta)_U \\ {\scriptstyle s\cdot -}\downarrow & & \downarrow{\scriptstyle s\cdot -} \\ (T_Q)_U & \xrightarrow{-\cdot g} & (T_Q)_U \end{array}$$

must send e to g and is an $\mathrm{SL}_2(U)$-equivalence, since all other morphisms in the diagram are. Hence, by Lemma 2.3, it is multiplication by g. This shows that the morphism $T_Q \times R^1_\Delta \to T_Q$ defines an R^1_Δ-action on T_Q. It makes T_Q into an R^1_Δ-torsor, as the map $T_Q \times R^1_\Delta \to T_Q \times T_Q$ is an isomorphism by Lemma 2.2.

(b) Write $U' = T_{Q_1} \times U$ and let $s \in T_{Q_1}(U')$ be the obvious section. Suppose we have an isomorphism of U-schemes $\varphi : (T_{Q_1})_U \xrightarrow{\sim} (T_{Q_2})_U$ and consider the isomorphism $(R^1_\Delta)_{U'} \xrightarrow{\sim} (R^1_\Delta)_{U'}$ making the following diagram commute:

$$\begin{array}{ccc} (R^1_\Delta)_{U'} & \xrightarrow{\sim} & (R^1_\Delta)_{U'} \\ {\scriptstyle s\cdot -}\downarrow & & \downarrow{\scriptstyle \varphi_{U'}(s)\cdot -} \\ (T_{Q_1})_{U'} & \xrightarrow{\varphi_{U'}} & (T_{Q_2})_{U'} \end{array}$$

Note that φ is an isomorphism of $(R^1_\Delta)_U$-torsors if and only if $(R^1_\Delta)_{U'} \xrightarrow{\sim} (R^1_\Delta)_{U'}$ is the identity. But since it fixes e, it is by Lemma 2.3 the identity if and only if it is an $\mathrm{SL}_2(U')$-equivalence, which is equivalent to $\varphi_{U'}$ being so. Since $\varphi : (T_{Q_1})_U \xrightarrow{\sim} (T_{Q_2})_U$ is an isomorphism over U, this happens exactly when φ is an $\mathrm{SL}_2(U)$-equivalence.

(c) We have $[T_{Q_1}] + [T_{Q_2}] = [T_{Q_3}]$ in $H^1(X, R^1_\Delta)$ if and only there exists a morphism $T_{Q_1} \times T_{Q_2} \to T_{Q_3}$ compatible with the R^1_Δ-action in the sense of (2.4). But this is equivalent to the induced maps $(T_{Q_2})_{T_{Q_1}} \to (T_{Q_3})_{T_{Q_1}}$ and $(T_{Q_1})_{T_{Q_2}} \to (T_{Q_3})_{T_{Q_2}}$ being morphisms of $(R^1_\Delta)_{T_{Q_1}}$-torsors and $(R^1_\Delta)_{T_{Q_2}}$-torsors respectively, which are then automatically isomorphisms. By (b), this happens exactly when they are $\mathrm{SL}_2(T_{Q_1})$- and $\mathrm{SL}_2(T_{Q_2})$-equivalences respectively. The result now follows from Lemma 2.2. □

It remains to show that (2.5) is surjective, i.e. that every R^1_Δ-torsor is of the form T_Q for some $Q \in \mathcal{F}_\Delta$. But for an R^1_Δ-torsor T this is at least true after a faithfully flat base change, as we have $T_T \cong (R^1_\Delta)_T$. The last part of this chapter will employ faithfully flat descent to show that this indeed implies that $T \cong T_Q$ for some $Q \in \mathcal{F}_\Delta$.

Remark 2.7. If one already knows that a quadratic order $\mathcal{O}$ of discriminant Δ satisfies

$$\mathcal{F}_\Delta/\mathrm{SL}_2(\mathbb{Z}) \cong \begin{cases} \mathrm{Cl}^+(\mathcal{O}), & \text{if } \Delta > 0 \\ \mathrm{Cl}^+(\mathcal{O}) \oplus \{\pm 1\}, & \text{if } \Delta < 0 \end{cases}$$

then there is a shortcut to surjectivity. Namely, we will see in Chapter 3 that R^1_Δ fits into a short exact sequence

$$0 \longrightarrow R^1_{Y/X}(\mathbb{G}_{m,Y}) \longrightarrow R_{Y/X}(\mathbb{G}_{m,Y}) \longrightarrow \mathbb{G}_{m,X} \longrightarrow 0$$

for the fppf topology, whose long exact sequence of cohomology groups gives rise to a short exact sequence

$$0 \longrightarrow \{\pm 1\}/N_{\mathcal{O}/\mathbb{Z}}(\mathcal{O}^\times) \longrightarrow H^1(\operatorname{Spec}\mathbb{Z}, R^1_\Delta) \longrightarrow \mathrm{Cl}(\mathcal{O}) \longrightarrow 0.$$

Since the canonical surjection from the narrow class group $\mathrm{Cl}^+(\mathcal{O})$ to the wide class group $\mathrm{Cl}(\mathcal{O})$ has kernel of order 2 if $\mathcal{O}$ has an element of norm -1 and of order 1 otherwise, the order of $H^1(\operatorname{Spec}\mathbb{Z}, R^1_\Delta)$ exactly matches the cardinality of $\mathcal{F}_\Delta/\mathrm{SL}_2(\mathbb{Z})$. This order is finite, as $\mathrm{Cl}(\mathcal{O})$ is finite, and surjectivity follows. In any case, the short exact sequence does show that $H^1(\operatorname{Spec}\mathbb{Z}, R^1_\Delta)$ is finite, which was needed to make Theorem 1.2 follow from Theorem 2.5.

Still, we opt to prove directly that every R^1_Δ-torsor is of the form T_Q, as this keeps closer to Gauss's theory of quadratic forms and includes the case that Δ is square. We will derive the correspondence between $\mathcal{F}_\Delta/\mathrm{SL}_2(\mathbb{Z})$ and the narrow class group ourselves in §3.4.

2.3 Faithfully flat descent of quadratic forms

Our references for descent are [Mil80, Rmk. I.2.21] and [Mur67, Chapter 7]. Before we discuss descent of quadratic forms, we briefly recall descent of modules. Let A be a faithfully flat $\mathbb{Z}$-algebra. Let M be a $\mathbb{Z}$-module and write $N = A \otimes_\mathbb{Z} M$. There is an isomorphism of $A \otimes_\mathbb{Z} A$-modules

$$\begin{aligned} \varphi : \quad N \otimes_\mathbb{Z} A &\xrightarrow{\sim} A \otimes_\mathbb{Z} N \\ (a \otimes m) \otimes a' &\longmapsto a \otimes (a' \otimes m) \end{aligned} \tag{2.6}$$

and M can be recovered from the pair (N, φ) as

$$M = \{n \in N : \varphi(n \otimes 1) = 1 \otimes n\}.$$

Faithfully flat descent tells us exactly which pairs (N, φ) arise in this way.

Let N be an A-module and $\varphi : N \otimes_\mathbb{Z} A \xrightarrow{\sim} A \otimes_\mathbb{Z} N$ an isomorphism of $A \otimes_\mathbb{Z} A$-modules. Define

$$\begin{aligned} \varphi_1 &: A \otimes_\mathbb{Z} N \otimes_\mathbb{Z} A \xrightarrow{\sim} A \otimes_\mathbb{Z} A \otimes_\mathbb{Z} N \\ \varphi_2 &: N \otimes_\mathbb{Z} A \otimes_\mathbb{Z} A \xrightarrow{\sim} A \otimes_\mathbb{Z} A \otimes_\mathbb{Z} N \\ \varphi_3 &: N \otimes_\mathbb{Z} A \otimes_\mathbb{Z} A \xrightarrow{\sim} A \otimes_\mathbb{Z} N \otimes_\mathbb{Z} A \end{aligned}$$

by tensoring φ with id_A in the first, second and third position respectively. Then the pair (N, φ) arises from a $\mathbb{Z}$-module M as above if and only if φ satisfies the *cocycle condition*

$$\varphi_2 \;=\; \varphi_1 \circ \varphi_3.$$

That is to say, there exists a $\mathbb{Z}$-module M and an isomorphism $\gamma : A \otimes_{\mathbb{Z}} M \xrightarrow{\sim} N$ such that the diagram

$$\begin{array}{ccc} (A \otimes_{\mathbb{Z}} M) \otimes_{\mathbb{Z}} A & \xrightarrow{\gamma \otimes \mathrm{id}_A} & N \otimes_{\mathbb{Z}} A \\ {\scriptstyle \varphi'}\downarrow & & \downarrow{\scriptstyle \varphi} \\ A \otimes_{\mathbb{Z}} (A \otimes_{\mathbb{Z}} M) & \xrightarrow{\mathrm{id}_A \otimes \gamma} & A \otimes_{\mathbb{Z}} N \end{array}$$

commutes, where φ' is the isomorphism in (2.6). Specifically, M is the kernel of the morphism $d^1 - \varphi \circ d^2 : N \to A \otimes_{\mathbb{Z}} N$, where

$$\begin{aligned} d^1 : N \;&\longrightarrow\; A \otimes_{\mathbb{Z}} N \\ d^2 : N \;&\longrightarrow\; N \otimes_{\mathbb{Z}} A \end{aligned}$$

are obtained by tensoring with $\mathbb{Z} \to A$ in the first and second position respectively. The isomorphism $\gamma : A \otimes_{\mathbb{Z}} M \xrightarrow{\sim} N$ is induced by the injection $M \to N$, i.e. it is given by $a \otimes m \mapsto am$.

If N is a finitely generated torsion-free A-module, then M is a finitely generated torsion-free $\mathbb{Z}$-module, which must be free. It follows that if N is free of rank n, then so is M.

We are interested in descent of binary quadratic forms $Q' = ax^2 + bxy + cy^2 \in A[x, y]$, which we now view as maps $Q' : A^2 \to A$. We identify $A^2 \otimes_{\mathbb{Z}} A$ and $A \otimes_{\mathbb{Z}} A^2$ both with $(A \otimes_{\mathbb{Z}} A)^2$ via the isomorphisms

$$\begin{array}{ccc} A^2 \otimes_{\mathbb{Z}} A \xrightarrow{\sim} (A \otimes_{\mathbb{Z}} A)^2 & \quad \text{and} \quad & A \otimes_{\mathbb{Z}} A^2 \xrightarrow{\sim} (A \otimes_{\mathbb{Z}} A)^2 \\ (a, a') \otimes b \longmapsto (a \otimes b, a' \otimes b) & & a \otimes (b, b') \longmapsto (a \otimes b, a \otimes b') \end{array}$$

so that (2.6) becomes the identity on $(A \otimes_{\mathbb{Z}} A)^2$. In this case, a *descent datum* is a pair (Q', φ), where Q' is a binary quadratic form over A and φ is a matrix in $\mathrm{SL}_2(A \otimes_{\mathbb{Z}} A)$ that satisfies the cocycle condition $\varphi_2 = \varphi_1\varphi_3$ and preserves Q', in the sense that it satisfies $Q'(\varphi(x, y)) = Q'(x, y)$ over $A \otimes_{\mathbb{Z}} A$. The following result says that every such descent datum comes from a binary quadratic form over $\mathbb{Z}$.

Proposition 2.8. *Let A be a faithfully flat $\mathbb{Z}$-algebra and let $Q' \in A[x, y]$ be a binary quadratic form over A. Suppose that there exists a matrix $\varphi \in \mathrm{SL}_2(A \otimes_{\mathbb{Z}} A)$ that preserves Q' and satisfies the cocycle condition $\varphi_2 = \varphi_3\varphi_1$. Then there exists a binary quadratic form $Q \in \mathbb{Z}[x, y]$ and a matrix $\gamma \in \mathrm{SL}_2(A)$ such that*

$$Q'(\gamma(x, y)) \;=\; Q(x, y) \qquad \textit{and} \qquad (\mathrm{id}_A \otimes \gamma) \;=\; \varphi \circ (\gamma \otimes \mathrm{id}_A).$$

Proof. By the descent of modules described above, the pair (A^2, φ) descends to a $\mathbb{Z}$-module. As noted, since A^2 is free of rank 2, this $\mathbb{Z}$-module must be a free of rank 2 and therefore isomorphic to $\mathbb{Z}^2$. That is, there is an exact sequence

$$0 \;\longrightarrow\; \mathbb{Z}^2 \;\longrightarrow\; A^2 \xrightarrow{d^1 - \varphi \circ d^2} (A \otimes_{\mathbb{Z}} A)^2.$$

and the map $\gamma : \mathbb{Z}^2 \otimes_{\mathbb{Z}} A = A^2 \to A^2$ induced by the injection $\mathbb{Z}^2 \to A^2$ is an isomorphism satisfying $\mathrm{id}_A \otimes \gamma = \varphi \circ (\gamma \otimes \mathrm{id}_A)$. This last condition together with $\det(\varphi) = 1$ implies $1 \otimes \det(\gamma) = \det(\gamma) \otimes 1$ and therefore $\det(\gamma) \in \mathbb{Z}^\times$. By possibly changing coordinates of $\mathbb{Z}^2$, we may assume $\det(\gamma) = 1$. Since φ preserves Q', we have a commutative diagram

$$\begin{array}{ccc} A^2 & \xrightarrow{d^1 - \varphi \circ d^2} & (A \otimes_{\mathbb{Z}} A)^2 \\ {\scriptstyle Q'}\downarrow & & \downarrow{\scriptstyle Q'} \\ A & \xrightarrow{d^1 - d^2} & A \otimes_{\mathbb{Z}} A \end{array}$$

and Q' therefore restricts to a quadratic form $Q : \mathbb{Z}^2 \to \mathbb{Z}$ between the kernels. That is, we have a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{Z}^2 & \longrightarrow & A^2 & \xrightarrow{d^1 - \varphi \circ d^2} & (A \otimes_{\mathbb{Z}} A)^2 \\ & & {\scriptstyle Q}\downarrow & & {\scriptstyle Q'}\downarrow & & \downarrow{\scriptstyle Q'} \\ 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & A & \xrightarrow{d^1 - d^2} & A \otimes_{\mathbb{Z}} A. \end{array}$$

Since $\gamma : \mathbb{Z}^2 \otimes A = A^2 \xrightarrow{\sim} A^2$ is the map induced by the injection $\mathbb{Z}^2 \to A$ in this diagram, we obtain a commutative diagram

$$\begin{array}{ccc} \mathbb{Z}^2 \otimes_{\mathbb{Z}} A & \xrightarrow{\gamma} & A^2 \\ {\scriptstyle Q}\downarrow & & \downarrow{\scriptstyle Q'} \\ \mathbb{Z} \otimes_{\mathbb{Z}} A & \xrightarrow{\mathrm{id}} & A \end{array}$$

which shows $Q'(\gamma(x, y)) = Q(x, y)$. □

To prove surjectivity of the map (2.5) in Theorem 2.5, we have to show that every R^1_Δ-torsor is of the form T_Q for some $Q \in \mathcal{F}_\Delta$. We will do this by associating a descent datum on the principal form Q_0 to T and applying Proposition 2.8.

Proof of Theorem 2.5. After Lemma 2.6, it remains only to prove that (2.5) is surjective, i.e. that every R^1_Δ-torsor is isomorphic to T_Q for some $Q \in \mathcal{F}_\Delta$.

Let T be an R^1_Δ-torsor. Since T is faithfully flat and R^1_Δ is affine, it follows from $T_T \cong (R^1_\Delta)_T$ that T is affine, say $T = \operatorname{Spec} A$. Recall that, for a cover $(U_i)_i$ of $\operatorname{Spec} \mathbb{Z}$ with sections $s_i \in T(U_i)$ for every i, the element in $\check{H}^1((U_i)_i/\operatorname{Spec} \mathbb{Z}, R^1_\Delta)$ associated to T is the class of the cocycle $(g_{ij})_{i,j}$, where $g_{ij} \in R^1_\Delta(U_i \times U_j)$ is defined by $s_i|_{U_i \times U_j} g_{ij} = s_j|_{U_i \times U_j}$. Now, $T \to \operatorname{Spec} \mathbb{Z}$ is also an fppf cover and we have the canonical section in $T(T)$. The element of $\check{H}^1(T/X, R^1_\Delta)$ associated to the R^1_Δ-torsor T is then the class of the 1-cocycle $g \in R^1_\Delta(T \times T)$ making the diagram

$$\begin{array}{ccc} (R^1_\Delta)_{T \times T} & \xrightarrow{-\cdot g} & (R^1_\Delta)_{T \times T} \\ & {\scriptstyle s_2 \cdot -} \searrow & \downarrow{\scriptstyle s_1 \cdot -} \\ & & T_{T \times T} \end{array}$$

commute, where $s_1, s_2 \in T(T \times T)$ are the canonical sections. By Lemma 2.3, g is given by a matrix $\varphi \in \mathrm{SL}_2(A \otimes_{\mathbb{Z}} A)$ and it must preserve Q_0. Since g is a 1-cocycle, φ satisfies the

cocycle condition $\varphi_2 = \varphi_3\varphi_1$. Hence, by Proposition 2.8, there exists a binary quadratic form $Q \in \mathbb{Z}[x, y]$ and a matrix $\gamma \in \mathrm{SL}_2(A)$ such that

$$Q_0(\gamma(x, y)) = Q(x, y) \qquad \text{and} \qquad (\mathrm{id}_A \otimes \gamma) = \varphi \circ (\gamma \otimes \mathrm{id}_A).$$

It is easy to see that Q being $\mathrm{SL}_2(A)$-equivalent to Q_0 implies that it is primitive of discriminant Δ, i.e. $Q \in \mathcal{F}_\Delta$. Moreover, the matrices $(\mathrm{id}_A \otimes \gamma)^{-1}$ and $(\gamma \otimes \mathrm{id}_A)^{-1}$ define isomorphisms $(R^1_\Delta)_{T\times T} \xrightarrow{\sim} (T_Q)_{T\times T}$ and therefore sections $s_1, s_2 \in T_Q(T \times T)$. From $(\mathrm{id}_A \otimes \gamma)^{-1} \circ \varphi = (\gamma \otimes \mathrm{id}_A)^{-1}$ we see that they satisfy $s_1 g = s_2$. Thus, T and T_Q define the same element in $\check{H}^1(T/\mathrm{Spec}\,\mathbb{Z}, R^1_\Delta)$ and hence in $\check{H}^1(\mathrm{Spec}\,\mathbb{Z}, R^1_\Delta)$. We conclude that T and T_Q are isomorphic as R^1_Δ-torsors. This proves that (2.5) is surjective and hence an isomorphism. □

3 The norm class group

The group scheme R^1_Δ is a special case of the norm 1 group scheme $R^1_{Y/X}(\mathbb{G}_{m,Y})$, defined for any finite locally free morphism $f : Y \to X$ to be the kernel of the norm morphism

$$\mathbf{Norm} : R_{Y/X}(\mathbb{G}_{m,Y}) \longrightarrow \mathbb{G}_{m,X}$$

where $R_{Y/X}(\mathbb{G}_{m,Y})$ is the Weil restriction of $\mathbb{G}_{m,Y}$ along f. The goal of this chapter is to prove Theorem B, by constructing for any finite locally free $f : Y \to X$ an isomorphism

$$\mathrm{NormCl}\,(Y/X) \xrightarrow{\sim} H^1(X, R^1_{Y/X}(\mathbb{G}_{m,Y}))$$

where $\mathrm{NormCl}\,(Y/X)$ is the group of isomorphism classes of invertible $\mathcal{O}_Y$-modules $\mathcal{L}$ together with a choice of isomorphism $N(\mathcal{L}) \xrightarrow{\sim} \mathcal{O}_X$. This is similar in nature to the description of $H^1(X, \mu_{n,X})$ in [Mil80, p. 125]. We will first discuss the norm morphism and its properties in §3.1 before proving Theorem B in §3.2.

When Y is the spectrum of a quadratic ring of discriminant Δ over $\mathbb{Z}$, we will show that $R^1_{Y/X}(\mathbb{G}_{m,Y})$ is equal to R^1_Δ. In this case, Theorem B provides another perspective on the correspondence between binary quadratic forms and R^1_Δ-torsors. While Chapter 2 kept close to the work of Gauss, this new perspective is more akin to the theory of ideal classes that Dedekind introduced. This is the content of §3.3.

In §3.4, we will relate $\mathrm{NormCl}\,(B/\mathbb{Z})$ to the narrow class group $\mathrm{Cl}^+(B)$ in the case that B is an order in a number field. Specifically, we will prove that the canonical surjection $\mathrm{Cl}^+(B) \to \mathrm{Cl}(B)$ to the wide class group factors through $\mathrm{NormCl}\,(B/\mathbb{Z})$.

3.1 The norm morphism

Recall that a morphism of schemes $f : Y \to X$ is *finite locally free* (of rank n) if it is affine and $f_*\mathcal{O}_Y$ is a finite locally free $\mathcal{O}_X$-module (of rank n). A morphism is finite locally free if and only if it is finite, flat and locally of finite presentation. We start with the norm morphism as described by Grothendieck.

Proposition 3.1. *Let $f : Y \to X$ be a finite locally free morphism of schemes.*

(a) There is a unique morphism of sheaves of sets

$$\mathbf{norm} : f_*\mathcal{O}_Y \longrightarrow \mathcal{O}_X$$

such that for every open $U \subseteq X$ with $f_*\mathcal{O}_Y|_U \cong \mathcal{O}_U^n$ and $s \in f_*\mathcal{O}_Y(U)$, the determinant of the endomorphism of the free $\mathcal{O}_X(U)$-module $f_*\mathcal{O}_Y(U)$ given by multiplication by s is $\mathbf{norm}_U(s) \in \mathcal{O}_X(U)$.

(b) For global sections $s, s' \in \mathcal{O}_Y(Y) = (f_*\mathcal{O}_Y)(X)$ we have

$$\mathbf{norm}_X(ss') = \mathbf{norm}_X(s)\mathbf{norm}_X(s')$$

and we have $s \in \mathcal{O}_Y(Y)^\times$ if and only if $\mathrm{norm}_X(s) \in \mathcal{O}_X(X)^\times$.

(c) The norm is compatible with base change, i.e. for a cartesian diagram of schemes

$$\begin{array}{ccc} Y' & \xrightarrow{h} & Y \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle f} \\ X' & \xrightarrow{g} & X \end{array}$$

the following diagram commutes:

$$\begin{array}{ccc} f_*\mathcal{O}_Y & \xrightarrow{\mathbf{norm}} & \mathcal{O}_X \\ {\scriptstyle f_*h^\sharp}\downarrow & & \downarrow{\scriptstyle g^\sharp} \\ g_*f'_*\mathcal{O}_{Y'} & \xrightarrow{g_*\mathbf{norm}} & g_*\mathcal{O}_{X'} \end{array}$$

Proof. See [EGAII, §6.5]. □

Fix a finite locally free morphism of schemes $f : Y \to X$. By Proposition 3.1, we have for every X-scheme T a group homomorphism

$$\mathbf{norm}_T|_{\mathcal{O}_{T\times_X Y}(T\times_X Y)^\times} : \mathcal{O}_{T\times_X Y}(T\times_X Y)^\times \longrightarrow \mathcal{O}_T(T)^\times \tag{3.1}$$

and this is natural in T. For any smooth affine scheme V over Y, the presheaf of sets

$$f_*V = \mathrm{Hom}_Y(-\times_X Y, V) : (\mathbf{Sch}/X)^{\mathrm{op}} \longrightarrow \mathbf{Sets}$$

is representable by a smooth affine scheme $R_{Y/X}(V)$ over X, its *Weil restriction* [Sch94, Prop. 4.1]. The Weil restriction of a group scheme is itself naturally a group scheme. In particular, the functor

$$\mathcal{O}_{-\times_X Y}(-\times_X Y)^\times : (\mathbf{Sch}/X)^{\mathrm{op}} \longrightarrow \mathbf{Ab}$$

is represented by a smooth affine commutative group scheme $R_{Y/X}(\mathbb{G}_{m,Y})$. Hence, (3.1) defines a morphism of group schemes

$$\mathbf{Norm} : R_{Y/X}(\mathbb{G}_{m,Y}) \longrightarrow \mathbb{G}_{m,X}$$

which we call the *norm morphism*. Its kernel is the *norm 1 group scheme* $R^1_{Y/X}(\mathbb{G}_{m,Y})$.

If $X = \mathrm{Spec}\, R$ and $Y = \mathrm{Spec}\, S$ are affine with S free of rank n as an R-module, we have an explicit description of the norm morphism. Let $b_1, \ldots, b_n \in S$ be an R-basis for S and let $Q_0 \in R[x_1, \ldots, x_n]$ be the image of $b_1x_1 + \cdots + b_nx_n$ under the map

$$\mathbf{norm}_{R[x_1,\ldots,x_n]} : S[x_1, \ldots, x_n] \longrightarrow R[x_1, \ldots, x_n].$$

Then for every R-algebra A, the map $\mathbf{norm}_R : A \otimes_R S \to A$ is given by

$$\mathbf{norm}_A(a_1 \otimes b_1 + \cdots + a_n \otimes b_n) = Q_0(a_1, \ldots, a_n) \tag{3.2}$$

for all $a_1, \ldots, a_n \in A$ by Proposition 3.1(c). Hence, by 3.1(b), the norm morphism $\mathbf{Norm} : R_{Y/X}(\mathbb{G}_{m,Y}) \to \mathbb{G}_{m,X}$ corresponds with the ring homomorphism

$$R[t, t^{-1}] \longrightarrow R[t, t^{-1}][x_1, \ldots, x_n]/(Q_0(x_1, \ldots, x_n) - t) \tag{3.3}$$

and its kernel is

$$R^1_{Y/X}(\mathbb{G}_{m,Y}) = \mathrm{Spec}\left(\frac{R[x_1, \ldots, x_n]}{(Q_0(x_1, \ldots, x_n) - 1)}\right).$$

Proposition 3.2. *The norm morphism* $\mathbf{Norm} : R_{Y/X}(\mathbb{G}_{m,Y}) \to \mathbb{G}_{m,X}$ *is faithfully flat.*

Proof. Since $f : Y \to X$ is finite locally free, X is covered by open affine U subschemes such that $U = \operatorname{Spec} R$ and $Y \times_X U = \operatorname{Spec} S$ with S free of finite rank as an R-module. The result therefore follows from the observation that (3.3) is a faithfully flat ring homomorphism, as Q_0 represents 1 over R. □

Corollary 3.3. *Both $R_{Y/X}(\mathbb{G}_{m,Y})$ and $R^1_{Y/X}(\mathbb{G}_{m,Y})$ are flat group schemes over X and the following is a short exact sequence of sheaves in the fppf topology on X:*

$$0 \longrightarrow R^1_{Y/X}(\mathbb{G}_{m,Y}) \longrightarrow R_{Y/X}(\mathbb{G}_{m,Y}) \xrightarrow{\mathbf{Norm}} \mathbb{G}_{m,X} \longrightarrow 0.$$

The long exact sequence of cohomology induced by this short exact sequence is

$$\begin{aligned} 1 \longrightarrow \mathcal{O}_Y(Y)^{\mathrm{Norm}=1} \longrightarrow \mathcal{O}_Y(Y)^\times \xrightarrow{\mathbf{Norm}} \mathcal{O}_X(X)^\times \\ \hookrightarrow H^1(X, R^1_{Y/X}(\mathbb{G}_{m,Y})) \longrightarrow H^1(X, R_{Y/X}(\mathbb{G}_{m,Y})) \xrightarrow{\mathbf{Norm}} H^1(X, \mathbb{G}_{m,X}) \longrightarrow \cdots . \end{aligned}$$

We know that $H^1(X, \mathbb{G}_{m,X})$ is the Picard group $\operatorname{Pic}(X)$, but the following proposition shows that we also have $H^1(X, R_{Y/X}(\mathbb{G}_{m,Y})) = \operatorname{Pic}(Y)$.

Proposition 3.4. *For every invertible $\mathcal{O}_Y$-module $\mathcal{L}$, there exists a Zariski open cover $(U_i)_i$ of X such that $\mathcal{L}|_{U_i \times_X Y} \cong \mathcal{O}_{U_i \times_X Y}$ for every i.*

Proof. See [EGAII, Lem. 6.1.12.1]. □

Specifically, the proposition implies that the natural injection of Čech cohomology groups $\check{H}^1(X, R_{Y/X}(\mathbb{G}_{m,Y})) \to \check{H}^1(Y, \mathbb{G}_{m,Y})$ is surjective, which gives a canonical isomorphism $H^1(X, R_{Y/X}(\mathbb{G}_{m,Y})) \cong \operatorname{Pic}(Y)$. Thus, the long exact sequence becomes

$$\begin{aligned} 1 \longrightarrow \mathcal{O}_Y(Y)^{\mathrm{Norm}=1} \longrightarrow \mathcal{O}_Y(Y)^\times \xrightarrow{\mathbf{Norm}} \mathcal{O}_X(X)^\times \\ \hookrightarrow H^1(X, R^1_{Y/X}(\mathbb{G}_{m,Y})) \longrightarrow \operatorname{Pic}(Y) \xrightarrow{\mathbf{Norm}} \operatorname{Pic}(X) \longrightarrow \cdots . \end{aligned} \tag{3.4}$$

We will now define the norm class group $\operatorname{NormCl}(Y/X)$ and prove that it is isomorphic to $H^1(X, R^1_{Y/X}(\mathbb{G}_{m,Y}))$, by showing that it fits into the same exact sequence.

3.2 The norm class group

Let $\mathcal{L}$ be an invertible $\mathcal{O}_Y$-module. In [EGAII, §6.5], Grothendieck defines the *norm* of $N(\mathcal{L})$ of $\mathcal{L}$, which is an invertible $\mathcal{O}_X$-module. We will summarize the construction here.

By Proposition 3.4, there exists a Zariski open cover $(U_i)_i$ of X with for every i an isomorphism $\eta_i : \mathcal{L}|_{U_i \times_X Y} \xrightarrow{\sim} \mathcal{O}_{U_i \times_X Y}$. For all i and j, one obtains an automorphism $\eta_i \circ \eta_j^{-1}$ of $\mathcal{O}_{U_{ij} \times_X Y}$, which corresponds to an element $\omega_{ij} \in \mathbb{G}_{m,Y}(U_{ij} \times_X Y) = R_{Y/X}(\mathbb{G}_{m,Y})(U_{ij})$. The images $\mathbf{Norm}\,(\omega_{ij}) \in \mathbb{G}_{m,X}(U_{ij})$ of these elements under the norm morphism define a 1-cocycle and hence an invertible $\mathcal{O}_X$-module $N(\mathcal{L})$. Explicitly, $N(\mathcal{L})$ is obtained by gluing the trivial $\mathcal{O}_{U_i}$-module $\mathcal{O}_{U_i}$ along the isomorphisms $\mathcal{O}_{U_{ij}} \xrightarrow{\sim} \mathcal{O}_{U_{ij}}$ given by multiplication by $\mathbf{Norm}\,(\omega_{ij})$. This is independent of the choice of trivialization of $\mathcal{L}$.

It is clear from this construction that the map $\mathbf{Norm} : \mathrm{Pic}(Y) \to \mathrm{Pic}(X)$ in (3.4) is given by $[\mathcal{L}] \mapsto [N(\mathcal{L})]$. In particular, we have canonical isomorphisms

$$N(\mathcal{L} \otimes \mathcal{L}') \cong N(\mathcal{L}) \otimes N(\mathcal{L}') \qquad \text{and} \qquad N(\mathcal{O}_Y) \cong \mathcal{O}_X.$$

Furthermore, a morphism of $\mathcal{O}_Y$-modules $\varphi : \mathcal{L} \to \mathcal{L}'$ induces a morphism of $\mathcal{O}_X$-modules $N(\varphi) : N(\mathcal{L}) \to N(\mathcal{L}')$ in the obvious way, and this is functorial and compatible with the tensor product. For an automorphism $\varphi : \mathcal{O}_Y \xrightarrow{\sim} \mathcal{O}_Y$, the following diagram commutes:

$$\begin{array}{ccc} f_*\mathcal{O}_Y & \xrightarrow{\mathbf{norm}} & \mathcal{O}_X \\ {\scriptstyle f_*\varphi}\downarrow & & \downarrow{\scriptstyle N(\varphi)} \\ f_*\mathcal{O}_Y & \xrightarrow{\mathbf{norm}} & \mathcal{O}_X. \end{array} \tag{3.5}$$

For details, see [EGAII, §6.5]. This allows us to define the norm class group as follows.

Definition 3.5. Consider pairs $(\mathcal{L}, \varphi)$, where $\mathcal{L}$ is an invertible $\mathcal{O}_Y$-module satisfying $N(\mathcal{L}) \cong \mathcal{O}_X$, and φ is a specific choice of isomorphism $\varphi : N(\mathcal{L}) \xrightarrow{\sim} \mathcal{O}_X$. We define an *isomorphism* $\psi : (\mathcal{L}, \varphi) \xrightarrow{\sim} (\mathcal{L}', \varphi')$ between such pairs to be an isomorphism of $\mathcal{O}_Y$-modules $\psi : \mathcal{L} \to \mathcal{L}'$ satisfying $\varphi' \circ N(\psi) = \varphi$. The *norm class group* is the group $\mathrm{NormCl}\,(Y/X)$ of isomorphism classes of such pairs, with the tensor product as the group operation.

There are two homomorphisms

$$\begin{array}{rcl} \mathcal{O}_X(X)^\times & \longrightarrow & \mathrm{NormCl}(Y/X) \\ u & \longmapsto & [(\mathcal{O}_Y, s \mapsto us)] \end{array} \qquad \text{and} \qquad \begin{array}{rcl} \mathrm{NormCl}(Y/X) & \longrightarrow & \mathrm{Pic}(Y). \\ [(\mathcal{L}, \varphi)] & \longmapsto & [\mathcal{L}] \end{array}$$

associated to $\mathrm{NormCl}\,(Y/X)$. It is easy to see that they fit into an exact sequence

$$\mathcal{O}_Y(Y)^\times \xrightarrow{\mathbf{Norm}} \mathcal{O}_X(X)^\times \longrightarrow \mathrm{NormCl}\,(Y/X) \longrightarrow \mathrm{Pic}(Y) \xrightarrow{\mathbf{Norm}} \mathrm{Pic}(X). \tag{3.6}$$

We will now prove Theorem B by comparing this sequence with (3.4).

Theorem 3.6. *For a finite locally free morphism $f : Y \to X$, there is an isomorphism*

$$\mathrm{NormCl}\,(Y/X) \xrightarrow{\sim} H^1(X, R^1_{Y/X}(\mathbb{G}_{m,Y}))$$

making the following diagram commute:

$$\begin{array}{ccccc} \mathcal{O}_X(X)^\times & \longrightarrow & \mathrm{NormCl}(Y/X) & \longrightarrow & \mathrm{Pic}(Y) \\ \| & & \downarrow & & \downarrow{\scriptstyle \sim} \\ \mathcal{O}_X(X)^\times & \longrightarrow & H^1(X, R^1_{Y/X}(\mathbb{G}_{m,Y})) & \longrightarrow & H^1(X, R_{Y/X}(\mathbb{G}_{m,X})) \end{array} \tag{3.7}$$

Proof. It is enough to construct a map $\mathrm{NormCl}\,(Y/X) \to H^1(X, R^1_{Y/X}(\mathbb{G}_{m,Y}))$ making the diagram commute, as (3.4) and (3.6) imply that it is an isomorphism by the Five Lemma. We will construct this map using Čech cohomology.

Since $\mathbf{Norm} : R_{Y/X}(\mathbb{G}_{m,Y}) \to \mathbb{G}_{m,X}$ is surjective, there exists for every $u \in \mathcal{O}_X(X)^\times$ an fppf cover $(U_i)_i$ of X and elements $v_i \in R_{Y/X}(\mathbb{G}_{m,Y})(U_i)$ satisfying $\mathbf{Norm}\,(v_i) = u|_{U_i}$.

The connecting morphism $\mathcal{O}_X(X)^\times \to \check{H}^1(X, R^1_{Y/X}(\mathbb{G}_{m,Y}))$ in the long exact sequence for Čech cohomology sends u to the class of the 1-cocycle $v_i v_j^{-1} \in R^1_{Y/X}(\mathbb{G}_{m,Y})(U_{ij})$.

Now, let $\mathcal{L}$ be an invertible $\mathcal{O}_Y$-module with an isomorphism $\varphi : N(\mathcal{L}) \xrightarrow{\sim} \mathcal{O}_X$. We define a 1-cocycle for $R^1_{Y/X}(\mathbb{G}_{m,Y})$ as follows. By Proposition 3.4, there exists a Zariski open cover $(U_i)_i$ of X with isomorphisms $\eta_i : \mathcal{L}|_{U_i \times_X Y} \xrightarrow{\sim} \mathcal{O}_{U_i \times_X Y}$ for all i. As before, define the element $\omega_{ij} \in R_{Y/X}(\mathbb{G}_{m,Y})(U_{ij})$ corresponding to $\eta_i \circ \eta_j^{-1}$ for all i and j. Consider for every i the element $u_i \in \mathcal{O}_X(U_i)$ such that $N(\eta_i) \circ \varphi^{-1} : \mathcal{O}_{U_i} \xrightarrow{\sim} \mathcal{O}_{U_i}$ is multiplication by u_i. Note that this gives

$$\mathbf{Norm}\,(\omega_{ij}) \;=\; u_i u_j^{-1}.$$

Since $\mathbf{Norm} : R_{Y/X}(\mathbb{G}_{m,Y}) \to \mathbb{G}_{m,X}$ is surjective, there exists for every i an fppf cover of U_i with $R^1_{Y/X}(\mathbb{G}_{m,Y})$-sections mapping to u_i. By refining $(U_i)_i$, we may assume that each of these covers consists of a single fppf morphism $V_i \to U_i$ with $v_i \in R_{Y/X}(\mathbb{G}_{m,Y})(V_i)$ satisfying $\mathbf{Norm}\,(v_i) = u_i|_{V_i}$, for ease of notation. Then for all i and j, the element

$$\omega'_{ij} \;\coloneqq\; v_i^{-1} v_j \cdot \omega_{ij} \in R_{Y/X}(\mathbb{G}_{m,Y})(V_{ij})$$

satisfies the cocycle condition and has norm 1. Hence, $(\omega'_{ij})_{i,j}$ defines an element of $\check{H}^1(X, R^1_{Y/X}(\mathbb{G}_{m,Y}))$. We define this to be the image of $[(\mathcal{L}, \varphi)] \in \mathrm{NormCl}(Y/X)$ under the map

$$\mathrm{NormCl}\,(Y/X) \to \check{H}^1(X, R^1_{Y/X}(\mathbb{G}_{m,Y})).$$

Clearly, different choices of covers yield cohomologous cocycles and this map is a homomorphism. Since $(v_i^{-1} v_j)_{i,j}$ is a coboundary for $R_{Y/X}(\mathbb{G}_{m,Y})$, the class of $(\omega'_{ij})_{i,j}$ in $\check{H}^1(X, R_{Y/X}(\mathbb{G}_{m,Y}))$ is the same as the class of $(\omega_{ij})_{i,j}$, which corresponds to $[\mathcal{L}]$ in $\mathrm{Pic}(Y)$. This means that the right square of (3.7) commutes. From our description of the map $\mathcal{O}_X(X)^\times \to \check{H}^1(X, R^1_{Y/X}(\mathbb{G}_{m,Y}))$, it is also clear that the left square commutes. □

3.3 Relation with quadratic forms

We will now see how a class $[(\mathcal{L}, \varphi)] \in \mathrm{NormCl}\,(Y/X)$ can be associated to a quadratic form up to equivalence. First in the generality of a finite locally free morphism $Y \to X$ of rank 2, and then we will relate this to Chapter 2 in the case $X = \operatorname{Spec} \mathbb{Z}$.

Proposition 3.7. *Let $\mathcal{L}$ be an invertible $\mathcal{O}_Y$-module. There is a unique morpism of sheaves of sets $\nu : f_*\mathcal{L} \to N(\mathcal{L})$ such that for every open $U \subseteq X$ and isomorphism $\eta : \mathcal{L}|_{U \times_X Y} \xrightarrow{\sim} \mathcal{O}_{U_i \times_X Y}$, the following diagram commutes:*

$$\begin{array}{ccc} (f_*\mathcal{L})|_U & \xrightarrow{\;\nu\;} & N(\mathcal{L})|_U \\ \Big\downarrow{\scriptstyle \eta} & & \Big\downarrow{\scriptstyle N(\eta)} \\ (f_*\mathcal{O}_Y)|_U & \xrightarrow{\;\mathbf{norm}\;} & \mathcal{O}_U. \end{array}$$

Proof. Uniqueness is clear. The existence of such ν is equivalent to the equality

$$N(\eta_i)^{-1} \circ \mathbf{norm} \circ f_*\eta_i \;=\; N(\eta_j)^{-1} \circ \mathbf{norm} \circ f_*\eta_j$$

holding for all i, j, with $(U_i)_i$ and $\eta_i : \mathcal{L}|_{U_i \times_X Y} \xrightarrow{\sim} \mathcal{O}_{U_i \times_X Y}$ as in Proposition 3.4. But this is equivalent to $\mathbf{norm} \circ f_*(\eta_i \circ \eta_j^{-1}) = N(\eta_i \circ \eta_j^{-1}) \circ \mathbf{norm}$ which follows from (3.5). □

Remark 3.8. The morphism $\nu : f_*\mathcal{L} \to N(\mathcal{L})$ is what is called the *universal normic polynomial law* of $\mathcal{L}$ in [GNR24, §3.1].

Assume that $f : Y \to X$ is finite locally free of rank 2. Suppose that, locally on an open affine $U \subseteq X$, the $\mathcal{O}_U$-module $(f_*\mathcal{O}_Y)|_U$ has a basis $b_1, b_2 \in (f_*\mathcal{O}_Y)(U)$. Recall from (3.2) that the norm is given by

$$\mathbf{norm}(xb_1 + yb_2) \;=\; Q_0(x, y)$$

for a quadratic form $Q_0 \in \mathcal{O}_X(U)[x, y]$. Now, if we associate to b_1, b_2 the dual basis $b_1^\vee, b_2^\vee \in (f_*\mathcal{O}_Y)^\vee(U)$ of the dual $\mathcal{O}_U$-module $(f_*\mathcal{O}_Y)^\vee|_U$, then $Q_0(b_1^\vee, b_2^\vee)$ is an element of the symmetric algebra $\mathrm{Sym}^2\left((f_*\mathcal{O}_Y)^\vee\right)|_U$. More is true: if $(\mathcal{L}, \varphi)$ is a pair of an invertible $\mathcal{O}_Y$-module and an isomorphism $\varphi : N(\mathcal{L}) \xrightarrow{\sim} \mathcal{O}_X$ and $\eta : \mathcal{L}_U \xrightarrow{\sim} \mathcal{O}_{U\times_X Y}$ is a trivialization of $\mathcal{L}$ on U, then we obtain an element

$$\varphi \circ N(\eta)^{-1} \circ Q_0\left(b_1^\vee \circ f_*\eta, b_2^\vee \circ f_*\eta\right) \in \mathrm{Sym}^2\left((f_*\mathcal{L})^\vee\right)|_U.$$

By Proposition 3.2, these glue to a global form

$$Q_{(\mathcal{L},\varphi)} \in \mathrm{Sym}^2\left((f_*\mathcal{L})^\vee\right).$$

It is primitive, in the sense that it represents 1 locally everywhere. Hence, it is an example of what is called a *primitive binary quadratic form* over X in [Woo11], i.e. a locally free $\mathcal{O}_X$-module $\mathcal{V}$ of rank 2 with a global section $Q \in \mathrm{Sym}^2(\mathcal{V})$. For two pairs $(\mathcal{L}, \varphi)$ and $(\mathcal{L}', \varphi')$ and an isomorphism $\psi : \mathcal{L} \xrightarrow{\sim} \mathcal{L}'$, the induced isomorphism

$$\mathrm{Sym}^2\left((f_*\psi)^\vee\right) : \mathrm{Sym}^2\left((f_*\mathcal{L}')^\vee\right) \xrightarrow{\sim} \mathrm{Sym}^2\left((f_*\mathcal{L})^\vee\right)$$

maps $Q_{(\mathcal{L}',\varphi')}$ to $Q_{(\mathcal{L},\varphi)}$ if and only if ψ satisfies $\varphi = \varphi' \circ N(\psi)$. Note that this does not mean that $(\mathcal{L}, \varphi)$ and $(\mathcal{L}', \varphi')$ are isomorphic when there exists an isomorphism of $\mathcal{O}_X$-modules $\psi : f_*\mathcal{L} \xrightarrow{\sim} f_*\mathcal{L}'$ satisfying $\mathrm{Sym}^2\left(\psi^\vee\right)\left(Q_{(\mathcal{L},\varphi)}\right) = Q_{(\mathcal{L}',\varphi')}$; over $\mathbb{Z}$, this is the difference between $\mathrm{GL}_2(\mathbb{Z})$-equivalence and $\mathrm{SL}_2(\mathbb{Z})$-equivalence.

Take $X = \operatorname{Spec}\mathbb{Z}$. Since any finite locally free $\mathbb{Z}$-module is free, we have $Y = \operatorname{Spec} B$ for a ring B that is free of degree 2 over $\mathbb{Z}$. Such a ring is called a *quadratic ring*. For every integer $\Delta \equiv 0, 1 \mod 4$ there is a quadratic ring

$$S(\Delta) = \mathbb{Z}[\alpha]/\left(\alpha^2 - \varepsilon\alpha - \tfrac{\Delta-\varepsilon}{4}\right)$$

with $\varepsilon \in \{0, 1\}$ such that $\Delta \equiv \varepsilon \mod 4$. Every quadratic ring is isomorphic to $S(\Delta)$ for exactly one Δ. See [Bha04, §3.1].

Fix a non-zero $\Delta \equiv 0, 1 \mod 4$ and let $B = S(\Delta)$. Note that, with respect to the basis $1, \alpha$, we have

$$\begin{aligned}\mathbf{norm}(x + y\alpha) \;&=\; (x + y\alpha)(x + \varepsilon y - y\alpha) \;=\; x^2 + \varepsilon xy - \frac{\Delta-\varepsilon}{4}y^2\\ (x + y\alpha)(z + w\alpha) \;&=\; xz - \frac{\Delta-\varepsilon}{4}yw + (xw + yz + \varepsilon yw)\alpha.\end{aligned}$$

The group scheme $R^1_{B/\mathbb{Z}}(\mathbb{G}_{m,B})$ is therefore exactly the group scheme R^1_Δ defined in §2.1.

Let $(\mathcal{L}, \varphi)$ be a pair of an invertible B-module $\mathcal{L}$ and an isomorphism $\varphi : N(\mathcal{L}) \xrightarrow{\sim} \mathbb{Z}$. As every finite locally free $\mathbb{Z}$-module is free, we obtain from $Q_{(\mathcal{L},\varphi)} \in \mathrm{Sym}^2\left((f_*\mathcal{L})^\vee\right)$ a

form $Q \in \mathcal{F}_\Delta$ by pick a basis b_1, b_2 for $\mathcal{L}$, but the class of $[Q]$ in $\mathcal{F}_\Delta/\mathrm{SL}_2(\mathbb{Z})$ depends on the choice of basis. However, if $B_1, B_2 \in \mathbb{Z}[x,y,z,w]$ are the bilinear forms satisfying

$$(xb_1 + yb_2)(z + w\alpha) \;=\; B_1(x,y,z,w)b_1 + B_2(x,y,z,w)b_2$$

in $f_*\mathcal{L} \otimes_{\mathbb{Z}} \mathbb{Z}[x,y,z,w]$, then we do get a unique form $Q \in \mathcal{F}_\Delta$ up to $\mathrm{SL}_2(\mathbb{Z})$-equivalence if we impose that B_1, B_2 define a Gauss composition $T_Q \times R^1_\Delta \to T_Q$. By going through the proof of Theorem 3.6, one finds that the class of the R^1_Δ-torsor T_Q in $H^1(\operatorname{Spec}\mathbb{Z}, R^1_\Delta)$ coincides with the image of $[(\mathcal{L}, \varphi)]$ under the isomorphism of Theorem 3.6.

3.4 Relation with the narrow class group

We restrict to the case that $f : Y \to X$ is the morphism $\operatorname{Spec} B \to \operatorname{Spec} A$ corresponding to an extension of integral domains $A \subseteq B$. Let $K \subseteq L$ be their fields of fractions. In this case, the norm morphism is given by the field norm $N_{L/K} : L \to K$ and every invertible B-module is isomorphic to an invertible B-ideal $I \subseteq L$, whose norm $N(I)$ is the invertible A-module $N_{L/K}(I)$. An isomorphism $N(I) \xrightarrow{\sim} A$ is simply a choice of generator $x \in K^\times$ of $N(I)$. Thus, the norm class group $\mathrm{NormCl}\,(B/A)$ can be described as follows. Let $\mathcal{NI}_B$ be the group of *normed ideals* of A under multiplication, i.e. pairs (I, x) with I an invertible B-ideal and $x \in K^\times$ a generator of its norm. Let $\mathcal{NP}_B = \{((\alpha), N_{L/K}(\alpha)) : \alpha \in L^\times\}$ be the subgroup of *principal normed ideals*. Then $\mathrm{NormCl}\,(B/A)$ is their quotient, i.e. there is a short exact sequence

$$0 \longrightarrow \mathcal{NP}_B \longrightarrow \mathcal{NI}_B \longrightarrow \mathrm{NormCl}\,(B/A) \longrightarrow 0. \tag{3.8}$$

Note that $\mathcal{NP}_B$ itself fits into a short exact sequence

$$0 \longrightarrow B^{\mathrm{Norm}=1} \longrightarrow L^\times \longrightarrow \mathcal{NP}_B \longrightarrow 0. \tag{3.9}$$

This is the description of the norm class group that we will use in Chapter 4.

For now, take $A = \mathbb{Z}$. Then for every invertible B-ideal I, the norm ideal $N(I)$ has two possible generators, a positive and a negative one. For a principal ideal $I = (\alpha)$, these are $\pm N_{L/K}(\alpha)$, and the normed ideal $(I, N_{L/K}(\alpha))$ is principal if and only if α can be chosen such that $N_{L/K}(\alpha)$ is positive. In particular, when B is a quadratic ring, the notion of normed ideals is equivalent to the notion of oriented ideals used in [Bha04].

We will now compare the norm class group with the narrow class group. Recall that the *narrow class group* $\mathrm{Cl}^+(B)$ is the group of invertible B-ideals modulo the principal B-ideals generated by a *totally positive* element, i.e. an element $\alpha \in L^\times$ such that $\sigma(\alpha)$ is positive for every real embedding $\sigma : K \to \mathbb{R}$. Since the field norm $N_{L/\mathbb{Q}}$ is given by

$$N_{L/\mathbb{Q}}(\alpha) \;=\; \prod_{\sigma : L \to \mathbb{C}} \sigma(\alpha)$$

and the complex embeddings come in conjugate pairs $\sigma, \bar\sigma$ satisfying $\sigma(\alpha)\bar\sigma(\alpha) > 0$, we have

$$\operatorname{sign}(N_{L/\mathbb{Q}}(\alpha)) \;=\; \prod_{\sigma : L \to \mathbb{R}} \operatorname{sign}(\sigma(\alpha)).$$

In particular, a B-ideal that is generated by a totally positive element, is generated by an element of positive norm. The converse holds if K has at most two real embeddings, since an ideal generated by a totally negative element is also generated by a totally positive element. We obtain the following result.

Theorem 3.9. *Let B be an order in a number field L. Associating to an invertible B-ideal I the pair (I, x) with x the positive generator of $N(I)$ induces a homomorphism*

$$\mathrm{Cl}^+(B) \longrightarrow \mathrm{NormCl}(B/\mathbb{Z}) \cong H^1(\operatorname{Spec}\mathbb{Z}, R^1_{B/\mathbb{Z}}(\mathbb{G}_{m,B})) \tag{3.10}$$

through which the canonical surjection $\mathrm{Cl}^+(B) \twoheadrightarrow \mathrm{Cl}(B)$ factors.

- *If B has at least one real embedding, then it is surjective.*
- *If B has one or two real embeddings, then it is an isomorphism.*
- *If B has zero real embeddings, it is injective and we obtain an isomorphism*

  $$\mathrm{Cl}^+(B) \oplus \{\pm 1\} \xrightarrow{\sim} \mathrm{NormCl}(B/\mathbb{Z})$$

  by sending -1 to the class of $(B, -1)$.

Proof. The fact that the homomorphism is well-defined follows from the observation that a B-ideal generated by a totally positive element is generated by an element of positive norm. The converse holds when L has at most two real embeddings, which makes it injective in this case.

If L has at least one real embedding, then it contains an element $\alpha \in L^\times$ of negative norm, and a class $[(I, x)] \in \mathrm{NormCl(B/\mathbb{Z})}$ is the image of $[I] \in \mathrm{Cl}^+_K$ if $x > 0$ and the image of $[\alpha I]$ if $x < 0$.

If L has no real embeddings, then a class $[(I, x)] \in \mathrm{NormCl}(B/\mathbb{Z})$ is the image of the homomorphism if and only if $x > 0$, as all elements of $L^\times$ have positive norm. The stated isomorphism follows. □

When L is a quadratic number field of discriminant Δ, Theorems 2.5 and 3.9 together imply the classical result that Cl^+_K is naturally isomorphic to the group of forms $\mathcal{F}_\Delta/\mathrm{SL}_2(\mathbb{Z})$ under composition if $\Delta > 0$, and the group of positive definite forms if $\Delta < 0$.

Remark 3.10. Note that this means that the group $H^1(\operatorname{Spec}\mathbb{Z}, R^1_{B/\mathbb{Z}}(\mathbb{G}_{m,B}))$ gleans at least some information about the narrow class group $\mathrm{Cl}(B)^+$, without having to treat the places at infinity separately. Or even all of the information if L has at most two real embeddings. If L has more than two real embeddings, this information is relatively minimal, as $\mathrm{NormCl}(B/\mathbb{Z}) \twoheadrightarrow \mathrm{Cl}_K$ is at most a double cover.

4 The 4-torsion of the norm class group

This chapter presents an application of the theory of the norm class group to the problem of finding the 2- and 4-torsion of the class group for a quadratic extension of global fields.

The 2-torsion of the class group of a quadratic number field K of discriminant Δ is described by *genus theory*. In §4.1, we will apply the Galois cohomological argument for genus theory in [Lan80, Lem. 13.4.1] to find $\mathrm{NormCl}\,(B/A)[2]$ for a quadratic extension of Dedekind domains B/A where A is a PID.

In §4.2, we move up to the 4-torsion. The 4-rank of the narrow class group of a quadratic number field was described by Rédei [Réd34] as the difference between its 2-rank and the rank of a certain square matrix over $\mathbb{F}_2$. We will prove Theorem C, which is a similar statement for norm class groups of quadratic extensions of global fields. The proof of Rédei using genus fields has been generalized to quadratic extensions of $\mathbb{F}_q(t)$ with q odd [Wit09] and quadratic extensions of a number field with odd class number [Qin09]. In the spirit of this thesis, the proof of Theorem C is geometric in nature, relying on the Hochschild–Serre spectral sequence.

4.1 Genus theory

For this entire chapter, we fix the following notation. Let A be a principal ideal domain with field of fractions K. Let L/K be a quadratic field extension and B the integral closure of A in L. Hence, B is a Dedekind domain with field of fractions L and, as A is a PID, it is free of rank 2 as an A-module. Let $p_1, \ldots, p_t \in A$ be generators of the prime ideals of A at which B/A is ramified. Write

$$\widetilde{A} = A[\tfrac{1}{p_1}, \ldots, \tfrac{1}{p_t}] \qquad \text{and} \qquad \widetilde{B} = B \otimes_A \widetilde{A} = B[\tfrac{1}{p_1}, \ldots, \tfrac{1}{p_t}]. \tag{4.1}$$

Note that $\operatorname{Spec} \widetilde{A}$ is the largest open subscheme of $\operatorname{Spec} A$ where the map $\operatorname{Spec} B \to \operatorname{Spec} A$ is étale, as in [Mil80, Prop. I.3.8]. By unique factorization, the unit group of $\widetilde{A}$ factors as

$$\widetilde{A}^\times = A^\times \times p_1^{\mathbb{Z}} \times \cdots \times p_t^{\mathbb{Z}}.$$

As B/A is quadratic and ramified at p_i, there is a unique prime ideal $\mathfrak{p}_i$ of B lying above p_i, for every i.

For a quadratic number field F, genus theory states that the 2-torsion part of the narrow class group Cl_F^+ is generated by the classes of the ramified primes modulo a single relation. One proof uses Galois cohomology, exploiting the fact that the 2-torsion elements of Cl_F^+ are those classes fixed by $\mathrm{Gal}(F/\mathbb{Q})$ [Lan80, Lem. 13.4.1]. These are called *ambiguous classes*. The use of the narrow class group ensures that every ambiguous class contains an *ambiguous ideal*, i.e. an $\mathcal{O}_F$-ideal that is fixed by the action of $\mathrm{Gal}(F/\mathbb{Q})$. The same is not true for the wide class group: for example, $\mathrm{Cl}_{\mathbb{Q}(\sqrt{34})}$ has order 2 while all ambiguous ideals are principal.

The following lemma shows that an analogue does hold for the norm class group $\mathrm{NormCl}\,(B/A)$. If one defines *ambiguous normed ideals* to be pairs $(I, x) \in \mathcal{NI}_B$ that are fixed by $\mathrm{Gal}(L/K)$ and *ambiguous classes* to be classes in $\mathrm{NormCl}\,(B/A) = \mathcal{NI}_B/\mathcal{NP}_B$ that are fixed by $\mathrm{Gal}(L/K)$, then every ambiguous class contains an ambiguous normed ideal. This and more is proven in the following lemma, as normed ideals (I, x) with I a product of the ramified primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ are ambiguous.

Lemma 4.1. *With notation as above, there is an isomorphism*

$$\begin{aligned} \widetilde{A}^\times/N_{L/K}(\widetilde{B}^\times) &\xrightarrow{\sim} \operatorname{NormCl}(B/A)[2]. \\ [x] &\longmapsto \left[\left(\prod_{i=1}^{t}\mathfrak{p}_i^{\operatorname{ord}_{p_i}(x)}, x\right)\right] \end{aligned}$$

Proof. First, we show that the map $\widetilde{A}^\times \to \operatorname{NormCl}(B/A)$ is surjective. As L/K is a quadratic extension, $G = \operatorname{Gal}(L/K)$ is generated by an element σ of order 2. Since it acts on $\operatorname{NormCl}(B/A)$ by inversion, we have $\operatorname{NormCl}(B/A)^G = \operatorname{NormCl}(B/A)[2]$. The long exact sequence of Galois cohomology given by (3.8) is

$$0 \to \mathcal{NP}_B^G \longrightarrow \mathcal{NI}_B^G \longrightarrow \operatorname{NormCl}(B/A)^G \longrightarrow H^1(G, \mathcal{NP}_B) \longrightarrow H^1(G, \mathcal{NI}_B). \tag{4.2}$$

We will show that the last map is injective. As G is cyclic of order 2, the first cohomology group is the kernel of the norm $x \mapsto x\sigma(x)$ modulo the image of the difference map $x \mapsto \sigma(x)x^{-1}$. Suppose we have $[((\alpha), N_{L/K}(\alpha))] \in \ker(H^1(G, \mathcal{NP}_B) \to H^1(G, \mathcal{NI}_B))$ for a pair $((\alpha), N_{L/K}(\alpha))$ in the kernel of the norm on $\mathcal{NP}_B$. Then this pair is equal to $(\sigma(I), x)(I^{-1}, x^{-1}) = (\sigma(I)I^{-1}, 1)$ for some $(I, x) \in \mathcal{NI}_B$, which gives $N_{L/K}(\alpha) = 1$. By Hilbert 90, we therefore have $\alpha = \sigma(\beta)\beta^{-1}$ for some $\beta \in L^\times$, which means that $((\alpha), N_{L/K}(\alpha)) = ((\sigma(\beta)\beta^{-1}), 1)$ is in the image of the difference on $\mathcal{NP}_B$. We conclude that the last map of (4.2) is injective. We obtain a short exact sequence

$$0 \longrightarrow \mathcal{NP}_B^G \longrightarrow \mathcal{NI}_B^G \longrightarrow \operatorname{NormCl}(B/A)^G \longrightarrow 0. \tag{4.3}$$

A Galois invariant B-ideal is the product of an A-ideal with a collection of ramified primes, as the split primes in its prime ideal factorization must come in conjugate pairs and the inert primes are already A-ideals. Since A-ideals are principal, this means that every element of $\mathcal{NI}_B^G$ is equivalent to a pair of the form $(\prod_i \mathfrak{p}_i^{r_i}, x)$ in $\operatorname{NormCl}(B/A)$. The generator x of $N_{L/K}\prod_i \mathfrak{p}_i^{r_i} = (\prod_i p_i^{r_i})$ satisfies $\operatorname{ord}_{p_i}(x) = r_i$. This proves surjectivity.

It remains to show that the kernel of the map $\widetilde{A}^\times \to \operatorname{NormCl}(B/A)$ is the image of the norm $\widetilde{B}^\times \to \widetilde{A}^\times$. For $\alpha \in \widetilde{B}^\times$ we have $\operatorname{ord}_{\mathfrak{p}}(\alpha) = 0$ whenever $\mathfrak{p}$ is unramified, which means that the prime ideal factorization of (α) is

$$(\alpha) = \prod_{\mathfrak{p}\text{ prime}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(\alpha)} = \prod_{i=1}^{t} \mathfrak{p}_{\mathfrak{i}}^{\operatorname{ord}_{p_i}(N_{L/K}(\alpha))}.$$

This shows that the image of the norm $\widetilde{B}^\times \to \widetilde{A}^\times$ is contained in the kernel of the map $\widetilde{A}^\times \to \operatorname{NormCl}(B/A)$. Conversely, if $x \in \widetilde{A}^\times$ satisfies

$$\left(\prod_i \mathfrak{p}_i^{\operatorname{ord}_{p_i}(x)}, x\right) = ((\alpha), N_{L/K}(\alpha))$$

for some $\alpha \in L^\times$, then we have $x = N_{L/K}(\alpha)$ and from

$$\operatorname{ord}_{\mathfrak{p}}(\alpha) = \operatorname{ord}_{\mathfrak{p}}\left(\prod_i \mathfrak{p}_i^{\operatorname{ord}_{p_i}(x)}\right) = 0 \qquad \text{for } \mathfrak{p} \text{ unramified}$$

it follows that α is in $\widetilde{B}^\times$. This concludes the proof. □

Thus, $\mathrm{NormCl}(B/A)[2]$ is generated by the classes of $(\mathfrak{p}_i, p_i)$ for $i = 1, \ldots, t$ together with the classes of (B, u) for $u \in A^\times/(A^\times)^2$, and all relations between these classes come from norms of elements of $\widetilde{B}^\times$. The next theorem shows that the number of these relations is equal to the order of $B^{\mathrm{Norm}=1}/(B^{\mathrm{Norm}=1})^2$. When $A = \mathbb{Z}$ and $L/\mathbb{Q}$ is real quadratic, $\mathbb{Z}^\times/(\mathbb{Z}^\times)^2$ is generated by -1 and $\mathcal{O}_L^{\mathrm{Norm}=1}/(\mathcal{O}_L^{\mathrm{Norm}=1})^2$ is generated by -1 together with either a fundamental unit of norm 1 or the square of a fundamental unit of norm -1. Hence, in this case, $\mathrm{NormCl}\,(B/A)$ is generated by the classes of the ramified primes modulo a single relation. This is independent of the norm of the fundamental unit. The following theorem can therefore be seen as a generalization of genus theory.

Theorem 4.2. *Let B/A be a quadratic extension of Dedekind domains with A a PID. Suppose this extension is ramified at t prime ideals. Then we have*

$$\#\mathrm{NormCl}\,(B/A)[2] \;=\; \frac{2^t \cdot [A^\times : (A^\times)^2]}{[B^{\mathrm{Norm}=1} : (B^{\mathrm{Norm}=1})^2]}.$$

Proof. We use the same notation as above and write $G = \mathrm{Gal}(L/K)$. Define the subgroup $\mathcal{NP}_A = \{((x), x^2) : x \in K^\times\}$ of $\mathcal{NP}_B^G$. Then (4.3) gives a short exact sequence

$$0 \longrightarrow \mathcal{NP}_B^G/\mathcal{NP}_A \longrightarrow \mathcal{NI}_B^G/\mathcal{NP}_A \longrightarrow \mathrm{NormCl}\,(B/A)^G \longrightarrow 0 \tag{4.4}$$

and the long exact sequence of Galois cohomology coming from the short exact sequence (3.9) is

$$0 \longrightarrow (B^{\mathrm{Norm}=1})^G \longrightarrow K^\times \longrightarrow \mathcal{NP}_B^G \longrightarrow H^1(G, B^{\mathrm{Norm}=1}) \longrightarrow H^1(G, L^\times).$$

The cokernel of the map $K^\times \to \mathcal{NP}_B^G$ is exactly $\mathcal{NP}_B^G/\mathcal{NP}_A$ and we have $H^1(G, L^\times) = 0$ by Hilbert 90. We therefore obtain

$$\mathcal{NP}_B^G/\mathcal{NP}_A \;\cong\; H^1\left(G, B^{\mathrm{Norm}=1}\right) \;=\; B^{\mathrm{Norm}=1}/\left(B^{\mathrm{Norm}=1}\right)^2. \tag{4.5}$$

Note that the map $\mathcal{NI}_B^G \to (\mathbb{Z}/2\mathbb{Z})^t$ given by $(I, x) \mapsto (\mathrm{ord}_{p_i}(x) \mod 2)_i$ is surjective and its kernel contains $\mathcal{NP}_A$. We will show that the induced map $\mathcal{NI}_B^G/\mathcal{NP}_A \to (\mathbb{Z}/2\mathbb{Z})^t$ fits into a short exact sequence

$$0 \longrightarrow A^\times/(A^\times)^2 \longrightarrow \mathcal{NI}_B^G/\mathcal{NP}_A \longrightarrow (\mathbb{Z}/2\mathbb{Z})^t \longrightarrow 0. \tag{4.6}$$

As discussed in the proof of Lemma 4.1, every Galois-invariant ideal of B is the product of an A-ideal with a collection of ramified primes. Since all A-ideals and all $\mathfrak{p}_i^2 = (p_i)$ are principal generated by an element of $K^\times$, every pair (I, x) in the kernel of $\mathcal{NI}_B^G \to (\mathbb{Z}/2\mathbb{Z})^t$ is of the form $((x), ux^2)$ for some $x \in K^\times$ and $u \in A^\times$. Thus, every class in the kernel of $\mathcal{NI}_B^G/\mathcal{NP}_A \to (\mathbb{Z}/2\mathbb{Z})^t$ is in the image of $A^\times \to \mathcal{NI}_B^G/\mathcal{NP}_A,\ u \mapsto (B, u)$. The kernel of the latter map consists exactly of the squares. This proves the exact sequence (4.6), which together with (4.4) and (4.5) yields the result. □

4.2 The Rédei matrix

Assume now and for the rest of this chapter that L/K is an extension of global fields of characteristic different from 2. A *global field* is a number field or a finite separable extension of $\mathbb{F}_p(t)$ for some prime p, see [Cas67, §II.12]. Let S be the set of primes of K not corresponding to a point in $\mathrm{Spec}\,\widetilde{A}$. When K is a number field, S will always include the archimedean primes. Assume that S is finite and set $s = \#S$.

In this case, Theorem 4.2 can be made even more explicit using the S-Unit Theorem [Cas67, §II.18], which states that $\widetilde{A}^\times$ is the product of the group μ_K of roots of unity of K with a free abelian group of rank $s-1$. It also follows from the S-Unit Theorem that $A^\times$ is the product of μ_K with a free abelian group of rank $s-t-1$, where t is again the number of ramified primes in $\operatorname{Spec} A$. We will consider all 2-torsion groups as $\mathbb{F}_2$-vector spaces and we define the *2-rank*

$$r_2(B/A) \;=\; \dim_{\mathbb{F}_2} \operatorname{NormCl}(B/A)[2].$$

Note that we have $\dim_{\mathbb{F}_2}(\mu_K/\mu_K^2) = \dim_{\mathbb{F}_2}(\mu_K[2]) = 2$ since μ_K is a finite group. Hence, we have $\dim_{\mathbb{F}_2} A^\times/(A^\times)^2 = s-t$ and Theorem 4.2 can be restated as follows.

Corollary 4.3. *With notation as above, we have*

$$r_2(B/A) \;=\; s - \dim_{\mathbb{F}_2}\left(B^{\mathrm{Norm}=1}/(B^{\mathrm{Norm}=1})^2\right).$$

We now turn to the 4-rank

$$r_4(B/A) \;=\; \dim_{\mathbb{F}_2} \operatorname{NormCl}(B/A)[4]/\operatorname{NormCl}(B/A)[2].$$

Computing this 4-rank is the same as computing the 2-torsion of the group

$$\operatorname{NormCl}(B/A)/\operatorname{NormCl}(B/A)[2].$$

This group turns out to be canonically isomorphic to the Picard group $\operatorname{Pic}(\widetilde{B})$.

Lemma 4.4. *For a quadratic extension of Dedekind domains B/A with A a PID, there is a short exact sequence*

$$0 \longrightarrow \operatorname{NormCl}(B/A)[2] \longrightarrow \operatorname{NormCl}(B/A) \longrightarrow \operatorname{Pic}(\widetilde{B}) \longrightarrow 0.$$

Proof. The map $\operatorname{NormCl}(B/A) \to \operatorname{Pic}(\widetilde{B})$ is surjective as the composition of the surjective maps $\operatorname{NormCl}(B/A) \longrightarrow \operatorname{Pic}(B)$ and $\operatorname{Pic}(B) \to \operatorname{Pic}(\widetilde{B})$. It is clear from Lemma 4.1 that $\operatorname{NormCl}(B/A)[2]$ is contained in its kernel. Conversely, an element in its kernel is the class of $((\alpha)\prod_i \mathfrak{p}_i^{s_i}, uN(\alpha)\prod_i p_i^{s_i})$ for some $\alpha \in L^\times$ and $u \in B^\times$, and its square is the class of $((\beta), N_{L/K}(\beta))$ with $\beta = u\alpha^2\prod_i p_i^{s_i}$, which is trivial. □

Remark 4.5. Lemmas 4.1 and 4.4 together imply that the natural map

$$\operatorname{NormCl}(B/A) \;\longrightarrow\; \operatorname{NormCl}(\widetilde{B}/\widetilde{A})$$

is an isomorphism, as it fits into a commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \widetilde{A}^\times/N_{L/K}(\widetilde{B}^\times) & \longrightarrow & \operatorname{NormCl}(B/A) & \longrightarrow & \operatorname{Pic}(\widetilde{B}) \longrightarrow 0 \\
 & & \| & & \downarrow & & \| \\
0 & \longrightarrow & \widetilde{A}^\times/N_{L/K}(\widetilde{B}^\times) & \longrightarrow & \operatorname{NormCl}(\widetilde{B}/\widetilde{A}) & \longrightarrow & \operatorname{Pic}(\widetilde{B}) \longrightarrow 0
\end{array}$$

where the rows are exact.

For the discussion of the 4-torsion of $\mathrm{NormCl}\,(B/A)$, it is essential that the morphism $\operatorname{Spec}\widetilde{B} \to \operatorname{Spec}\widetilde{A}$ is Galois with Galois group $\mathrm{Gal}(L/K)$. Recall that a morphism of schemes $Y \to X$ with a finite group G acting on Y over X is called *Galois* with *Galois group* G if it is faithfully flat and the map

$$\begin{aligned} \psi : \bigsqcup_{\sigma\in G} Y &\longrightarrow Y \times_X Y \\ (\sigma, y) &\longmapsto (y, y\sigma) \end{aligned} \tag{4.7}$$

is an isomorphism [Mil80, Rmk. I.5.4]. In our case, $\widetilde{B}$ has a basis $1, \alpha$ since $\widetilde{A}$ is a PID, and the morphism (4.7) corresponds to the homomorphism

$$\begin{aligned} \widetilde{B} \otimes_{\widetilde{A}} \widetilde{B} &\longrightarrow \widetilde{B} \times \widetilde{B} \\ x \otimes 1 + y \otimes \alpha &\longmapsto (x + y\alpha, x + y\sigma(\alpha)) \end{aligned} \tag{4.8}$$

where σ is the generator of $G = \mathrm{Gal}(L/K)$. With respect to the obvious bases, this is a $\widetilde{B}$-linear map given by a 2×2-matrix of determinant $\sigma(\alpha) - \alpha$. By definition of $\widetilde{B}$, the discrimant $\Delta = (\sigma(\alpha) - \alpha)^2$ is a unit in $\widetilde{B}$, which means that $\sigma(\alpha) - \alpha$ is a unit in $\widetilde{B}$. We conclude that (4.8) is an isomorphism and that $\operatorname{Spec}\widetilde{B} \to \operatorname{Spec}\widetilde{A}$ is Galois.

We will now prove the analogue of Rédei theory using the Hochschild-Serre spectral sequence [Mil80, Thm. III.2.20 and Rmk. III.2.21]. For a finite Galois morphism of schemes $Y \to X$ with Galois group G and a sheaf $\mathcal{F}$ (for the fppf topology) on X, this is a spectral sequence whose second page is $H^p(G, H^q(Y, \mathcal{F}))$ and which converges to $H^{p+q}(X, \mathcal{F})$, i.e.

$$H^p(G, H^q(Y, \mathcal{F})) \implies H^{p+q}(X, \mathcal{F}).$$

As with any spectral sequence, the second page provides a five-term exact sequence of low degree terms

$$0 \longrightarrow H^1(G, \mathcal{F}(X)) \longrightarrow H^1(X, \mathcal{F}) \longrightarrow H^1(Y, \mathcal{F})^G \longrightarrow H^2(G, \mathcal{F}(X)) \longrightarrow H^2(X, \mathcal{F}).$$

We will apply this to the Galois morphism $\operatorname{Spec}\widetilde{B} \to \operatorname{Spec}\widetilde{A}$ to prove the following theorem.

Theorem 4.6. *Let A be a PID with field of fractions K. Let L/K be a quadratic extension and let B be the integral closure of A in L. Define $\widetilde{A}$ and $\widetilde{B}$ as in* (4.1)*. Assume that K and L are global fields with* $\mathrm{char}(K) \neq 2$*. Let S be the set of places of K not corresponding to a point in* $\operatorname{Spec}\widetilde{A}$*. For every $v \in S$, there is an injective homomorphism*

$$\theta_v : K_v^\times / N_{L\otimes_K K_v/K_v}(L \otimes_K K_v)^\times \longrightarrow \mathbb{Z}/2\mathbb{Z}.$$

The 4-torsion group $\mathrm{NormCl}\,(B/A)[4]/\mathrm{NormCl}\,(B/A)[2]$ *is canonically isomorphic to the kernel of the map*

$$\prod_{v\in S} \theta_v : \widetilde{A}^\times / N_{L/K}(\widetilde{B}^\times) \longrightarrow (\mathbb{Z}/2\mathbb{Z})^S \tag{4.9}$$

Proof. As noted, the morphism of schemes $\operatorname{Spec}\widetilde{B} \to \operatorname{Spec}\widetilde{A}$ is Galois with Galois group $G = \mathrm{Gal}(L/K)$ of order 2. Hence, we have the Hochschild–Serre spectral sequence

$$H^p(G, H^q(\widetilde{B}, \mathbb{G}_{m,\widetilde{A}})) \implies H^{p+q}(\widetilde{A}, \mathbb{G}_{m,\widetilde{A}}).$$

Its five-term exact of low-degree terms is

$$0 \longrightarrow H^1(G, \widetilde{B}^\times) \longrightarrow \mathrm{Pic}(\widetilde{A}) \longrightarrow \mathrm{Pic}(\widetilde{B})^G \longrightarrow H^2(G, \widetilde{B}^\times) \longrightarrow \mathrm{Br}(\widetilde{A})$$

where $\mathrm{Br}(\widetilde{A}) \coloneqq H^2(\widetilde{A}, \mathbb{G}_{m,\widetilde{A}})$ is the cohomological Brauer group [Mil80, p. 147]. We have $\mathrm{Pic}(\widetilde{A}) = 0$ as $\widetilde{A}$ is a PID and $H^2(G, \widetilde{B}^\times) = \widetilde{A}^\times / N_{L/K}(\widetilde{B}^\times)$ as G is cyclic. We also consider the Hochschild-Serre spectral sequence

$$H^p(G, H^q(L \otimes_K K_v, \mathbb{G}_m)) \implies H^{p+q}(K_v, \mathbb{G}_m)$$

for every place $v \in S$. Since $\mathrm{Pic}(L \otimes_K K_v) = 0$, the last three terms in the five-term exact sequence are

$$0 \longrightarrow K_v^\times / N_{L \otimes_K K_v}(L \otimes_K K_v)^\times \longrightarrow \mathrm{Br}(K_v).$$

We have an injective map $\mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$ for every $v \in S$ [Ser79, Prop. XIII.3.5] and since $K_v^\times / N_{L \otimes_K K_v}(L \otimes_K K_v)^\times$ is 2-torsion, this gives the injective maps θ_v. For every $v \in S$, the morphism of schemes $\mathrm{Spec}\, K_v \to \mathrm{Spec}\, \widetilde{A}$ induces a natural transformation between the two spectral sequences, which gives a commutative diagram.

$$\begin{array}{ccccc} 0 \longrightarrow & \mathrm{Pic}(\widetilde{B})^G & \longrightarrow & \widetilde{A}^\times / N_{L/K}(\widetilde{B}^\times) & \longrightarrow \mathrm{Br}(\widetilde{A}) \\ & \downarrow & & \downarrow & \downarrow \\ & 0 & \longrightarrow & \bigoplus_{v \in S} K_v^\times / N_{L \otimes_K K_v}(L \otimes_K K_v)^\times & \longrightarrow \bigoplus_{v \in S} \mathrm{Br}(K_v) \end{array}$$

where the rows are exact. But since S is the set of places of K not corresponding to a point in $\mathrm{Spec}\, \widetilde{A}$, the map $\mathrm{Br}(\widetilde{A}) \to \bigoplus_{v \in S} \mathrm{Br}(K_v)$ is injective [Mil80, Ex. III.2.22(a)]. Hence, the kernel $\mathrm{Pic}(\widetilde{B})^G$ of the top right arrow must be equal to the kernel of the central vertical arrow, which is exactly the kernel of (4.9). Since G acts by inversion on $\mathrm{Pic}(\widetilde{B})$, we have $\mathrm{Pic}(\widetilde{B})^G = \mathrm{Pic}(\widetilde{B})[2]$ and we obtain a canonical isomorphism

$$\mathrm{NormCl}\,(B/A)[4]/\mathrm{NormCl}\,(B/A)[2] \xrightarrow{\sim} \mathrm{Pic}(\widetilde{B})[2]$$

by Lemma 4.4. □

If L/K is ramified or inert at v, then $L \otimes_K K_v$ is L_w where w is the unique extension of v to L. If L/K is split at v, then we have $L \otimes_K K_v = K_v \times K_v$ and $K_v^\times / N_{L \otimes_K K_v / K}(L \otimes_K K_v)$ is trivial. Hence, θ_v is the *local Artin symbol* or *norm residue symbol* [Ser79, §XIII.4] of L/K at v.

Analogous to the theory of Rédei [Réd34], the order of the kernel of (4.9) can be found explicitly by computing the rank of a matrix R_4 over $\mathbb{F}_2$, called the Rédei matrix.

Definition 4.7. With notation as before, let $v_1, \ldots, v_s$ be the places in S and let $\epsilon_1, \ldots, \epsilon_s$ be a basis for $\widetilde{A}^\times / (\widetilde{A}^\times)^2$. The *Rédei matrix* of B/A with respect to $v_1, \ldots, v_s$ and $\epsilon_1, \ldots, \epsilon_s$ is the $s \times s$-matrix

$$R_4 = (\theta_{v_i}(\epsilon_j))_{i,j}$$

over $\mathbb{F}_2$ with θ_{v_i} the local Artin symbols.

In the notation of Theorem 4.6, the matrix R_4 represents the homomorphism

$$\prod_{v \in S} \theta_v : \widetilde{A}^\times / (\widetilde{A})^2 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^S$$

with respect to the basis $\epsilon_1, \ldots, \epsilon_s$. The following relation between R_4 and the 4-rank of $\mathrm{NormCl}\,(B/A)$ therefore follows from Theorem 4.6 and Lemma 4.1.

Corollary 4.8. *For B/A as in Theorem 4.6, we have*

$$r_4(B/A) \;=\; r_2(B/A) - \operatorname{rk} R_4.$$

Remark 4.9. In the proof of Theorem 4.6, the image of $\mathrm{Br}(\widetilde{A})$ is in the kernel of the sum map $\bigoplus_{v\in S} \mathrm{Br}(K_v) \to \mathbb{Z}/2\mathbb{Z}$. Hence, the θ_{v_i} satisfy

$$\sum_{i=1}^{s} \theta_{v_i}(u) = 0 \tag{4.10}$$

for every $u \in \widetilde{A}$, which means that the columns of R_4 sum to zero. This can be used to aid calculation if a tactical choice of basis $\epsilon_1, \ldots, \epsilon_s$ is made. We will see this in the following example.

Example 4.10. Take $A = \mathbb{Z}[i]$ with $K = \mathrm{Frac}(A) = \mathbb{Q}(i)$ and $L = \mathbb{Q}(i, \sqrt{65})$. The ramified primes are $1 \pm 2i, 2 \pm 3i \in \mathbb{Z}[i]$. Since $\mathbb{Q}(i)$ has just one infinite place, this gives $s = 5$. As L has 2 pairs of complex embeddings, we have $\mathcal{O}_L^\times = \mu_L \times \langle \eta \rangle$ for some fundamental unit η by the Dirichlet Unit Theorem. Regardless of the norm of η, we must have $\mathcal{O}_L^{\mathrm{Norm}=1}/(\mathcal{O}_L^{\mathrm{Norm}=1})^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and Theorem 4.2 yields

$$r_2(\mathcal{O}_L/\mathcal{O}_K) \;=\; s - \dim_{\mathbb{F}_2} \mathcal{O}_L^{\mathrm{Norm}=1}/(\mathcal{O}_L^{\mathrm{Norm}=1})^2 \;=\; 5 - 2 \;=\; 3.$$

Note that for $u \in \mathcal{O}_p^\times$, the local Artin symbol θ_p satisfies

$$\theta_p(u) \;=\; 0 \iff u \text{ is a square modulo } p$$

for each of the ramified primes p by Hensel's Lemma. For instance, for the prime $p = 1+2i$, the isomorphism $\mathbb{Z}[i]/(1+2i) \xrightarrow{\sim} \mathbb{F}_5$ sends $2-3i$ to the square 1 and sends $1-2i$, $2+3i$ and i to non-squares, which gives $\theta_{1+2i}(2-3i) = 0$ and $\theta_{1+2i}(\epsilon) = 1$ for $\epsilon \in \{1-2i, 2+3i, i\}$. A similar calculation for the other primes allows us to fill in the Rédei matrix as follows:

$$\begin{array}{r} \\ 1+2i \\ 1-2i \\ 2+3i \\ 2-3i \\ \infty \end{array}
\begin{array}{c}
\begin{array}{ccccc} 1+2i & 1-2i & 2+3i & 2-3i & i \end{array} \\
\left(\begin{array}{ccccc}
 & 1 & 1 & 0 & 1 \\
1 & & 0 & 1 & 1 \\
0 & 1 & & 0 & 1 \\
1 & 0 & 0 & & 1 \\
0 & 0 & 0 & 0 & 0
\end{array}\right)
\end{array}$$

The bottom row being 0 reflects the fact that the unique infinite place ∞ of $\mathbb{Q}(i)$ is complex and therefore split in L/K. Note that we only needed to calculate $\theta_p(u)$ for u coprime to p, as the diagonal entries can be filled in using (4.10). One finds $\operatorname{rk} R_4 = 2$ and

$$r_4(\mathcal{O}_L/\mathcal{O}_K) \;=\; r_2(\mathcal{O}_L/\mathcal{O}_K) - \operatorname{rk} R_4 \;=\; 3 - 2 \;=\; 1.$$

From $r_2(\mathcal{O}_L/\mathcal{O}_K) = 3$ and $r_4(\mathcal{O}_L/\mathcal{O}_K) = 1$ we conclude that $\mathrm{NormCl}\,(\mathcal{O}_L/\mathcal{O}_K)[2]$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^k\mathbb{Z}$ for some $k \geq 2$. We can relate this information back

to the wide class group Cl_L using the exact sequence (3.6) associated to the norm class group. For each of the ramified primes, this gives a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}[i]^\times/N_{L/K}(\mathcal{O}_L^\times) & \longrightarrow & \mathrm{NormCl}\,(\mathcal{O}_L/\mathcal{O}_K) & \longrightarrow & \mathrm{Cl}_L & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & K_p^\times/N_{L_p/K_p}(L_p^\times) & \xrightarrow{\sim} & \mathrm{NormCl}\,(L_p/K_p) & \longrightarrow & 0 & & \end{array}$$

where the rows are exact. As with the narrow class group, relating the norm class group to the wide class group requires determining whether elements are norms or not. In this case, we observe $N_{L/K}(i) = -1$, and since we had $\theta_p(i) = 1$ in the Rédei matrix for every ramified p, this makes the vertical arrow $\mathbb{Z}[i]^\times/N_{L/K}(\mathcal{O}_L^\times) \to K_p^\times/N_{L_p/K_p}(L_p^\times)$ an isomorphism. For any such p, this provides a retraction $\mathrm{NormCl}\,(\mathcal{O}_L/\mathcal{O}_K) \to \mathbb{Z}[i]^\times/N_{L/K}(\mathcal{O}_L^\times)$ and we find

$$\mathrm{NormCl}\,(\mathcal{O}_L/\mathcal{O}_K) \;\cong\; \mathrm{Cl}_L \oplus \mathbb{Z}/2\mathbb{Z}.$$

Thus, we conclude that the 2-part of Cl_L is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^k\mathbb{Z}$ for some $k \geq 2$. Indeed, this class group is $\mathrm{Cl}_L \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, see [LMFDB].

Bibliography

[Bha04] M. Bhargava. "Higher composition laws I: A new view on Gauss composition, and quadratic generalizations". In: *Annals of Mathematics* 159 (2004), pp. 217–250.

[Cas67] J. W. S. Cassels. "Global Fields". In: *Algebraic Number Theory*. Academic Press, 1967, pp. 42–84.

[CF15] B. Calmès and J. Fasel. *Groupes classiques*. Vol. II. Autour des schémas en groupes 46. Société Mathematique de France, 2015. Chap. 4, pp. 1–133.

[Cox89] D. A. Cox. *Primes of the form $x^2 + ny^2$*. Wiley, 1989.

[Dir1894] P. J. L. Dirichlet. *Vorlesungen über Zahlentheorie*. Braunschweig, F. Vieweg und sohn, 1894.

[EGAII] A. Grothendieck. *Éléments de Géométrie Algébrique II*. Institut des Hautes Études, 1961, pp. 5–222.

[Gau1801] C. F. Gauss. *Disquisitiones Arithmeticae*. Leipzig, 1801, pp. 108–374.

[Gil24] P. Gille. *Torsors over affine curves*. PCMI Lecture Notes. 2024.

[Gir71] J. Giraud. *Cohomologie non abélienne*. Vol. 179. Grundlehren der mathematischen Wissenschaften. Springer Berlin, Heidelberg, 1971.

[GNR24] P. Gille, E. Neher, and C. Ruether. *The Norm Functor over Schemes*. Preprint. 2024. arXiv: `2401.15051`.

[Lan80] S. Lang. *Cyclotomic Fields II*. Graduate Texts in Mathematics, 69. Springer US, 1980.

[LMFDB] The LMFDB Collaboration. *The number field database, number field `4.0.67600.2`*. `www.lmfdb.org/NumberField/4.0.67600.2`. [Online; accessed 7 August 2025]. 2025.

[Mil80] J. S. Milne. *Étale Cohomology*. Princeton University Press, 1980.

[Mur67] J. Murre. *Lectures on an introduction to Grothendieck's theory of the fundamental group*. Tata Institute of Fundamental Research, 1967.

[Qin09] Y. Qin. "The generalized Rédei-matrix". In: *Mathematische Zeitschrift* 261.1 (2009), pp. 23–37.

[Réd34] L. Rédei. "Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper". In: *Journal für die reine und angewandte Mathematik* 171 (1934), pp. 55–60.

[Sch94] C. Scheiderer. *Real and Étale Cohomology*. Springer Berlin, Heidelberg, 1994.

[Ser79] J. Serre. *Local Fields*. Vol. 67. Graduate Texts in Mathematics. Springer New York, 1979.

[Wit09] C. Wittmann. "Densities for 4-class ranks of quadratic function fields". In: *Journal of Number Theory* 129.10 (2009), pp. 2635–2645.

[Woo11] M. M. Wood. "Gauss composition over an arbitrary base". In: *Advances in mathematics* 226.2 (2011), pp. 1756–1771.