Author: Gunawan, Albert

Title: Gauss's theorem on sums of 3 squares, sheaves, and Gauss composition

Issue Date: 2016-03-08

Gauss's theorem on sums of 3 squares, sheaves, and Gauss composition

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op dinsdag 8 maart 2016
klokke 16:15 uur

door

Albert Gunawan
geboren te Temanggung in 1988

Promotor: Prof. dr. Bas Edixhoven

Promotor: Prof. dr. Qing Liu (Université de Bordeaux)

Samenstelling van de promotiecommissie:

Prof. dr. Philippe Gille (CNRS, Université Lyon)

Prof. dr. Hendrik Lenstra (secretaris)

Prof. dr. Aad van der Vaart (voorzitter)

Prof. dr. Don Zagier (Max Planck Institute for Mathematics, Bonn)

This work was funded by Algant-Doc Erasmus-Mundus and was carried out at Universiteit Leiden and Université de Bordeaux.

THÈSE EN COTUTELLE PRÉSENTÉE

POUR OBTENIR LE GRADE DE

DOCTEUR DE L'UNIVERSITÉ DE BORDEAUX ET DE UNIVERSITEIT LEIDEN

ÉCOLE DOCTORALE MATHÉMATIQUES ET INFORMATIQUE

MATHEMATISCH INSTITUUT LEIDEN

SPECIALITÉ : Mathématiques Pures

Par Albert GUNAWAN

GAUSS'S THEOREM ON SUMS OF 3 SQUARES, SHEAVES, AND GAUSS COMPOSITION

Sous la direction de : Bas EDIXHOVEN et Qing LIU

Soutenue le : 8 Mars 2016 à Leiden

Membres du jury :

M LENSTRA, Hendrik	Prof.	Universiteit Leiden	Président
M GILLE, Philippe	Prof.	CNRS, Université Lyon	Rapporteur
M ZAGIER, Don	Prof.	MPIM, Bonn	Rapporteur
Mme LORENZO, Elisa	Dr.	Universiteit Leiden	Examinateur

Contents

1 Introduction **1**

1.1 Motivation . . . 1

1.2 Cohomological interpretation . . . 2

1.2.2 Examples . . . 3

1.2.3 Sheaves of groups . . . 4

1.3 Gauss composition on the sphere . . . 5

1.3.1 Explicit description by lattices, and a computation . 5

2 Tools **9**

2.1 Presheaves . . . 9

2.2 Sheaves . . . 11

2.2.5 Sheafification . . . 14

2.3 Sheaves of groups acting on sheaves of sets and quotients . . 18

2.4 Torsors . . . 22

2.5 Twisting by a torsor . . . 27

2.6 A transitive action . . . 31

2.7 The Zariski topology on the spectrum of a ring . . . 36

2.8 Cohomology groups and Picard groups . . . 41

2.9 Bilinear forms and symmetries . . . 45

2.9.4 Minkowski's theorem 49
2.10 Descent 49
2.11 Schemes 52
2.12 Grothendieck (pre)topologies and sites 59
2.13 Group schemes 62
2.13.8 Affine group schemes 65

3 Cohomological interpretation 67

3.1 Gauss's theorem 67
3.2 The sheaf SO_3 acts transitively on spheres 69
3.3 Triviality of the first cohomology set of SO_3 73
3.4 Existence of integral solutions 76
3.4.2 Existence of a rational solution 77
3.4.5 Existence of a solution over $\mathbb{Z}_{(p)}$ 78
3.4.8 The proof of Legendre's theorem by sheaf theory . . 81
3.5 The stabilizer in Gauss's theorem 83
3.5.4 The orthogonal complement $P^\perp$ of P in $\mathbb{Z}^3$ 84
3.5.7 The embedding of $\mathcal{H}$ in $\mathcal{N}$ 86
3.5.12 The automorphism group scheme of $P^\perp$ 89
3.5.17 Determination of $\mathcal{H}$ over $\mathbb{Z}[1/2]$ 95
3.6 The group $\mathrm{H}^1(S, \mathcal{T})$ as Picard group 99
3.7 The proof of Gauss's theorem 101

4 Gauss composition on the 2-sphere 107

4.1 The general situation 107
4.1.1 A more direct description 109
4.2 Gauss composition: the case of the 2-sphere 109
4.2.1 Description in terms of lattices in $\mathbb{Q}^3$ 110
4.2.5 Summary of the method 114

4.3 Finding an orthonormal basis for M explicitly 115

4.3.3 The quotient of $ts^{-1}M + \mathbb{Z}^3$ by $\mathbb{Z}^3$ 117

4.3.6 Explicit computation for $ts^{-1}M + \mathbb{Z}^3 \subset \mathbb{Q}^3$ continued 122

4.3.7 Getting a basis for $ts^{-1}M$ given one for $ts^{-1}M + \mathbb{Z}^3$ 124

4.4 Some explicit computation 129

4.4.2 An example of Gauss composition for 770 132

4.4.3 Another example for 770 135

Bibliography **139**

Summary **143**

Samenvatting **145**

Résumé **147**

Acknowledgments **149**

Curriculum Vitae **151**

Chapter 1

Introduction

1.1 Motivation

Many Diophantine problems ask for integer solutions of systems of polynomial equations with integer coefficients. Meanwhile algebraic geometers study geometry using polynomials or vice versa. The area of arithmetic geometry is motivated by studying the questions in Diophantine problems through algebraic geometry. Before the 20th century number theorists borrowed several techniques from algebra and analysis, but since last century number theorists have seen several important results due to algebraic geometry. Some of the great successes include proofs of the Mordell conjecture, Fermat's Last Theorem and the modularity conjecture. With its powerful tools, arithmetic geometry also opens possibilities to prove "old" theorems in number theory using new methods that possibly will simplify the proofs and generalize the theorems.

We want to show in this thesis how some basic modern tools from topology, such as sheaves and cohomology, shed new light on an old theorem of

Gauss in number theory: in how many ways can an integer be written as a sum of three squares? Surprisingly the answer, if non-zero, is given by a class number of an imaginary quadratic ring O. We use the action of the *orthogonal group* $\mathrm{SO}_3(\mathbb{Q})$ on the *sphere* of radius $\sqrt{n}$ to reprove Gauss's theorem, and more. We also show that the class group of O acts naturally on the set of $\mathrm{SO}_3(\mathbb{Z})$-orbits in the set of primitive integral points of that sphere, and we make this action explicit directly in term of the $\mathrm{SO}_3(\mathbb{Q})$-action.

In the article [18], Shimura expresses the representation numbers of $x_1^2 + \cdots + x_d^2$ in terms of class numbers of certain groups, also using orthogonal groups but with adelic methods. There is also recent work by Bhargava and Gross [2] that discusses arithmetic invariants for certain representations of some reductive groups. The paper by Gross [9], Section 3 describes explicitly the action of $\mathrm{Pic}(O)$ in terms of ideals, quaternions, and adèles. In [23] and [12], page 90–92, Zagier gives a proof of Gauss's theorem using modular forms of weight 3/2, providing the first example of what is now called mock modular form.

The main contents of this thesis are in Chapters 3–4. In the next 2 sections, we give an overview of what we do there. No preliminary knowledge of sheaves, schemes, and group schemes is necessary for reading this thesis, and actually one learns some of it by getting nice and simple examples. Chapter 2 gives a summary of the mathematical tools that we use in Chapters 3–4.

1.2 Cohomological interpretation

This section describes the content of Chapter 3.

Notation: for $d \in \mathbb{Z}$ not a square and $d \equiv 0, 1 (\mathrm{mod}\ 4)$, let $O_d := \mathbb{Z}[\frac{\sqrt{d}+d}{2}]$, the quadratic order of discriminant d.

1.2.1 Theorem. (Gauss) *Let $n \in \mathbb{Z}_{\geq 1}$ be a positive integer. Let*

$$\mathcal{X}_n(\mathbb{Z}) = \{x \in \mathbb{Z}^3 : x_1^2 + x_2^2 + x_3^2 = n \text{ and } \gcd(x_1, x_2, x_3) = 1\}.$$

Then:

$$\#\mathcal{X}_n(\mathbb{Z}) = \begin{cases} 0 & \text{if } n \equiv 0, 4, 7(8), \\ 48\frac{\#\operatorname{Pic}(O_{-n})}{\#(O_{-n}^{\times})} & \text{if } n \equiv 3(8), \\ 24\frac{\#\operatorname{Pic}(O_{-4n})}{\#(O_{-4n}^{\times})} & \text{if } n \equiv 1, 2(4). \end{cases}$$

A precise reference is: page 339 of [6], Article 292. Gauss formulated it in terms of equivalence classes of quadratic forms, not of ideals.

Let $n \in \mathbb{Z}_{\geq 1}$. Suppose $\mathcal{X}_n(\mathbb{Z}) \neq \emptyset$ and let $x \in \mathcal{X}_n(\mathbb{Z})$. Let $\mathrm{SO}_3(\mathbb{Z})_x$ be the stabilizer subgroup of x in $\mathrm{SO}_3(\mathbb{Z})$. We will show in Chapter 3 that

$$\#\mathcal{X}_n(\mathbb{Z}) = \frac{\#\,\mathrm{SO}_3(\mathbb{Z})}{\#\,\mathrm{SO}_3(\mathbb{Z})_x}\#\operatorname{Pic}(\mathbb{Z}[1/2, \sqrt{-n}]).$$

The number of elements of $\mathrm{SO}_3(\mathbb{Z})$ is 24. For $n > 3$, the action of $\mathrm{SO}_3(\mathbb{Z})$ on $\mathcal{X}_n(\mathbb{Z})$ is free, so $\#\,\mathrm{SO}_3(\mathbb{Z})_x = 1$. Thus, for $n > 3$, one has

$$\#\mathcal{X}_n(\mathbb{Z}) = 24\cdot\#\operatorname{Pic}(\mathbb{Z}[1/2, \sqrt{-n}]).$$

1.2.2 Examples

Let us take $n = 26$. The number of $\mathrm{SO}_3(\mathbb{Z})$-orbits on $\mathcal{X}_n(\mathbb{Z})$ is 3:

$$26 = 5^2 + 1^2 + 0^2 = 4^2 + 3^2 + 1^2 = (-4)^2 + 3^2 + 1^2.$$

By Gauss's theorem, we get $\#\operatorname{Pic}(\mathbb{Z}[1/2, \sqrt{-26}]) = 3$ and $\#\operatorname{Pic}(O_{-4\cdot 26}) = 6$.

Another example: $n = 770$. We write it as sum of 3 squares up to $\mathrm{SO}_3(\mathbb{Z})$-action as:

$$\begin{aligned} 770 &= (\pm 27)^2 + 5^2 + 4^2 = (\pm 25)^2 + 9^2 + 8^2 = (\pm 25)^2 + 12^2 + 1^2 \\ &= (\pm 24)^2 + 13^2 + 5^2 = (\pm 23)^2 + 15^2 + 4^2 = (\pm 20)^2 + 19^2 + 3^2 \\ &= (\pm 20)^2 + 17^2 + 9^2 = (\pm 17)^2 + 16^2 + 15^2. \end{aligned}$$

We get $\# \operatorname{Pic}(\mathbb{Z}[1/2, \sqrt{-770}]) = 16$ and $\# \operatorname{Pic}(O_{-4 \cdot 770}) = 32$.

1.2.3 Sheaves of groups

For $x \in \mathcal{X}_n(\mathbb{Z})$, let $G_x \subset G := \mathrm{SO}_3$ be the stabilizer subgroup scheme. We only need G and G_x as sheaves on $\operatorname{Spec}(\mathbb{Z})$ with the Zariski topology. The non-empty open subsets of $\operatorname{Spec}(\mathbb{Z})$ are $\operatorname{Spec}(\mathbb{Z}[1/m])$ for $m \geq 1$. We have

$$G(\mathbb{Z}[1/m]) = \{g \in \mathrm{M}_3(\mathbb{Z}[1/m]) : g^t \cdot g = 1, \det(g) = 1\}.$$

We also get

$$G_x(\mathbb{Z}[1/m]) = \{g \in G(\mathbb{Z}[1/m]) : gx = x\}.$$

For x and y in $\mathcal{X}_n(\mathbb{Z})$ and $m \geq 1$ let

$${}_yG_x(\mathbb{Z}[1/m]) = \{g \in G(\mathbb{Z}[1/m]) : gx = y\}.$$

For all x, y and m, the right-action of $G_x(\mathbb{Z}[1/m])$ on ${}_yG_x(\mathbb{Z}[1/m])$ is free and transitive, and we will show that for every prime number p, there exists m such that $p \nmid m$ and ${}_yG_x(\mathbb{Z}[1/m]) \neq \emptyset$. This means that ${}_yG_x$ is a G_x-torsor for the Zariski topology.

For $y \in \mathcal{X}_n(\mathbb{Z})$ let $[y]$ be the orbit of y under the $\mathrm{SO}_3(\mathbb{Z})$-action. From now on assume that $\mathcal{X}_n(\mathbb{Z}) \neq \emptyset$. Let $x \in \mathcal{X}_n(\mathbb{Z})$. Let $\mathrm{H}^1(\operatorname{Spec}(\mathbb{Z}), G_x)$ be the set of isomorphism classes of G_x-torsors. For $y \in \mathcal{X}_n(\mathbb{Z})$ let $[{}_yG_x]$ be the class of ${}_yG_x$. Sheaf theory gives a bijection

$$\mathrm{SO}_3(\mathbb{Z}) \backslash \mathcal{X}_n(\mathbb{Z}) \to \mathrm{H}^1(\operatorname{Spec}(\mathbb{Z}), G_x), \quad [y] \mapsto [{}_yG_x].$$

As G_x is a sheaf of *commutative* groups, $\mathrm{H}^1(\operatorname{Spec}(\mathbb{Z}), G_x)$ is a commutative group. We will show, with a lot of work, that it is isomorphic to $\operatorname{Pic}(\mathbb{Z}[1/2, \sqrt{-n}])$.

1.3 Gauss composition on the sphere

We will show that the bijection $\mathrm{SO}_3(\mathbb{Z})\backslash\mathcal{X}_n(\mathbb{Z}) \to \mathrm{H}^1(\mathrm{Spec}(\mathbb{Z}), G_x)$, gives a natural action of $\mathrm{Pic}(\mathbb{Z}[1/2, \sqrt{-n}])$ on $\mathrm{SO}_3(\mathbb{Z})\backslash\mathcal{X}_n(\mathbb{Z})$ which is free and transitive. Conclusion: $\mathrm{SO}_3(\mathbb{Z})\backslash\mathcal{X}_n(\mathbb{Z})$, if non-empty, is an *affine space* under $\mathrm{Pic}(\mathbb{Z}[1/2, \sqrt{-n}])$. This is analogous to the set of solutions of an inhomogeneous system of linear equations $Ax = b$ being acted upon freely and transitively by the vector space of solutions of the homogeneous equations $Ax = 0$, via translations.

What we mean as Gauss composition on the sphere is the *parallelogram law* on the affine space $\mathrm{SO}_3(\mathbb{Z})\backslash\mathcal{X}_n(\mathbb{Z})$: for x, y and x' in $\mathcal{X}_n(\mathbb{Z})$, we get $[{}_yG_x]\cdot[x']$ in $\mathrm{SO}_3(\mathbb{Z})\backslash\mathcal{X}_n(\mathbb{Z})$, there is a $y' \in \mathcal{X}_n(\mathbb{Z})$, unique up to $\mathrm{SO}_3(\mathbb{Z})$, such that $[{}_yG_x]\cdot[x'] = [y']$.

We make this operation explicit. As G_x is commutative, G_x and $G_{x'}$ are naturally isomorphic. Then ${}_yG_x$ is a $G_{x'}$-torsor. The inverse of the bijection

$$\mathrm{SO}_3(\mathbb{Z})\backslash\mathcal{X}_n(\mathbb{Z}) \to \mathrm{H}^1(\mathrm{Spec}(\mathbb{Z}), G_{x'}), \quad [y'] \mapsto [{}_{y'}G_{x'}]$$

gives y'. What follows can be seen as a 3D version of how one uses rational functions, divisors and invertible modules: G_x replaces $\mathbb{G}_\mathrm{m}$ of a number ring, and $\mathbb{Z}^3$ replaces the number ring.

1.3.1 Explicit description by lattices, and a computation

As computations in class groups are not a triviality, there cannot be a simple formula for Gauss composition on the sphere as for example the cross product. We will use a description in terms of lattices of $\mathbb{Q}^3$ to give the composition law. Let n be a positive integer. Let x, y and x' be elements of $\mathcal{X}_n(\mathbb{Z})$. Let t be in ${}_yG_x(\mathbb{Q})$. Let $M \subset \mathbb{Q}^3$ be the lattice such that for all primes p:

$$M_{(p)} := {}_{x'}G_x(\mathbb{Z}_{(p)})t^{-1}\mathbb{Z}^3_{(p)},$$

where $\mathbb{Z}_{(p)}$ is the localization of $\mathbb{Z}$ at the prime ideal (p). It is a unimodular lattice for the standard inner product, containing x'. Let (m_1, m_2, m_3) be an oriented orthonormal basis of M. Let m be the matrix with columns (m_1, m_2, m_3). It is in $G(\mathbb{Q})$. Then $y' := m^{-1}{\cdot}x'$.

One explicit example is the following: let $n = 770 = 2{\cdot}5{\cdot}7{\cdot}11$, the same example that Gauss gives in his Disquisitiones Arithmeticae [6] Article 292. For $n = 770$,

$$\mathrm{Pic}(\mathbb{Z}[1/2, \sqrt{-770}]) \cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

We take $x = (25, 9, -8)$, $y = (23, 15, 4)$, and $x' = (25, 12, 1)$. We obtain an element $t \in {}_yG_x(\mathbb{Q})$ by composing two symmetries: the first one is s_z the symmetry about the hyperplane perpendicular to $z := (0, 0, 1)$ and the second one is the symmetry about the hyperplane perpendicular to the vector $y - s_z(x)$. This gives

$$t = \frac{1}{7}\begin{pmatrix} 6 & 3 & 2 \\ 3 & -2 & -6 \\ -2 & 6 & -3 \end{pmatrix} \text{ in } {}_yG_x(\mathbb{Z}[1/7]).$$

We obtain an element $s \in {}_{x'}G_x(\mathbb{Q})$ by composing two symmetries: the first one is s_z and the second one is the symmetry about the hyperplane perpendicular to the vector $x' - s_z(x)$. This gives

$$s = \frac{1}{29}\begin{pmatrix} 29 & 0 & 0 \\ 0 & 20 & -21 \\ 0 & 21 & 20 \end{pmatrix} \text{ in } {}_{x'}G_x(\mathbb{Z}[1/29]).$$

It has a pole at 29. We will show that $29{\cdot}\mathbb{Z}^3 \subset ts^{-1}M \subset 29^{-1}\mathbb{Z}^3$. Next we consider the lattice $ts^{-1}M + \mathbb{Z}^3$ inside $\frac{1}{29}\mathbb{Z}^3$. Using the action of G_y on both lattices, we will show that $(ts^{-1}M + \mathbb{Z}^3)/\mathbb{Z}^3$ is a free $\mathbb{Z}/29\mathbb{Z}$-module of rank 1. We will get a basis for $\mathbb{Z}^3 + ts^{-1}M$:

$$(1/29, 8/29, 15/29), \quad (0,1,0), \quad (0,0,1).$$

We will show that $\mathbb{Z}^3 + ts^{-1}M$ has two sublattices of index 29 on which the inner product is integral: $\mathbb{Z}^3$ and $ts^{-1}M$. We will find a basis for $ts^{-1}M$ and then via multiplication by st^{-1} a basis for M:

$$(-1, 32, -2)/7, (-2, -6, 3)/7, (0, 119, -7)/7.$$

The LLL-algorithm gives us an orthonormal basis for M:

$$(-6, 3, 2)/7, (-2, -6, 3)/7, (3, 2, 6)/7.$$

This gives $y' = (-16, -17, 15)$.

We have shown how to do an addition in $\mathrm{Pic}(\mathbb{Z}[1/2, \sqrt{-n}])$ purely in terms of $\mathcal{X}_n(\mathbb{Z})$ and $\mathrm{SO}_3(\mathbb{Q})$.

Chapter 2

Tools

In this chapter we present, mostly in a self-contained way, and at the level of a beginning graduate student, the technical tools that will be applied in the next 2 chapters. These tools are well known and in each section below we indicate where they can be found. The results in the first 6 sections on presheaves and sheaves on topological spaces could have been given for presheaves and sheaves on sites. We have chosen not to do that because we want this work to be as elementary as possible. The reader is advised to skip the discussions on schemes, sites, and group schemes in the last 3 sections, and only read them if necessary.

2.1 Presheaves

The results on presheaves and sheaves in this chapter can be found in [21, Tag 006A].

2.1.1 Definition. Let S be a topological space. A *presheaf of sets* on S is a contravariant functor $\mathcal{F}$ from $\mathrm{Open}(S)$ to Sets, where $\mathrm{Open}(S)$ is the category whose objects are the open subsets of S and whose morphisms are the inclusion maps, and where Sets is the category of sets. *Morphisms of presheaves* are transformations of functors. The category of presheaves of sets is denoted $\mathrm{Psh}(S)$.

Let S be a topological space and $\mathcal{F}$ be a presheaf of sets on S. So for each U in $\mathrm{Open}(S)$ we have a set $\mathcal{F}(U)$. The elements of this set are called the *sections* of $\mathcal{F}$ over U. For each inclusion $i : V \to U$ with V and U in $\mathrm{Open}(S)$, the map $\mathcal{F}(i)\colon \mathcal{F}(U) \to \mathcal{F}(V)$ is called the *restriction map*. Often one uses the notation $s|_V := \mathcal{F}(i)(s)$, for $s \in \mathcal{F}(U)$. Functoriality means that for all inclusions $j\colon W \to V$ and $i\colon V \to U$ with W, V, U in $\mathrm{Open}(S)$, $\mathcal{F}(i \circ j) = \mathcal{F}(j) \circ \mathcal{F}(i)$. A morphism of presheaves $\phi\colon \mathcal{F} \to \mathcal{G}$, where $\mathcal{F}$ and $\mathcal{G}$ are presheaves of sets on S, consists of maps $\phi(U)\colon \mathcal{F}(U) \to \mathcal{G}(U)$, for all U in $\mathrm{Open}(S)$, such that for all inclusions $i\colon V \to U$, we have $\mathcal{G}(i) \circ \phi(U) = \phi(V) \circ \mathcal{F}(i)$, that is, the diagram

$$\begin{tikzcd}
\mathcal{F}(U) \arrow[r, "\phi(U)"] \arrow[d, "\mathcal{F}(i)"'] & \mathcal{G}(U) \arrow[d, "\mathcal{G}(i)"] \\
\mathcal{F}(V) \arrow[r, "\phi(V)"] & \mathcal{G}(V)
\end{tikzcd}$$

is commutative.

2.1.2 Example. Let S be a topological space and let A be a set. Then the *constant presheaf* on S with values in A is given by $U \mapsto A$ for all U in $\mathrm{Open}(S)$, and with all restriction maps id_A.

Similarly, we define presheaves of groups, rings and so on. More generally we may define presheaves with values in a category.

2.1.3 Definition. Let S be a topological space and $\mathcal{A}$ be a category. A *presheaf* $\mathcal{F}$ on S with *values in* $\mathcal{A}$ is a contravariant functor from $\mathrm{Open}(S)$

to $\mathcal{A}$, that is

$$\mathcal{F}\colon\ \mathrm{Open}(\mathcal{S})^{opp} \to \mathcal{A}.$$

A *morphism of presheaves* $\mathcal{F} \to \mathcal{G}$ on S with values in $\mathcal{A}$ is a transformation of functors from $\mathcal{F}$ to $\mathcal{G}$.

These presheaves and transformation of functors form objects and morphisms in the category of presheaves on S with values in $\mathcal{A}$. Next we will discuss limits and colimits of presheaves of sets. All presheaves and sheaves in this and the next section that we consider are presheaves and sheaves of sets unless mentioned otherwise.

Let S be a topological space and $\mathcal{I}$ a small category. Let $\mathcal{F}\colon \mathcal{I} \to \mathrm{Psh}(S)$, $i \mapsto \mathcal{F}_i$ be a functor. Both $\lim_i \mathcal{F}_i$ and $\mathrm{colim}_i\, \mathcal{F}_i$ exist. For any open U in $\mathrm{Open}(S)$, we have

$$(\lim_i \mathcal{F}_i)(U) = \lim_i \mathcal{F}_i(U), \quad (\mathrm{colim}_i\, \mathcal{F}_i)(U) = \mathrm{colim}_i\, \mathcal{F}_i(U).$$

2.2 Sheaves

Sheaves are presheaves that satisfy the sheaf condition, that is their sets of sections are “determined locally”. The following definition makes this precise.

2.2.1 Definition. Let S be a topological space, and $\mathcal{F}$ a presheaf on S. Then $\mathcal{F}$ is a *sheaf of sets* if for all U in $\mathrm{Open}(S)$ and all open covers $(U_i)_{i\in I}$ of U with I any set, and for all collections of sections $(s_i \in \mathcal{F}(U_i))_{i\in I}$ such that for all i and j in I we have $s_i|_{U_i\cap U_j} = s_j|_{U_i\cap U_j}$, there exists a unique section $s \in \mathcal{F}(U)$ such that for all $i \in I, s_i = s|_{U_i}$.

A *morphism of sheaves of sets* is simply a morphism of presheaves of sets. The category of sheaves of sets on S is denoted $\mathrm{Sh}(S)$.

Another way to state the above definition is as follows.

For $U \subset S$ an open subset, $(U_i)_{i\in I}$ an open covering of U with I any set, and each pair $(i,j) \in I \times I$ we have the inclusions

$$\mathrm{pr}_0^{(i,j)} \colon U_i \cap U_j \longrightarrow U_i \text{ and } \mathrm{pr}_1^{(i,j)} \colon U_i \cap U_j \longrightarrow U_j.$$

These induces natural maps

$$\begin{tikzcd} \prod_{i\in I} \mathcal{F}(U_i) \arrow[r, shift left, "\mathcal{F}(\mathrm{pr}_0)"] \arrow[r, shift right, "\mathcal{F}(\mathrm{pr}_1)"'] & \prod_{(i_0,i_1)\in I\times I} \mathcal{F}(U_{i_0} \cap U_{i_1}) \end{tikzcd} ,$$

that are given explicitly by

$$\mathcal{F}(\mathrm{pr}_0) \colon (s_i)_{i\in I} \longmapsto (s_i|_{U_i\cap U_j})_{(i,j)\in I\times I},$$
$$\mathcal{F}(\mathrm{pr}_1) \colon (s_i)_{i\in I} \longmapsto (s_j|_{U_i\cap U_j})_{(i,j)\in I\times I}.$$

Finally consider the natural map

$$\mathcal{F}(U) \longrightarrow \prod_{i\in I} \mathcal{F}(U_i), \quad s \longmapsto (s|_{U_i})_{i\in I}.$$

So $\mathcal{F}$ is a sheaf of sets on S if and only if for all U in $\mathrm{Open}(S)$ and all open covers $(U_i)_{i\in I}$ of U with I any set, the diagram

$$\begin{tikzcd} \mathcal{F}(U) \arrow[r] & \prod_{i\in I} \mathcal{F}(U_i) \arrow[r, shift left, "\mathcal{F}(\mathrm{pr}_0)"] \arrow[r, shift right, "\mathcal{F}(\mathrm{pr}_1)"'] & \prod_{(i_0,i_1)\in I\times I} \mathcal{F}(U_{i_0} \cap U_{i_1}) \end{tikzcd}$$

is an equalizer.

2.2.2 Remark. Let $\mathcal{F}$ be a sheaf of sets on S and $U = \emptyset$, we can cover U by the open cover $(U_i)_{i\in I}$ where $I = \emptyset$. The empty product in the category of sets is a singleton (the element in this singleton is $\mathrm{id}_\emptyset$). Then $\mathcal{F}(U) = \{*\}$, because $\mathcal{F}(U)$ is an equalizer of two maps from $\{\mathrm{id}_\emptyset\}$ to $\{\mathrm{id}_\emptyset\}$. In particular, this condition implies that for disjoint U, V in $\mathrm{Open}(S)$, we have $\mathcal{F}(U \cup V) = \mathcal{F}(U) \times \mathcal{F}(V)$.

2.2.3 Remark. Let S be a topological space, $\mathcal{I}$ a small category, and $\mathcal{F}\colon \mathcal{I} \to \mathrm{Sh}(S), i \mapsto \mathcal{F}_i$ a functor. Then $\lim_i \mathcal{F}_i$ exists. For any open U in $\mathrm{Open}(S)$, we define

$$(\lim_i \mathcal{F}_i)(U) := \lim_i \mathcal{F}_i(U).$$

It is a sheaf and it has the required properties.

For colimit cases we need sheafification (that we will discuss later). If in addition S is a noetherian topological space, I is a partially ordered set, and the diagram of sheaves is filtered, then $\mathrm{colim}_i\, \mathcal{F}_i$ exists and for any U in $\mathrm{Open}(S)$, we have

$$(\mathrm{colim}_i\, \mathcal{F}_i)(U) = \mathrm{colim}_i\, \mathcal{F}_i(U).$$

We define sheaves with values in the category *Groups* of groups, the category *Ab* of abelian groups, or the category of rings. *A sheaf of groups (or abelian groups or rings)* on a topological space S is a presheaf of groups (or abelian groups or rings) that, as a presheaf of sets, is a sheaf.

2.2.4 Example. Let S be a topological space, then the presheaf $C^0_{S,\mathbb{R}}$ of continuous real functions on S is defined as follows. For U in $\mathrm{Open}(S)$,

$$C^0_{S,\mathbb{R}}(U) = \{f\colon U \to \mathbb{R} : f \text{ is continuous}\},$$

with, for $V \subset U$, and for $f \in C^0_{S,\mathbb{R}}(U)$, $f|_V \in C^0_{S,\mathbb{R}}(V)$ the restriction of f to V. It is indeed a sheaf. Let U be in $\mathrm{Open}(S)$ and suppose that $U = \bigcup_{i\in I} U_i$ is an open covering, and $f_i \in C^0_{S,\mathbb{R}}(U_i)$, $i \in I$ with $f_i|_{U_i\cap U_j} = f_j|_{U_i\cap U_j}$ for all $i, j \in I$. We define $f\colon U \to \mathbb{R}$ by setting $f(u)$ equal to the value of $f_i(u)$ for any $i \in I$ such that $u \in U_i$. This is well defined by assumption. Moreover, $f\colon U \to \mathbb{R}$ is a map such that its restriction to U_i agrees with the continuous map f_i on U_i. Hence f is continuous.

Similarly, for X a smooth real manifold, we have the sheaf $C^\infty_{X,\mathbb{R}}$ of smooth real functions: for U in $\mathrm{Open}(S)$,

$$C^\infty_{X,\mathbb{R}}(U) = \{f\colon U \to \mathbb{R} : f \text{ is smooth}\},$$

with the usual restriction maps.

We could also consider a complex analytic manifold and define its sheaf of complex analytic functions.

2.2.5 Sheafification

There is a general procedure to make a sheaf from a presheaf. First we will discuss sheafification of presheaves of sets, and then sheafification for presheaves of groups, abelian groups and rings.

2.2.6 Theorem. *Let S be a topological space, and let $\mathcal{F}$ be a presheaf of sets on S. Then there is a sheaf $\mathcal{F}^\#$ and a morphism of presheaves $j_\mathcal{F}\colon \mathcal{F} \to \mathcal{F}^\#$ such that for every morphism of presheaves $f\colon \mathcal{F} \to \mathcal{G}$ with $\mathcal{G}$ a sheaf, there is a unique $f^\#\colon \mathcal{F}^\# \to \mathcal{G}$ such that $f = f^\# \circ j_\mathcal{F}$. In a diagram:*

$$\begin{tikzcd}
\mathcal{F} \arrow[r, "j_\mathcal{F}"] \arrow[d, "f"'] & \mathcal{F}^\# \arrow[dl, dashed, "\exists! f^\#"] \\
\mathcal{G} &
\end{tikzcd}$$

For proving this theorem, we will use the notion of stalks of presheaves.

2.2.7 Definition. Let S be a topological space and $\mathcal{F}$ be a presheaf of sets on S. Let $s \in S$ be a point. The *stalk of $\mathcal{F}$ at s* is the set

$$\mathcal{F}_s := \mathrm{colim}_{s\in U}\, \mathcal{F}(U)$$

where the colimit is over the opposite full subcategory of $\mathrm{Open}(S)$ of open neighbourhoods of s.

The transition maps in the system are given by the restriction maps of $\mathcal{F}$. The colimit is a directed colimit and we can describe $\mathcal{F}_s$ explicitly

$$\mathcal{F}_s = \{(U, f) \mid s \in U, f \in \mathcal{F}(U)\}/\sim$$

with equivalence relation given by $(U, f) \sim (V, g)$ if and only if there exists an open $W \subset U \cap V$ with s in W and $f|_W = g|_W$.

2.2.8 Example. Let $\mathcal{O}_{\mathbb{C}}$ be the sheaf of complex analytic functions on open subsets of $\mathbb{C}$, that is for each open $U \subset \mathbb{C}$

$$\mathcal{O}_{\mathbb{C}}(U) = \{f \colon U \to \mathbb{C} \text{ analytic}\}.$$

The stalk of $\mathcal{O}_{\mathbb{C}}$ at 0 is the set of formal power series with positive radius of convergence.

2.2.9 Remark. For every open U in $\mathrm{Open}(S)$ there is a canonical map

$$\mathcal{F}(U) \longrightarrow \prod_{s \in U} \mathcal{F}_s$$

defined by $f \mapsto \prod_{s \in U}[U, f]$. For $\mathcal{F}$ a presheaf, the map is not necessarily injective, but it is injective if $\mathcal{F}$ is a sheaf.

We sometimes denote $[U, f]$ as f_s, or even f the corresponding element in $\mathcal{F}_s$. The construction of the stalk $\mathcal{F}_s$ is functorial in the presheaf $\mathcal{F}$. Namely, if $\phi \colon \mathcal{F} \to \mathcal{G}$ is a morphism of presheaves, then we define $\phi_s \colon \mathcal{F}_s \to \mathcal{G}_s$ given by $[U, f] \mapsto [U, \phi(U)(f)]$. This map is well defined because ϕ is compatible with the restriction mappings, so for $[U, f] = [V, g] \in \mathcal{F}_s$ we have $[U, \phi(U)(f)] = [V, \phi(V)(g)] \in \mathcal{G}_s$.

Now we can prove the theorem.

Proof. Let us construct the sheaf $\mathcal{F}^{\#}$. For U in Open(S), let us consider the set $\mathcal{F}^{\#}(U)$ of functions $f\colon U \to \coprod_{s\in U} \mathcal{F}_s$ such that for every $s \in U, f(s) \in \mathcal{F}_s$ and there exists an open neighbourhood $V \subset U$ of s and a section $g \in \mathcal{F}(V)$ such that $f(x) = g_x$ for every $x \in V$. The map $j_{\mathcal{F}}\colon \mathcal{F} \to \mathcal{F}^{\#}$ is given by: for U in Open(S), $j_{\mathcal{F}}(U)(f) = \bar{f}$, where $\bar{f}$ is the function $\bar{f}\colon U \to \coprod_{s\in U} \mathcal{F}_s$ such that $f(s) = f_s$ for every $s \in U$.

To see that $\mathcal{F}^{\#}$ is a sheaf, first we show that $j_{\mathcal{F},s}\colon \mathcal{F}_s \xrightarrow{\sim} \mathcal{F}_s^{\#}$ for every $s \in S$. The injectivity is indeed true because if $f_s, g_s \in \mathcal{F}_s$ such that $\bar{f}_s = \bar{g}_s$, then $\bar{f} = \bar{g}$ on some open neighbourhood $W \subset U \cap V$ of s. This implies $f_s = g_s$. For surjectivity, let $h \in \mathcal{F}_s^{\#}$. On some open neighborhood $W \subset S$ of s, there exists $g \in \mathcal{F}(W)$ such that $h(x) = g_x$ for every $x \in W$. So $\bar{g}_s = h$.

Now let U be any element in Open(S). Suppose that $U = \bigcup_{i\in I} U_i$ is an open covering, and $f_i \in \mathcal{F}^{\#}(U_i)$, $i \in I$ with $f_i|_{U_i\cap U_j} = f_j|_{U_i\cap U_j}$ for all $i, j \in I$. We define $f\colon U \to \coprod_{s\in U} \mathcal{F}_s$ by setting $f(s)$ equal to the value of $f_i(s)$ for any $i \in I$ such that $s \in U_i$. This is well defined because its restriction to U_i agrees f_i on U_i. That is for each $s \in U$ then $s \in U_i$ for some $i \in I$, so there exists $V \subset U_i$ and a section $g \in \mathcal{F}(V)$ such that $f_i(x) = g_x$ for every $x \in V$. But this g defines a function $\bar{g} = j_{\mathcal{F}}(V)(g)$ and $f(x) = f_i(x) = g_x = \bar{g}_x$. The last equality because $\mathcal{F}_s \xrightarrow{\sim} \mathcal{F}_s^{\#}$.

Finally, let $\mathcal{G}$ be a sheaf and $f\colon \mathcal{F} \to \mathcal{G}$ be a morphism. Because $\mathcal{G}$ is a sheaf, we have the following diagram

$$\begin{tikzcd}
\mathcal{F} \arrow[r] \arrow[d, "f"] & \mathcal{F}^{\#} \arrow[d] \\
\mathcal{G} \arrow[r] & \mathcal{G}^{\#}
\end{tikzcd}$$

where the map $\mathcal{F}^{\#} \to \mathcal{G}^{\#}$ is obtained from the map

$$\prod_{s\in U} \mathcal{F}_s \to \prod_{s\in U} \mathcal{G}_s.$$

The map $\mathcal{G} \to \mathcal{G}^{\#}$ is an isomorphism of sheaves because it induces an isomorphism on all stalks. The uniqueness comes because two maps of sheaves $\phi, \pi \colon \mathcal{F}^{\#} \to \mathcal{G}^{\#}$ such that $\phi_s = \pi_s$ for every $s \in S$ are the same map. □

For other algebraic structures, we denote $\mathcal{A}$ for one of these categories: the category of abelian groups, the category of groups or the category of rings. Let $F \colon \mathcal{A} \to \text{Sets}$ be the functor that sends an object to its underlying set. Then F is faithful, $\mathcal{A}$ has limits and F commutes with them, $\mathcal{A}$ has filtered colimits and F commutes with them, and F reflects isomorphisms (meaning that if $f \colon A \to B$ is such that $F(f)$ is bijective, then f is an isomorphism in $\mathcal{A}$).

2.2.10 Lemma. *Let $\mathcal{A}$ be the above category and let S be a topological space. Let $s \in S$ be a point. Let $\mathcal{F}$ be presheaf with values in $\mathcal{A}$. Then*

$$\mathcal{F}_s = \operatorname{colim}_{s \in U} \mathcal{F}(U)$$

exists in $\mathcal{A}$. Its underlying set is equal to the stalk of the underlying presheaf sets of $\mathcal{F}$. Moreover, the construction $\mathcal{F} \to \mathcal{F}_x$ is a functor from the category presheaves with values in $\mathcal{A}$ to $\mathcal{A}$.

Proof. The partially ordered set S of open neighbourhoods of s is a directed system, so the colimit in $\mathcal{A}$ agrees with its colimit in Sets. We can define addition and multiplication (if applicable) of a pair of elements (U, f) and (V, g) as the $(U \cap V, f|_{U \cap V} + g|_{U \cap V})$ and $(U \cap V, f|_{U \cap V} {\cdot} g|_{U \cap V})$. The faithfulness of F allows us to not distinguish between the morphism in $\mathcal{A}$ and the underlying map of sets. □

Now we can do sheafification with values in $\mathcal{A}$, but we will not prove it.

2.2.11 Lemma. *Let S be a topological space. Let $\mathcal{A}$ be above category. Let $\mathcal{F}$ be a presheaf with values in $\mathcal{A}$ on S. Then there exists a sheaf $\mathcal{F}^{\#}$ with values in $\mathcal{A}$ and a morphism $\mathcal{F} \to \mathcal{F}^{\#}$ of presheaves with values in $\mathcal{A}$ with the following properties: For any morphism $\mathcal{F} \to \mathcal{G}$, where $\mathcal{G}$ is a sheaf with values in $\mathcal{A}$ there exists a unique factorization $\mathcal{F} \to \mathcal{F}^{\#} \to \mathcal{G}$.*

Moreover the map $\mathcal{F} \to \mathcal{F}^{\#}$ identifies the underlying sheaf of sets of $\mathcal{F}^{\#}$ with the sheafification of the underlying presheaf of sets of $\mathcal{F}$.

Note that the category of sheaves of abelian groups on a topological space S is denoted by $Ab(S)$. Until now, we have talked only about sheaves on a single topological space. Now we define some operations on sheaves, linked with a continuous map between topological spaces.

2.2.12 Definition. Let X and Y be topological spaces, and $f\colon X \to Y$ be a continuous map. For any sheaf of sets (groups, rings) $\mathcal{F}$ on X, we define the *direct image* sheaf $f_*\mathcal{F}$ on Y by: for any V in Open(Y), $f_*\mathcal{F}(V) := \mathcal{F}(f^{-1}(V))$. For any sheaf of sets (groups, rings) $\mathcal{G}$ on Y, we define the *inverse image* sheaf $f^{-1}\mathcal{G}$ on X to be the sheaf associated to the presheaf $U \mapsto \operatorname{colim}_{V \supset f(U)} \mathcal{G}(V)$, where U is in Open(X), and the colimit is taken over all open sets V of Y containing $f(U)$.

2.3 Sheaves of groups acting on sheaves of sets and quotients

The results that we present in this section and the next 3 sections can be found in Chapter III of [8] in the more general context of sites.

For a group G and a set X, a (left)action of G on X is a map

$$G \times X \to X\colon (g, x) \mapsto g \cdot x,$$

that satisfies: $e{\cdot}x = x$ where e is the identity element of G, and $(gh){\cdot}x = g{\cdot}(h{\cdot}x)$ for every $g, h \in G$ and $x \in X$. We generalize this to sheaves.

2.3.1 Definition. Let S be a topological space, $\mathcal{G}$ a presheaf of groups on S, and $\mathcal{X}$ a presheaf of sets on S. A *left-action* of $\mathcal{G}$ on $\mathcal{X}$ consists of an action of the group $\mathcal{G}(U)$ on the set $\mathcal{X}(U)$, for all U in $\mathrm{Open}(S)$, such that for all inclusions $V \subset U$, for all $g \in \mathcal{G}(U)$ and $x \in \mathcal{X}(U)$, $(gx)|_V = (g|_V)(x|_V)$.

Equivalently, an action of $\mathcal{G}$ on $\mathcal{X}$ is a morphism of presheaves $\mathcal{G}\times\mathcal{X} \to \mathcal{X}$ such that for each U in $\mathrm{Open}(S)$, the map $(\mathcal{G}\times\mathcal{X})(U) = \mathcal{G}(U)\times\mathcal{X}(U) \to \mathcal{X}(U)$ is an action of $\mathcal{G}(U)$ on $\mathcal{X}(U)$.

If $\mathcal{G}$ and $\mathcal{X}$ are sheaves, then an *action* of $\mathcal{G}$ on $\mathcal{X}$ is an action of presheaves.

2.3.2 Remark. What we have defined are left-actions. We define right-actions similarly.

We want to take the quotient of a sheaf of sets by the action of a sheaf of groups. Here, it makes a difference if we do this for presheaves, or for sheaves.

2.3.3 Definition. Let S be a topological space, $\mathcal{X}$ a (pre)sheaf of sets on S with a right-action by a (pre)sheaf of groups $\mathcal{G}$ on S. A morphism of (pre)sheaves $q\colon \mathcal{X} \to \mathcal{Y}$ is called a *quotient* of $\mathcal{X}$ for the $\mathcal{G}$-action if q satisfies the universal property: for every morphism of (pre)sheaves $f\colon \mathcal{X} \to \mathcal{Z}$ such that for all U in $\mathrm{Open}(S)$, all $g \in \mathcal{G}(U)$, all $x \in \mathcal{X}(U)$ we have $f(U)(xg) = f(U)(x)$, there is a unique morphism of (pre)sheaves $\bar{f}\colon \mathcal{Y} \to \mathcal{Z}$ such that $f = \bar{f} \circ q$.

If such a quotient exists, then by the universal property it is unique up to unique isomorphism.

We define a presheaf $(\mathcal{X}/\mathcal{G})_p$: for every U open, $(\mathcal{X}/\mathcal{G})_p(U) := \mathcal{X}(U)/\mathcal{G}(U)$, with restriction maps induced by those of $\mathcal{X}$ and $\mathcal{G}$. The map $q\colon \mathcal{X} \to (\mathcal{X}/\mathcal{G})_p$ is a quotient. But in the category of sheaves the situation is more complicated.

2.3.4 Example. Let $S = \{-1, 0, 1\}$ with

$$\mathrm{Open}(S) = \{\emptyset, \{0\}, \{-1, 0\}, \{0, 1\}, \{-1, 0, 1\}\}.$$

Here is the diagram of open sets:

$$\begin{tikzcd}
& \{-1,0,1\} & \\
\{-1,0\} \arrow[ur] & & \{0,1\} \arrow[ul] \\
& \{0\} \arrow[ul] \arrow[ur] \arrow[uu] & \\
& \emptyset \arrow[u] &
\end{tikzcd}$$

Let now $\mathcal{X}$ be the constant sheaf $\mathbb{Z}_S$; it is in fact a sheaf of groups. And we let $\mathcal{G}$ be the subsheaf of groups with $\mathcal{G}(S) = \{0\}$, $\mathcal{G}(\{-1, 0\}) = 0$, $\mathcal{G}(\{0, 1\}) = 0$ and $\mathcal{G}(\{0\}) = \mathbb{Z}$, and we let $\mathcal{G}$ act on $\mathcal{X}$ by addition. Here are the values of $\mathcal{G}$, $\mathcal{X}$ and the presheaf quotient $(\mathcal{X}/\mathcal{G})_p$ on each open of S:

$$\begin{tikzcd}
& \mathcal{G} & & & \mathcal{X} & & & (\mathcal{X}/\mathcal{G})_p & \\
& 0 \arrow[dl] \arrow[dr] \arrow[dd] & & & \mathbb{Z} \arrow[dl] \arrow[dr] \arrow[dd] & & & \mathbb{Z} \arrow[dl] \arrow[dr] \arrow[dd] & \\
0 \arrow[dr] & & 0 \arrow[dl] & \mathbb{Z} \arrow[dr] & & \mathbb{Z} \arrow[dl] & \mathbb{Z} \arrow[dr] & & \mathbb{Z} \arrow[dl] \\
& \mathbb{Z} \arrow[d] & & & \mathbb{Z} \arrow[d] & & & 0 \arrow[d] & \\
& 0 & & & 0 & & & 0 &
\end{tikzcd}$$

The presheaf quotient $(\mathcal{X}/\mathcal{G})_p$ is not a sheaf, because

$$(\mathcal{X}/\mathcal{G})_p(S) \to (\mathcal{X}/\mathcal{G})_p(\{-1,0\}) \times (\mathcal{X}/\mathcal{G})_p(\{0,1\})$$

does not have the right image; we have the diagonal map $\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ and it should be a bijection. In other words: not all compatible systems of local sections are given by a global section.

2.3.5 Remark. The above example is well known, as $\mathcal{X}$ is the smallest topological space with an abelian sheaf $\mathcal{G}$ with non-trivial first cohomology group.

2.3.6 Theorem. *Let S be a topological space, $\mathcal{X}$ a sheaf of sets on S with a right-action by a sheaf of groups $\mathcal{G}$ on S. Then $\mathcal{X} \to (\mathcal{X}/\mathcal{G})_p \to ((\mathcal{X}/\mathcal{G})_p)^\#$ is a quotient for the action by $\mathcal{G}$ on $\mathcal{X}$. Notation: $\mathcal{X}/\mathcal{G}$.*

Proof. Let $f\colon \mathcal{X} \to \mathcal{Z}$ be a morphism of sheaves such that for all U in $\mathrm{Open}(S)$, all $g \in \mathcal{G}(U)$, all $x \in \mathcal{X}(U)$ we have $f(U)(xg) = f(U)(x)$. By the universal property of the presheaf quotient for the $\mathcal{G}$-action on $\mathcal{X}$, we have a map $(\mathcal{X}/\mathcal{G})_p \to \mathcal{Z}$. Now because $\mathcal{Z}$ is a sheaf, then the universal property of sheafification tells us that it factors uniquely through $\bar{f}\colon ((\mathcal{X}/\mathcal{G})_p)^\# \to \mathcal{Z}$. To prove the uniqueness of $\bar{f}$, suppose that $g\colon ((\mathcal{X}/\mathcal{G})_p)^\# \to \mathcal{Z}$ such that $g \circ q = \bar{f} \circ q = h$. For every $s \in S$, we have the maps on the stalks $\mathcal{X}_s \to \mathcal{Z}_s$, $h_s = g_s \circ q_s = \bar{f}_s \circ q_s$. Because q_s is a surjective map of sets, we get $g_s = \bar{f}_s$. This implies $f = g$. □

2.4 Torsors

Non-empty sets with a free and transitive group action occur frequently, and are often used to "identify the set with the group". Think of affine geometry. For example: the set of solutions of an inhomogeneous system of linear equations $Ax = b$, if non-empty, is an affine space under the vector space of solutions of the homogeneous equations $Ax = 0$, via translations. So choosing an element in the set of solutions of $Ax = b$ then translating it by any element in the set of solutions of the equations $Ax = 0$ gives a non-canonical bijection between the 2 sets.

We start with the definition of free and transitive action of a group on a set and the definition of torsor. Let G be a group and X a set with a G-action. For x in X, *the stabilizer in G of x* is the subset

$$G_x := \{g \in G : gx = x\}$$

of elements that fix x; it is a subgroup of G. For x in X, *the orbit of x under G* is the set

$$G{\cdot}x := \{y \in X : \text{there exists } g \in G \text{ such that } y = gx\} = \{gx : g \in G\}.$$

The action of G on X is *free* if for all x in X we have $G_x = \{1\}$. The action is *transitive* if for all x and y in X there is a g in G such that $y = gx$. A *torsor X for a group G* is a non-empty set X on which G acts freely and transitively. If X is a G-torsor, then for any x in X, the map $G \to X$, $g \mapsto gx$ is bijective.

We define the same properties in the context of sheaves.

2.4.1 Definition. Let S be a topological space, $\mathcal{G}$ a sheaf of groups, acting on a sheaf of sets $\mathcal{X}$.

1. For $x \in \mathcal{X}(S)$, the stabilizer $\mathcal{G}_x$ of x in $\mathcal{G}$ is the sheaf of subgroups given by $\mathcal{G}_x(U) = \mathcal{G}(U)|_{x|_U}$. It is indeed a sheaf.
2. The action of $\mathcal{G}$ on $\mathcal{X}$ is *free* if for all $U \subset S$ open, $\mathcal{G}(U)$ acts freely on $\mathcal{X}(U)$.
3. The action of $\mathcal{G}$ on $\mathcal{X}$ is *transitive* if for $U \subset S$ open, for all x and y in $\mathcal{X}(U)$, there exists an open cover $(U_i)_{(i \in I)}$ of U, and $(g_i \in \mathcal{G}(U_i))_{i \in I}$, such that for all $i \in I$, $g_i \cdot x|_{U_i} = y|_{U_i}$.

2.4.2 Definition. Let S be a topological space, $\mathcal{G}$ a sheaf of groups acting from the right on a sheaf of sets $\mathcal{X}$. Then $\mathcal{X}$ is called *right-$\mathcal{G}$-torsor* if it satisfies: the action of $\mathcal{G}$ on $\mathcal{X}$ is free and transitive, and locally $\mathcal{X}$ has sections: there is an open cover $(U_i)_{i \in I}$ of S, such that for each $i \in I$, $\mathcal{X}(U_i) \neq \emptyset$.

2.4.3 Example. Let S be a topological space, $\mathcal{G}$ a sheaf of groups acting transtively from the right on a sheaf of sets $\mathcal{X}$. For every $x, y \in \mathcal{X}(S)$ we define ${}_y\mathcal{G}_x$, *the transporter from x to y*, by:

$$\text{for } U \subset S \text{ open, } {}_y\mathcal{G}_x(U) = \{g \in \mathcal{G}(U) : g{\cdot}x|_U = y|_U\}.$$

We also define the stabiliser $\mathcal{G}_x$ of x as the transporter from x to x. Then ${}_y\mathcal{G}_x$ is a right $\mathcal{G}_x$-torsor. For a proof see Theorem 2.6.1.

For $\mathcal{X}$ a right $\mathcal{G}$-torsor on a space S, for an open set U of S and x in $\mathcal{X}(U)$, the morphism $\mathcal{G}|_U \to \mathcal{X}|_U$ defined by: for any open subset $V \subset U$, for each $g \in \mathcal{G}|_U(V)$, $g \mapsto gx|_V$, is an isomorphism of sheaves.

When X and Y are non-empty right G-sets that are free and transitive, any G-equivariant map $f\colon X \to Y$ (meaning for any $x \in X$ and $g \in G$ we have $f(xg) = f(x)g$) is an isomorphism. Let $\mathcal{G}$ be a sheaf of groups on S. We define for $\mathcal{X}$ and $\mathcal{Y}$ right $\mathcal{G}$-torsors, $f\colon \mathcal{X} \to \mathcal{Y}$ *a morphism of* $\mathcal{G}$*-torsors* if for all $U \subset S$ open and for any $x \in \mathcal{X}(U)$ and $g \in \mathcal{G}(U)$ we have $f(U)(xg) = f(U)(x)g$. We have similar result for sheaf torsors:

2.4.4 Lemma. *Let S be a topological space, $\mathcal{G}$ a sheaf of groups, and $\mathcal{X}$ and $\mathcal{Y}$ right $\mathcal{G}$-torsors. Then every morphism $f\colon \mathcal{X} \to \mathcal{Y}$ of $\mathcal{G}$-torsors is an isomorphism.*

Proof. Let U be in $\mathrm{Open}(S)$. If $\mathcal{Y}(U) = \emptyset$, then $\mathcal{X}(U) = \emptyset$ since there is no map from a non-empty set to an empty set. Assume there exists $y \in \mathcal{Y}(U)$. Then there is an open covering $(U_i)_{i\in I}$ of U such that both $\mathcal{X}(U_i)$ and $\mathcal{Y}(U_i)$ are non-empty. The maps $f(U_i)\colon \mathcal{X}(U_i) \to \mathcal{Y}(U_i)$ are bijective for all $i \in I$, hence there exists $(x_i)_{i\in I}$ such that $x_i \mapsto y|_{U_i}$. By bijectivity of the sections of $\mathcal{X}$ and $\mathcal{Y}$ on the intersections $U_i \cap U_j$, we have $x_i|_{U_i\cap U_j} = x_j|_{U_i\cap U_j}$, and they glue to a section $x \in \mathcal{X}(U)$ such that $x|_{U_i} = x_i$. Therefore $\mathcal{X}(U)$ is non-empty and we derive the same conclusion that $f(U)$ is bijective. □

Let us give a very useful example of how torsors can arise. For that purpose, we discuss sheaves of modules. See [11], Chapter II.5 for a more thorough exposition.

2.4.5 Definition. Let S be a topological space, and $\mathcal{O}$ a sheaf of rings on S. In particular, $(S, \mathcal{O})$ can also be any locally ringed space. A *sheaf of* $\mathcal{O}$*-modules* is a sheaf $\mathcal{E}$ of abelian groups, together with, for all open U in

Open(S), a map $\mathcal{O}(U) \times \mathcal{E}(U) \to \mathcal{E}(U)$ that makes $\mathcal{E}(U)$ into an $\mathcal{O}(U)$-module, such that for all inclusions $V \subset U$ of opens in Open(S), for all $f \in \mathcal{O}(U)$ and $e \in \mathcal{E}(U)$ we have $(fe)|_V = (f|_V)(e|_V)$. From now on we refer to sheaves of $\mathcal{O}$-modules simply as $\mathcal{O}$-modules.

A morphism of $\mathcal{O}$-modules $\phi\colon \mathcal{E} \to \mathcal{F}$ is a morphism of sheaves ϕ such that for all opens $U \subset S$, the morphism $\mathcal{E}(U) \to \mathcal{F}(U)$ is a morphism of $\mathcal{O}(U)$-modules.

If U is in Open(S), and if $\mathcal{E}$ is an $\mathcal{O}$-module, then $\mathcal{E}|_U$ is an $\mathcal{O}|_U$-module. If $\mathcal{E}$ and $\mathcal{F}$ are two $\mathcal{O}$-modules, the presheaves

$$U \mapsto \mathrm{Hom}_{\mathcal{O}|_U}(\mathcal{E}|_U, \mathcal{F}|_U), U \mapsto \mathrm{Isom}_{\mathcal{O}|_U}(\mathcal{E}|_U, \mathcal{F}|_U),$$

are sheaves. This is proved by gluing morphisms of sheaves. These sheaves are denoted by $\mathbf{Hom}_S(\mathcal{E}, \mathcal{F})$ and $\mathbf{Isom}_S(\mathcal{E}, \mathcal{F})$ respectively. In particular if $\mathcal{F} = \mathcal{O}$, we have $\mathcal{E}^\vee$ the *dual $\mathcal{O}$-module of $\mathcal{E}$*.

We define the *tensor product* $\mathcal{E} \otimes_{\mathcal{O}} \mathcal{F}$ of two $\mathcal{O}$-modules to be the sheaf associated to the presheaf $U \mapsto \mathcal{F}(U) \otimes_{\mathcal{O}(U)} \mathcal{G}(U)$. We define also the *tensor algebra* of $\mathcal{F}$ to be the sheaf of not necessarily commutative $\mathcal{O}$-algebras

$$\mathrm{T}(\mathcal{F}) = \mathrm{T}_{\mathcal{O}}(\mathcal{F}) = \bigoplus\nolimits_{n \geq 0} \mathrm{T}^n(\mathcal{F}).$$

Here $\mathrm{T}^0(\mathcal{F}) = \mathcal{O}$, $\mathrm{T}^1(\mathcal{F}) = \mathcal{F}$ and for $n \geq 2$ we have

$$\mathrm{T}^n(\mathcal{F}) = \mathcal{F} \otimes_{\mathcal{O}_X} \ldots \otimes_{\mathcal{O}_X} \mathcal{F} \quad (n \text{ factors})$$

We define the *exterior algebra* $\wedge(\mathcal{F})$ to be the quotient of $\mathrm{T}(\mathcal{F})$ by the two sided ideal generated by local sections $s \otimes s$ of $\mathrm{T}^2(\mathcal{F})$ where s is a local section of $\mathcal{F}$. The exterior algebra $\wedge(\mathcal{F})$ is a graded $\mathcal{O}_X$-algebra, with grading inherited from $\mathrm{T}(\mathcal{F})$. The sheaf $\wedge^n\mathcal{F}$ is the sheafification of the presheaf

$$U \longmapsto \wedge^n_{\mathcal{O}(U)}(\mathcal{F}(U)).$$

Moreover $\wedge(\mathcal{F})$ is graded-commutative, meaning that: for $U \subset S$ open, $\omega_i \in \wedge^i\mathcal{F}(U)$, and $\omega_j \in \wedge^j\mathcal{F}(U)$, $w_iw_j = (-1)^{ij}w_jw_i$.

Two $\mathcal{O}$-modules $\mathcal{E}$ and $\mathcal{F}$ are called *locally isomorphic* if there exists a cover $(U_i)_{i\in I}$ of S such that for all $i \in I$, $\mathcal{E}|_{U_i}$ is isomorphic to $\mathcal{F}|_{U_i}$, as $\mathcal{O}|_{U_i}$-modules. Let $n \in \mathbb{Z}_{\geq 0}$. A sheaf of $\mathcal{O}$-modules $\mathcal{E}$ is called *locally free of rank n* if it is locally isomorphic to $\mathcal{O}^n$ as $\mathcal{O}$-module.

2.4.6 Remark. Concretely the last statement means that there exists a cover $(U_i)_{i\in I}$ of S and $e_{i,1}, ..., e_{i,n}$ in $\mathcal{E}(U_i)$ such that for all open $V \subset U_i$ and all $e \in \mathcal{E}(V)$ there are unique $f_j \in \mathcal{O}(V), 1 \leq j \leq n$, such that $e = \Sigma_j f_j e_{i,j}|_V$.

We define the notion *locally isomorphic* for sheaves of sets, sheaves of groups, and sheaves of rings similarly.

2.4.7 Remark. Here is the statement about gluing morphisms of sheaves. Let S be a topological space and $S = \bigcup U_i$ be an open covering, where $i \in I$ an index set. Let $\mathcal{F}$, $\mathcal{G}$ be sheaves of sets (groups, rings) on S. Given a collection $f_i\colon \mathcal{F}|_{U_i} \longrightarrow \mathcal{G}|_{U_i}$ of maps of sheaves such that for all $i, j \in I$ the maps f_i, f_j restrict to the same map $\mathcal{F}|_{U_i\cap U_j} \to \mathcal{G}|_{U_i\cap U_j}$, then there exists a unique map of sheaves $f\colon \mathcal{F} \longrightarrow \mathcal{G}$, whose restriction to each U_i agrees with f_i.

2.4.8 Example. Let S be a topological space, and $\mathcal{O}$ a sheaf of rings on S. Let $n \in \mathbb{Z}_{\geq 0}$. We define the sheaf $\mathrm{GL}_n(\mathcal{O})$ of groups as follows:

$$\text{for every } U \text{ in } \mathrm{Open}(S), \mathrm{GL}_n(\mathcal{O})(U) := \mathrm{GL}_n(\mathcal{O}(U))$$

(the group of invertible n by n matrices with coefficients in $\mathcal{O}(U)$), it acts naturally on the left on the sheaf of modules $\mathcal{O}^n$. Moreover we have $\mathrm{GL}_n(\mathcal{O}) = \mathbf{Isom}_{\mathcal{O}}(\mathcal{O}^n, \mathcal{O}^n) = \mathbf{Aut}_{\mathcal{O}}(\mathcal{O}^n)$. For any locally free $\mathcal{O}$-module

$\mathcal{E}$ of rank n, the sheaf $\mathbf{Isom}_S(\mathcal{O}^n, \mathcal{E})$ is a right $\mathrm{GL}_n(\mathcal{O})$-torsor. This is because for $(U_i)_{i\in I}$ an open cover of S such that $\mathcal{E}|_{U_i}$ is isomorphic, as $\mathcal{O}|_{U_i}$-module, to the free $\mathcal{O}|_{U_i}$-module $\mathcal{O}|_{U_i}^n$, the set $\mathbf{Isom}_S(\mathcal{O}^n, \mathcal{E})(U_i)$ over U_i is non-empty and has free and transitive action by $\mathrm{GL}_n(\mathcal{O}(U_i))$.

2.5 Twisting by a torsor

First we discuss *the contracted product* for sets, not sheaves. This operation allows us to twist an object by a torsor.

Let G be a group, X a set with a right G-action, and Y a set with a left G-action. Then we define *the contracted product* $X \otimes_G Y$ to be the quotient of $X \times Y$ by the right G-action $(x, y) \cdot g = (xg, g^{-1}y)$. This is the same as dividing $X \times Y$ by the equivalence relation

$$\{((xg, y), (x, gy)) : x \in X, y \in Y, g \in G\} \subset (X \times Y)^2.$$

We have *the quotient map* $q\colon X \times Y \to X \otimes_G Y$ whose fibers are the orbits of G. This construction has the following universal property that is similar to that of tensor products of modules over rings. For every set Z, for every map $f\colon X \times Y \to Z$ such that for all $x \in X$, $y \in Y$, and $g \in G$ one has $f(xg, y) = f(x, gy)$, there is a unique map $\bar{f}\colon X \otimes_G Y \to Z$ such that $\bar{f} \circ q = f$.

Now for sheaves.

2.5.1 Definition. Let S be a topological space, $\mathcal{G}$ a sheaf of groups on S, $\mathcal{X}$ a sheaf of sets on S with right $\mathcal{G}$-action, and $\mathcal{Y}$ a sheaf of sets on S with left $\mathcal{G}$-action. We let $\mathcal{G}$ act on the right on $\mathcal{X} \times \mathcal{Y}$ by, for every U in $\mathrm{Open}(S)$,

$$\text{if } x \in \mathcal{X}(U),\ y \in \mathcal{Y}(U), \text{ and } g \in \mathcal{G}(U) \text{ then } (x, y) \cdot g = (xg, g^{-1}y).$$

We define *the contracted product* $\mathcal{X} \otimes_{\mathcal{G}} \mathcal{Y}$ to be $(\mathcal{X} \times \mathcal{Y})/\mathcal{G}$. We have the quotient map $q\colon \mathcal{X} \times \mathcal{Y} \to \mathcal{X} \otimes_{\mathcal{G}} \mathcal{Y}$. The contracted product is characterized by the universal property as following: For every sheaf of sets $\mathcal{Z}$, for every morphism of sheaves $f\colon \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ such that for all open $U \subset S$, $x \in \mathcal{X}(U)$, $y \in \mathcal{Y}(U)$, and $g \in \mathcal{G}(U)$ one has $f(U)(xg, y) = f(x, gy)$, there is a unique morphism of sheaves $\bar{f} : \mathcal{X} \otimes_{\mathcal{G}} \mathcal{Y} \to \mathcal{Z}$ such that $\bar{f} \circ q = f$.

2.5.2 Remark. The construction of $\mathcal{X} \otimes_{\mathcal{G}} \mathcal{Y}$ is functorial in $\mathcal{X}$ and $\mathcal{Y}$: for $f\colon \mathcal{X} \to \mathcal{X}'$ and $g\colon \mathcal{Y} \to \mathcal{Y}'$, we get an induced morphism

$$f \otimes_{\mathcal{G}} g\colon \mathcal{X} \otimes_{\mathcal{G}} \mathcal{Y} \to \mathcal{X}' \otimes_{\mathcal{G}} \mathcal{Y}'.$$

Now about examples of twisting processes. Again let S be a topological space, $\mathcal{G}$ a sheaf of groups on S, $\mathcal{X}$ a sheaf of sets on S with right $\mathcal{G}$-action, and $\mathcal{Y}$ a sheaf of sets on S with left $\mathcal{G}$-action. First let us make $\mathcal{G}$ as a (*trivial*) right $\mathcal{G}$-torsor by letting it act on itself by right multiplication, then $\mathcal{G} \times \mathcal{Y} \to \mathcal{Y}, (g, y) \mapsto gy$, induces an isomorphism $\mathcal{G} \otimes_{\mathcal{G}} \mathcal{Y} \to \mathcal{Y}$. It inverse is given by $\mathcal{Y} \to \mathcal{G} \times \mathcal{Y}, y \mapsto (1_{\mathcal{G}}, y)$. In particular, no sheafification is necessary for the quotient $q\colon \mathcal{G} \times \mathcal{Y} \to \mathcal{G} \otimes_{\mathcal{G}} \mathcal{Y}$. So twisting by the trivial torsor gives the same object.

Suppose now that $\mathcal{X}$ is a right $\mathcal{G}$-torsor, then $\mathcal{X} \otimes_{\mathcal{G}} \mathcal{Y}$ is locally isomorphic to $\mathcal{Y}$, as sheaf of sets on S. Indeed, for $U \subset S$ open and $x \in \mathcal{X}(U)$, we have an isomorphism of right $\mathcal{G}|_U$-torsors: $i\colon \mathcal{G}|_U(V) \to \mathcal{X}|_U(V), g|_V \mapsto x|_V \cdot g|_V$. Then $i \otimes \mathrm{id}_{\mathcal{Y}}$ is an isomorphism $(\mathcal{G} \otimes_{\mathcal{G}} \mathcal{Y})|_U \to (\mathcal{X} \otimes_{\mathcal{G}} \mathcal{Y})|_U$. And, we have seen that $(\mathcal{G} \otimes_{\mathcal{G}} \mathcal{Y})|_U$ is isomorphic to $\mathcal{Y}|_U$.

The next proposition shows that a locally free $\mathcal{O}$-module $\mathcal{E}$ on a topological space S can be recovered from the $\mathrm{GL}_n(\mathcal{O})$-torsor $\mathbf{Isom}_S(\mathcal{O}^n, \mathcal{E})$.

2.5.3 Proposition. *Let $n \in \mathbb{Z}_{\geq 0}$. Let S be a topological space, $\mathcal{O}$ a sheaf of rings on S, and $\mathcal{E}$ a locally free $\mathcal{O}$-module of rank n on S. Let $\mathbf{Isom}_S(\mathcal{O}^n, \mathcal{E})$ be as in Example 2.4.8. Then the morphism of sheaves*

$$f(U)\colon \mathbf{Isom}_S(\mathcal{O}^n, \mathcal{E})(U) \times \mathcal{O}^n(U) \to \mathcal{E}(U), \quad (\phi, s) \mapsto (\phi(U))(s)$$

factors through $q\colon \mathbf{Isom}_S(\mathcal{O}^n, \mathcal{E}) \times \mathcal{O}^n \to \mathbf{Isom}_S(\mathcal{O}^n, \mathcal{E}) \otimes_{\mathrm{GL}_n(\mathcal{O})} \mathcal{O}^n$, and induces an isomorphism

$$\mathbf{Isom}_S(\mathcal{O}^n, \mathcal{E}) \otimes_{\mathrm{GL}_n(\mathcal{O})} \mathcal{O}^n \to \mathcal{E}.$$

Proof. Let us show that f factors through q. For $\phi\colon \mathcal{O}^n|_U \to \mathcal{E}_U$ an isomorphism and s in $\mathcal{O}^n(U)$ and $g \in \mathrm{GL}_n(\mathcal{O}(U))$, we have to show that $(\phi \circ g, s)$ and $(\phi, g{\cdot}s)$ have the same image under $f(U)$. But that results from $f(\phi \circ g, s) = (\phi \circ g)s = \phi(g(s)) = f(\phi, g{\cdot}s)$.

Now we must show that $\overline{f}\colon \mathbf{Isom}_S(\mathcal{O}^n, \mathcal{E}) \otimes_{\mathrm{GL}_n(\mathcal{O})} \mathcal{O}^n \to \mathcal{E}$ is an isomorphism of sheaves. That is a local question, so we may assume that $\mathcal{E}$ is isomorphic to $\mathcal{O}^n$, and even that it *is* $\mathcal{O}^n$. But then $\mathbf{Isom}_S(\mathcal{O}^n, \mathcal{E})$ is $\mathrm{GL}_n(\mathcal{O})$, and the morphism f is the action, and we have seen above that this induces an isomorphism as desired. □

2.5.4 Lemma. *Let $n \in \mathbb{Z}_{\geq 0}$. Let S be a topological space, $\mathcal{O}$ a sheaf of rings on S, $\mathcal{G} = \mathrm{GL}_n(\mathcal{O})$, and $\mathcal{T}$ a right $\mathcal{G}$-torsor. Then we have an isomorphism of $\mathcal{G}$-torsors*

$$\mathcal{T} \to \mathbf{Isom}_S(\mathcal{O}^n, \mathcal{T} \otimes_{\mathcal{G}} \mathcal{O}^n).$$

Proof. It is sufficient to give a morphism of $\mathcal{G}$-torsors

$$\psi\colon \mathcal{T} \to \mathbf{Isom}_S(\mathcal{O}^n, \mathcal{T} \otimes_{\mathcal{G}} \mathcal{O}^n).$$

For $U \subset S$ open and $a \in \mathcal{T}(U)$, we have a map

$$\phi_a \colon \mathcal{O}^n|_U \to \mathcal{T}|_U \times \mathcal{O}^n|_U, x \mapsto (a, x).$$

This induces a map $\psi_a \colon \mathcal{O}^n|_U \to (\mathcal{T} \otimes_{\mathcal{G}} \mathcal{O}^n)|_U$. For any $g \in \mathrm{GL}_n(U)$, we have $\psi_a \circ g = \psi_{ag}$. Thus ψ is a morphism of $\mathcal{G}$-torsors. □

Next we talk about functoriality of torsors. Let S be a topological space, let $\phi \colon \mathcal{H} \to \mathcal{G}$ be a morphism of sheaves of groups on S. Then, for each right $\mathcal{H}$-torsor $\mathcal{X}$, we obtain a right $\mathcal{G}$-torsor $\mathcal{X} \otimes_{\mathcal{H}} \mathcal{G}$, where we let $\mathcal{H}$ act from the left on $\mathcal{G}$ via left multiplication via $\phi : h \cdot g := \phi(h)g$ (sections over some open $U \subset S$), and where the right action of $\mathcal{G}$ on itself provides the right $\mathcal{G}$ action on $\mathcal{X} \otimes_{\mathcal{H}} \mathcal{G}$. This construction is a functor from the category of right $\mathcal{H}$-torsors to that of right $\mathcal{G}$-torsors: $f \colon \mathcal{X} \to \mathcal{Y}$ induces $f \otimes \mathrm{id}_{\mathcal{G}} : \mathcal{X} \otimes_{\mathcal{H}} \mathcal{G} \to \mathcal{Y} \otimes_{\mathcal{H}} \mathcal{G}$.

2.5.5 Definition. Let S be a topological space, and $\mathcal{G}$ a sheaf of groups on S. Then we define $\mathrm{H}^1(S, \mathcal{G})$ to be the set of isomorphism classes of right $\mathcal{G}$-torsors on S. The isomorphism class of $\mathcal{X}$ will be denoted by $[\mathcal{X}] \in \mathrm{H}^1(S, \mathcal{G})$.

The set $\mathrm{H}^1(S, \mathcal{G})$ has a distinguished element: the isomorphism class of the trivial torsor $\mathcal{G}$ itself. Hence $\mathrm{H}^1(S, \mathcal{G})$ is actually a *pointed set*. It is called the *first cohomology set*. If $\mathcal{G}$ is commutative, then this set has a commutative group structure: $(\mathcal{T}_1, \mathcal{T}_2) \mapsto \mathcal{T}_1 \otimes_{\mathcal{G}} \mathcal{T}_2$ (there is no distinction between left and right, precisely because $\mathcal{G}$ is commutative). The inverse $\mathcal{T}^{-1}$ of $\mathcal{T}$ is $\mathcal{T}$ itself, but with $\mathcal{G}$ acting via $\mathcal{G} \to \mathcal{G}, g \mapsto g^{-1}$.

We say that an open covering $(U_i)_{i \in I}$ of S *trivialises* a torsor $\mathcal{T}$ if for all $i \in I$, $\mathcal{T}(U_i) \neq \emptyset$.

2.5.6 Example. Let S be a topological space and $\mathcal{O}$ a sheaf of rings on it. Then $\mathrm{H}^1(S, \mathrm{GL}_n(\mathcal{O}))$ is also the set of isomorphism classes of locally free $\mathcal{O}$-modules of rank n on S. This is an application of the constructions, Proposition 2.5.3, and Lemma 2.5.4. These give an equivalence of categories between the category of locally free $\mathcal{O}$-modules of rank n with morphisms only isomorphisms, and the category of right $\mathrm{GL}_n(\mathcal{O})$-torsors.

2.6 A transitive action

The following theorem is the result from sheaf theory (see also [8], Chapitre III, Corollaire 3.2.3 for this result in the context of sites) that will be applied to prove Gauss's theorem. We will formulate one long statement.

2.6.1 Theorem. *Let S be a topological space, $\mathcal{G}$ a sheaf of groups, $\mathcal{X}$ a sheaf of sets with a transitive left $\mathcal{G}$-action, and $x \in \mathcal{X}(S)$. We let $\mathcal{H} := \mathcal{G}_x$ the stabilizer of x in $\mathcal{G}$, and let $i\colon \mathcal{H} \to \mathcal{G}$ denote the inclusion. For every $y \in \mathcal{X}(S)$ we define ${}_y\mathcal{G}_x$,* the transporter from x to y, *by: for $U \subset S$ open, ${}_y\mathcal{G}_x(U) = \{g \in \mathcal{G}(U) : g{\cdot}x|_U = y|_U\}$; it is a right $\mathcal{H}$-torsor. Then $\mathcal{G}(S)$ acts on $\mathcal{X}(S)$, and we have maps*

$$\mathcal{X}(S) \xrightarrow{c} \mathrm{H}^1(S,\mathcal{H}) \xrightarrow{i} \mathrm{H}^1(S,\mathcal{G}) \tag{2.6.1.1}$$

where:

- *$c\colon \mathcal{X}(S) \to \mathrm{H}^1(S,\mathcal{H})$ sends $y \in \mathcal{X}(S)$ to the isomorphism class of ${}_y\mathcal{G}_x$;*
- *$i\colon\ \mathrm{H}^1(S,\mathcal{H}) \to \mathrm{H}^1(S,\mathcal{G})$ is the map that sends the isomorphism class of a right $\mathcal{H}$-torsor $\mathcal{X}$ to the isomorphism class of the right $\mathcal{G}$-torsor $\mathcal{X} \otimes_{\mathcal{H}} \mathcal{G}$, in other words, the map induced by $i\colon \mathcal{H} \to \mathcal{G}$.*

Then:

1. *for y_1 and y_2 in $\mathcal{X}(S)$, $c(y_1) = c(y_2)$ if and only if there exists $g \in \mathcal{G}(S)$ such that $y_2 = gy_1$;*

2. *for $\mathcal{T}$ a right $\mathcal{H}$-torsor, $\mathcal{T} \otimes_{\mathcal{H}} \mathcal{G}$ is trivial if and only if $[\mathcal{T}]$ is in the image of c;*

3. *if $\mathcal{H}$ is commutative, then for all y in $\mathcal{X}(S)$, $\mathcal{G}_y$ is naturally isomorphic to $\mathcal{H}$;*

4. *if $\mathcal{H}$ is commutative and $\mathcal{G}(S)$ is finite, then all non-empty fibers of c consist of $\#\mathcal{G}(S)/\#\mathcal{H}(S)$ elements.*

Proof. Let us first show that for $y \in \mathcal{X}(S)$, the presheaf ${}_y\mathcal{G}_x$ is a sheaf. Let U be an open subset of S, and $(U_i)_{i \in I}$ an open cover of it with I a set, and, for $i \in I, g_i$ in ${}_y\mathcal{G}_x(U_i)$, such that for all $(i,j) \in I^2, g_i|_{U_{i,j}} = g_j|_{U_{i,j}}$ in $\mathcal{G}(U_{i,j})$. Note that the g_i are in $\mathcal{G}(U_i)$. As $\mathcal{G}$ is a sheaf, there is a unique $g \in \mathcal{G}(U)$ such that for all $i \in I, g_i = g|_{U_i}$. Then we have $g \cdot x|_U$ in $\mathcal{X}(U)$. Then for all i in I we have $(g \cdot x|_U)|_{U_i} = g|_{U_i} x|_{U_i} = g_i x|_{U_i} = y|_{U_i}$, hence, as $\mathcal{X}$ is a sheaf, $(g \cdot x|_U) = y|_U$, hence g is in ${}_y\mathcal{G}_x(U)$.

Let us now show that for y in $\mathcal{X}(S)$, we have that ${}_y\mathcal{G}_x$ is a right $\mathcal{H}$-torsor. First the right $\mathcal{H}$-action. For $U \subset S$ open, h in $\mathcal{H}(U)$ and g in ${}_y\mathcal{G}_x(U)$, we have gh in $\mathcal{G}(U)$. By definition of $\mathcal{H}$, we have $h \cdot x|_U = x|_U$, and $g \cdot x|_U = y|_U$. Then $(gh) \cdot x|_U = y|_U$. Hence indeed gh is in ${}_y\mathcal{G}_x(U)$. Let us show that for all U the action of $\mathcal{H}(U)$ on ${}_y\mathcal{G}_x(U)$ is free. Let g be in ${}_y\mathcal{G}_x(U)$ and h in $\mathcal{H}(U)$ such that $gh = g$. Then $h = g^{-1}gh = g^{-1}g = 1$ in $\mathcal{G}(U)$. So the action is free. Now we show that the action of $\mathcal{H}$ on ${}_y\mathcal{G}_x$ is transitive. Let U be open, g_1 and g_2 in ${}_y\mathcal{G}_x(U)$. Then $g_2 = g_1 \cdot (g_1^{-1}g_2)$, and $h := g_1^{-1}g_2$ is in $\mathcal{H}(U)$ because $h \cdot x|_U = (g_1^{-1}g_2) \cdot x|_U = g_1^{-1} \cdot y|_U = x|_U$. Finally, we show that locally ${}_y\mathcal{G}_x$ has sections. But this is because $\mathcal{G}$ acts transitively on $\mathcal{X}$: there is a cover $(U_i)_{i \in I}$ with I a set and $g_i \in \mathcal{G}(U_i)$ such that $g_i \cdot x|_{U_i} = y|_{U_i}$ in $\mathcal{X}(U_i)$.

Let us prove (1). Let y_1 and y_2 in $\mathcal{X}(S)$.

Suppose that g is in $\mathcal{G}(S)$ and that $gy_1 = y_2$. Then left multiplication by g in $\mathcal{G}$ gives us an isomorphism of right $\mathcal{H}$-torsors from ${}_{y_1}\mathcal{G}_x$ to ${}_{y_2}\mathcal{G}_x$.

Suppose now that $c(y_1) = c(y_2)$. We have to show that there is a g in $\mathcal{G}(S)$ such that $gy_1 = y_2$. The assumption is that ${}_{y_1}\mathcal{G}_x$ and ${}_{y_2}\mathcal{G}_x$ are isomorphic. So let ϕ be an isomorphism from ${}_{y_1}\mathcal{G}_x$ to ${}_{y_2}\mathcal{G}_x$. Each of point in S has an open neighborhood U such that there exists a t in ${}_{y_1}\mathcal{G}_x(U)$. For such a t, we have $\phi(t)$ in ${}_{y_2}\mathcal{G}_x(U)$, and hence $(\phi(t))t^{-1}$ in $\mathcal{G}(U)$ with $(\phi(t))t^{-1}\cdot y_1 = \phi(t)x = y_2$. We claim that this element $(\phi(t))t^{-1}$ does not depend on the choice of t. Any t' in ${}_{y_1}\mathcal{G}_x(U)$ is of the form th for a unique h in $\mathcal{H}(U)$. Then we have

$$\phi(t')t'^{-1} = \phi(th)(th)^{-1} = \phi(t)hh^{-1}t^{-1} = \phi(t)t^{-1}\,.$$

So we let g_U be this element $\phi(t)t^{-1}$ of $\mathcal{G}(U)$. These g_U form a compatible collection of local sections of $\mathcal{G}$: for all U and V on which ${}_{y_1}\mathcal{G}_x$ has a section, g_U and g_V have the same restriction to $U \cap V$. As $\mathcal{G}$ is a sheaf, there is a unique g in $\mathcal{G}(S)$ such that for all U as above, $g_U = g|_U$. For each U we have $(gy_1)|_U = g|_U y_1|_U = g_U y_1|_U = y_2|_U$, hence (now using that $\mathcal{X}$ is a sheaf), $gy_1 = y_2$.

Let us prove (2). Let y be in $\mathcal{X}(S)$. We must show that ${}_y\mathcal{G}_x \otimes_{\mathcal{H}} \mathcal{G}$ is trivial, that is, that it has a global section. Let s be in S. As ${}_y\mathcal{G}_x$ has sections locally, s has an open neighborhood U such that ${}_y\mathcal{G}_x(U)$ is not empty. Let us take such a U and a g in ${}_y\mathcal{G}_x(U)$. This g is not unique, but any other g' in ${}_y\mathcal{G}_x(U)$ is of the form gh for a unique h in $\mathcal{H}(U)$. Now recall that ${}_y\mathcal{G}_x \otimes_{\mathcal{H}} \mathcal{G}$ is the quotient of ${}_y\mathcal{G}_x \times \mathcal{G}$ by $\mathcal{H}$, with $h \in \mathcal{H}(U)$ acting on $({}_y\mathcal{G}_x \times \mathcal{G})(U)$ by sending (g_1, g_2) to $(g_1h, h^{-1}g_2)$. Consider the element (g, g^{-1}) of $({}_y\mathcal{G}_x \times \mathcal{G})(U)$. This element depends on our choice of g, but we claim that modulo the action of $\mathcal{H}(U)$ it does *not* depend on that choice.

Here is why:

$$(g', g'^{-1}) = (gh, h^{-1}g) = (g, g^{-1})\cdot h\,.$$

Hence the image of (g, g^{-1}) in $({}_y\mathcal{G}_x \otimes_{\mathcal{H}} \mathcal{G})(U)$ does not depend on the choice of g, and we denote it by f_U. But then for V open in S such that ${}_y\mathcal{G}_x(V)$ is not empty, we have an f_V in $({}_y\mathcal{G}_x \otimes_{\mathcal{H}} \mathcal{G})(V)$, and by construction, we have, for all such V and V' that $f_V = f_{V'}$ in $({}_y\mathcal{G}_x \otimes_{\mathcal{H}} \mathcal{G})(V \cap V')$. As $({}_y\mathcal{G}_x \otimes_{\mathcal{H}} \mathcal{G})$ is a sheaf, this means that there is a unique f in $({}_y\mathcal{G}_x \otimes_{\mathcal{H}} \mathcal{G})(S)$ such that for all V with $({}_y\mathcal{G}_x \otimes_{\mathcal{H}} \mathcal{G})(V) \neq \emptyset$, $f|_V = f_V$.

Let us now show the opposite: let $\mathcal{T}$ be a right $\mathcal{H}$-torsor such that $\mathcal{T} \otimes_{\mathcal{H}} \mathcal{G}$ is trivial. We have to show that there is a y in $\mathcal{X}(S)$ such that $\mathcal{T}$ is isomorphic to ${}_y\mathcal{G}_x$. Let f be in $(\mathcal{T} \otimes_{\mathcal{H}} \mathcal{G})(S)$. Recall that $\mathcal{T} \otimes_{\mathcal{H}} \mathcal{G}$ is the quotient of $\mathcal{T} \times \mathcal{G}$ by $\mathcal{H}$. Each point in S has an open neighborhood U such that there exists a (t, g) in $(\mathcal{T} \times \mathcal{G})(U)$ giving $f|_U$, and any such (t', g') is of the form $(th, h^{-1}g)$ for a unique h in $\mathcal{H}(U)$. We define $y_U := g^{-1}x|_U$, then y_U is independent of the choice of (t, g) because $g'^{-1}x|_U = g^{-1}hx|_U = g^{-1}x|_U$. Therefore, there exists a unique $y \in \mathcal{X}(S)$ such that for all open U in S on which f can be represented by a section of $\mathcal{T} \times \mathcal{G}$ we have $y_U = y|_U$. Let us now show that $\mathcal{T}$ is isomorphic to ${}_y\mathcal{G}_x$. On each U as above, both $\mathcal{T}$ and ${}_y\mathcal{G}_x$ are trivial $\mathcal{H}$-torsors, because we have t is in $\mathcal{T}(U)$ and g^{-1} is in ${}_y\mathcal{G}_x(U)$. Therefore, on each U as above, we have a unique morphism ϕ_U from $\mathcal{T}|_U$ to ${}_y\mathcal{G}_x|_U$ that sends t to g^{-1}. We claim that ϕ_U does not depend on the choice of (t, g). Here is why:

$$\phi_U(t') = \phi_U(th) = \phi_U(t)h = g^{-1}h = (h^{-1}g)^{-1} = g'^{-1}\,.$$

Therefore, there is a unique ϕ from $\mathcal{T}$ to ${}_y\mathcal{G}_x$ such that for all U as above, $\phi_U = \phi|_U$. As all morphisms between $\mathcal{H}$-torsors are isomorphisms, ϕ is an isomorphism.

Let us prove (3). So now we assume that $\mathcal{H}$ is commutative. Let y be in $\mathcal{X}(S)$. Each point of S has an open neighborhood U such that there exists a g in ${}_y\mathcal{G}_x(U)$. Then, for each $V \subset U$, we have the map $c_g(V)\colon \mathcal{G}_x(V) \to \mathcal{G}_y(V)$ that sends h to ghg^{-1}. This map is an isomorphism of groups, and it is compatible with the restriction maps for $V' \subset V$, that is, c_g is an isomorphism of sheaves of groups from $\mathcal{G}_x|_U$ to $\mathcal{G}_y|_U$. We claim that c_g is in fact independent of the choice of g. Any g' in ${}_y\mathcal{G}_x(U)$ is of the form gh for a unique h in $\mathcal{H}(U)$. Then, for $V \subset U$:

$$c_{g'}(V)\colon k \mapsto g'kg'^{-1} = ghkh^{-1}g^{-1} = gkg^{-1} = (c_g(V))(k)\,.$$

Hence we can label the c_g as c_U, as they only depend on U. But then the $c_U\colon \mathcal{G}_x|_U \to \mathcal{G}_y|_U$ are a compatible collection of isomorphisms. Hence there exists a unique isomorphism $c\colon \mathcal{G}_x \to \mathcal{G}_y$ such that for each U as above, $c_U = c|_U$.

Let us prove (4). By (1), the fibers of c are the orbits of $\mathcal{G}(S)$ acting on $\mathcal{X}(S)$. For y in $\mathcal{X}(S)$ the map $\mathcal{G}(S) \to \mathcal{X}(S)$, $g \mapsto gy$ factors through the quotient map $\mathcal{G}(S) \to \mathcal{G}(S)/\mathcal{G}_y(S)$, and gives a bijection from $\mathcal{G}(S)/\mathcal{G}_y(S)$ to the $\mathcal{G}(S)$-orbit of y. Thus the number of elements in the orbit of y in $\mathcal{X}(S)$ is equal to $\#(\mathcal{G}(S)/\mathcal{G}_y(S))$. Since $\mathcal{G}(S)$ is finite, it is equal to $\#\mathcal{G}(S)/\#\mathcal{G}_y(S)$. By (3), we have, for all y in $\mathcal{X}(S)$, an isomorphism $\mathcal{H} \to \mathcal{G}_y$, in particular $\#\mathcal{G}_y(S) = \#\mathcal{H}(S)$, which shows that all $\mathcal{G}(S)$-orbits in $\mathcal{X}(S)$ have $\#\mathcal{G}(S)/\#\mathcal{H}(S)$ elements. □

The following lemma will be used in Chapter 4.

2.6.2 Lemma. *Let S be a topological space, and $\mathcal{G}$ a sheaf of groups, $\mathcal{X}$ a sheaf of sets with a transitive left $\mathcal{G}$-action, and $x \in \mathcal{X}(S)$. We let $\mathcal{H} := \mathcal{G}_x$ the stabilizer of x in $\mathcal{G}$, and let $i\colon \mathcal{H} \to \mathcal{G}$ denote the inclusion. Let y_1 and y_2 be in $\mathcal{X}(S)$. Then ${}_{y_2}\mathcal{G}_x$ is stable under the action of $\mathcal{H}$ on*

$\mathcal{G}$ by left translations, and that it is a left $\mathcal{H}$-torsor. The morphism of sheaves ${}_{y_1}\mathcal{G}_x(U) \times {}_x\mathcal{G}_{y_2}(U) \to {}_{y_1}\mathcal{G}_{y_2}(U)$, sending (g_1, g_2) to g_1g_2, induces an isomorphism of sheaves ${}_{y_1}\mathcal{G}_x \otimes_{\mathcal{H}} {}_x\mathcal{G}_{y_2} \to {}_{y_1}\mathcal{G}_{y_2}$.

Proof. It is clear that ${}_x\mathcal{G}_{y_2}$ is a left $\mathcal{H}$-torsor. The morphism of sheaves

$$ {}_{y_1}\mathcal{G}_x(U) \times {}_x\mathcal{G}_{y_2}(U) \to {}_{y_1}\mathcal{G}_{y_2}(U), $$

sending (g_1, g_2) to g_1g_2, factors through ${}_{y_1}\mathcal{G}_x \otimes_{\mathcal{H}} {}_x\mathcal{G}_{y_2} \to {}_{y_1}\mathcal{G}_{y_2}$, because for every $U \subset S$ open, and $h \in \mathcal{H}(U)$, $(g_1h, h^{-1}g_2)$ and (g_1, g_2) are mapped to the same element g_1g_2.

The map ${}_{y_1}\mathcal{G}_x \otimes_{\mathcal{H}} {}_x\mathcal{G}_{y_2} \to {}_{y_1}\mathcal{G}_{y_2}$ is a morphism of left-$\mathcal{G}_{y_1}$-torsors and therefore an isomorphism. Note that it is useful also to see ${}_{y_1}\mathcal{G}_{y_2}$ as a bitorsor, that is the action by $\mathcal{G}_{y_2}$ on the right, and the $\mathcal{G}_{y_1}$ on the left. □

We want to use 2.6.1 to prove Gauss's theorem on sums of 3 squares. To state the theorem, we need to introduce the notion of Picard group for a ring, that is defined as the Picard group of the spectrum of a ring with its Zariski topology.

2.7 The Zariski topology on the spectrum of a ring

The material of this and the next section can be found in [11]. It will be almost only be used for the rings $\mathbb{Z}$ and orders in imaginary quadratic fields.

Unless stated otherwise, we assume, in this thesis, that all rings are commutative with identity element 1. To any ring A we associate a topological space together with a sheaf of rings on it, called $\mathrm{Spec}(A)$. The topology defined is called the Zariski topology on $\mathrm{Spec}(A)$. Now let us begin with the definition of the spectrum of a ring, that is the set of prime ideals of a ring.

Let A be a ring. Then we let $\mathrm{Spec}(A)$ be the set of prime ideals of A, that is, the ideals $s \subset A$ such that A/s is an integral domain. For $s \in \mathrm{Spec}(A)$, we have the quotient A/s which is an integral domain, and we let $\kappa(s)$ be the field of fractions of A/s. We call $\kappa(s)$ the residue field at s. For f in A, and s in $\mathrm{Spec}(A)$, we call the image of f in $\kappa(s)$ the *value* $f(s)$ of f at s, and so f gives a function on $\mathrm{Spec}(A)$ with values in fields, but the field depends on the point where one takes the value. We define the *Zariski topology* on $\mathrm{Spec}(A)$: the closed subsets are the sets of the form $Z(T)$, for T a subset of A, and

$$Z(T) = \{s \in \mathrm{Spec}(A) : \forall f \in T, f(s) = 0 \text{ in } \kappa(s)\} = \{s \in \mathrm{Spec}(A) : s \supset T\}.$$

2.7.1 Proposition. *Let A be a ring. We have the following properties:*

1. *$Z(A) = \emptyset$ and $Z((0)) = \mathrm{Spec}(A)$.*

2. *For T_1 and T_2 are subsets of A, $Z(T_1) \cup Z(T_2) = Z(T_1 \cdot T_2)$, here $T_1 \cdot T_2$ is the set $\{f_1 f_2 : f_1 \in T_1, f_2 \in T_2\}$.*

3. *Let $(T_i)_i$ be a family of subsets of A. Then $\bigcap_i Z(T_i) = Z\big(\bigcup_i T_i\big)$.*

Proof. It is clear that $Z(A) = \emptyset$ and $Z((0)) = \mathrm{Spec}(A)$. If $s \in Z(T_1) \cup Z(T_2)$, then it follows immediately from the definition that $s \in Z(T_1 \cdot T_2)$. Now assume that s is in $Z(T_1 \cdot T_2)$, and that s is not in $Z(T_1)$. Then there is an f_1 in T_1 such that $f_1(s) \neq 0$. Now let g be any element in T_2. As $f_1 g$ is in $T_1 \cdot T_2$, we have $(f_1 g)(s) = 0$. But $(f_1 g)(s) = f_1(s) g(s)$ in $\kappa(s)$, and $f_1(s) \neq 0$, hence $g(s) = 0$ and $s \in Z(T_2)$. For the last statement, both inclusions are clear from the definition. □

For each f in A, we have the closed subset $Z(f)$ of $\mathrm{Spec}(A)$, and the complement $D(f) := \mathrm{Spec}(A) - Z(f)$ which is open in $\mathrm{Spec}(A)$. The sets of the form $D(f)$ constitute a base of open subsets on $\mathrm{Spec}(A)$. Indeed, every open subset of $\mathrm{Spec}(A)$ is of the form $\mathrm{Spec}(A) - Z(T)$ for some subset T of A. This is equal to the union of the $D(f)$ where f runs through the elements of T.

We define a sheaf of rings $\mathcal{O}$ on $\mathrm{Spec}(A)$. For each f in A, we have a ring morphism $\psi_f \colon A \to A_f$ that has the universal property that $\psi_f(f)$ is invertible, and for any ring morphism $\phi : A \to B$ such that $\phi(f)$ is invertible, there is a unique morphism $\phi' \colon A_f \to B$ such that $\phi = \phi' \circ \psi_f$. This defines $A \to A_f$ (up to unique isomorphism); it is the localization of A with respect to the multiplicative system $\{f^n : n \in \mathbb{Z}_{\geq 0}\}$. We would like to define $\mathcal{O}(D(f)) = A_f$, but for that we have to show that if $D(f) = D(g)$, then $A_f = A_g$. We also have to define restriction maps for inclusions $D(g) \subset D(f)$. If f and g are in A and $D(g) \subset D(f)$, then there are $n > 0$ and $a \in A$ such that $g^n = af$, and so by the universal property of ψ_f, there is a unique morphism $\psi_{f,g} : A_f \to A_g$ such that $\psi_g = \psi_{f,g} \circ \psi_f$. The $\psi_{f,g}$ should be the restriction map $\mathcal{O}(D(f)) \to \mathcal{O}(D(g))$. For every $f, g, h \in A$ such that $D(h) \subset D(g) \subset D(f)$, by the universal property of ψ_f, we have $\psi_{f,h} = \psi_{g,h} \circ \psi_{f,g}$. In particular if $D(f) = D(g)$, then $\psi_{f,g} \circ \psi_{g,f} = \mathrm{id}_{A_g}$ and $\psi_{g,f} \circ \psi_{f,g} = \mathrm{id}_{A_f}$. These give $\mathcal{O}$ as a presheaf of rings on the collection of principal opens $D(f)$ of $\mathrm{Spec}(A)$ (see [13] Chapter 2, Remark 2.6 for the notions of presheaf and sheaf on a basis for the topology, and Proposition 3.1 for a proof that $\mathcal{O}$ is a sheaf).

Moreover for any $s \in \mathrm{Spec}(A)$, the stalk $\mathcal{O}_s$ is canonically isomorphic to A_s, the localization of A at the prime ideal s. The canonical homomorphism $\psi : \mathrm{colim}_{f \notin s} A_f \to A_s$ is an isomorphism. It is surjective because every element $\alpha \in A_s$ can be written as $\alpha = af^{-1}$ for some $a \in A, f \notin s$ and is injective because if $x = af^{-n} \in A_f$ where $f \notin s$ is mapped to 0 in A_s, then there exists a $g \notin s$ such that $ga = 0$, so $x = 0$ in A_{gf}.

We will show a lemma that we will use several times.

2.7.2 Lemma. *Let A be an integral domain, with field of fractions K. Let η be* the generic point *of $S = \mathrm{Spec}(A)$ corresponding to the prime ideal* (0). *Then the local ring $\mathcal{O}_{S,\eta}$ at η is equal to K. Moreover, for every non-empty open subset U of S, we have η is in U, and the canonical homomorphism $\mathcal{O}_S(U) \to \mathcal{O}_{S,\eta}$ is injective. If $V \subset U$ are two non-empty open subsets of S, then the restriction map $\mathcal{O}_S(U) \to \mathcal{O}_S(V)$ is also injective.*

Proof. We have seen above that $\mathcal{O}_{S,\eta}$ is the localization of A with respect to the prime ideal (0), which is equal to K. If $U = D(f)$ for some $f \in A$, then $\mathcal{O}_S(U) = A_f \subset K$. In the general case, let $U = \cup_i D(f_i)$, if $s \in \mathcal{O}_S(U)$ is mapped to 0 in K, then $s|_{D(f_i)} = 0$ for every i, so $s = 0$. Therefore $\mathcal{O}_S(U) \to K$ is injective. This implies the injectivity of $\mathcal{O}_S(U) \to \mathcal{O}_S(V)$. □

This means that for an integral domain A, $\mathcal{O}_{\mathrm{Spec}(A)}$ is a subsheaf of the constant sheaf $K = \mathrm{Frac}(A)$.

2.7.3 Example. Let $S = \mathrm{Spec}(\mathbb{Z})$. A non-empty open subset of S is of the form $D(n)$, where n is an non-zero integer. We have $\mathcal{O}_S(D(n)) = \mathbb{Z}[1/n] \subset \mathbb{Q}$. A rational number a/b with $(a, b) = 1$ belongs to $\mathcal{O}_S(D(n))$ if and only if every prime number dividing b also divides n.

We prove the following proposition, that generalizes the lemma above for the ring $A = \mathrm{Spec}(\mathbb{Z})$.

2.7.4 Proposition. *Let $n \in \mathbb{N}$. Let $S =$* $\mathrm{Spec}(\mathbb{Z})$ *with its Zariski topology, η the generic point, and $\mathcal{M}$ a locally free $\mathcal{O}_S$-module of rank n. Then for any* *non-empty open subset U of S, the canonical homomorphism $\mathcal{M}(U) \to \mathcal{M}_\eta$ is injective. If $V \subset U$ are two non-empty open subsets of S, then the restriction map $\mathcal{M}(U) \to \mathcal{M}(V)$ is also injective. Moreover, $\mathcal{M}(S)$ is free of rank n as $\mathbb{Z}$-module.*

Proof. Let U be a non-empty open subset of S, then η is in U. Let $(U_i)_{i\in I}$ be an open covering of U such that for every i, U_i is non-empty and we have an isomorphism $\phi_i \colon \mathcal{O}^n_{U_i} \to \mathcal{M}|_{U_i}$. Since $\mathcal{M}$ is a sheaf, we have

$$0 \to \mathcal{M}(U) \to \prod\nolimits_i \mathcal{M}(U_i).$$

We have also the following commutative diagram

$$\begin{tikzcd}
\mathcal{O}(U_i)^n \arrow[r, "\phi_i(U_i)", "\sim"'] \arrow[d] & \mathcal{M}(U_i) \arrow[d] \\
\mathbb{Q}^n = \mathcal{O}^n_\eta \arrow[r, "\phi_{i,\eta}", "\sim"'] & \mathcal{M}_\eta,
\end{tikzcd}$$

Since $\mathcal{O}(U_i)^n \to \mathcal{O}^n_\eta$ is injective, we have $\mathcal{M}(U_i) \to \mathcal{M}_\eta$ is also injective. Therefore $\mathcal{M}(U) \to \mathcal{M}_\eta$ is injective. This also implies for $V \subset U$ two non-empty open subsets of S, $\mathcal{M}(U) \to \mathcal{M}(V)$ is injective.

We have an injection $\mathcal{M}(S) \to \mathcal{M}_\eta \simeq \mathbb{Q}^n$. In particular $\mathcal{M}(S)$ is a torsion free $\mathbb{Z}$-module. So to prove that $\mathcal{M}(S)$ is free of rank n, it is sufficient to show that $\mathcal{M}(S)$ is a finitely generated $\mathbb{Z}$-module. First we will show that given a section $t \in \mathcal{M}(D(f))$ of $\mathcal{M}$ over the open set $D(f)$, then for some $N > 0, f^N t$ extends to a global section of $\mathcal{M}$ over S. Since S is quasi compact, there exists a finite open covering $(U_j)_{j\in J}$ of S, and $U_j = D(f_j)$ for some $f_j \in \mathbb{Z}$, such that for all $j \in J$, $\mathcal{O}^n|_{U_j}$ is isomorphic to $\mathcal{M}|_{U_i}$, as $\mathcal{O}|_{U_j}$-modules. For each $j \in J$, we consider the element $t|_{U_j} \in \mathcal{M}(D(ff_j)) \simeq \mathbb{Z}[1/ff_j]^n$. By definition of localization, there exists an integer $n \geq 0$ and a unique $t_j \in \mathcal{M}(D(f_j)) \simeq \mathbb{Z}[1/f_j]^n$ such that

$t_j|_{D(ff_j)} = f^n t|_{D(ff_j)}$. The integer n may depend on j, but we take one large enough to work for all j. These t_j are compatible, and show that $f^n t$ extends uniquely to S.

We consider the dual $\mathcal{O}$-module $\mathcal{M}^\vee := \mathbf{Hom}_S(\mathcal{M}, \mathcal{O})$. It is also a locally free sheaf of rank n and $(\mathcal{M}^\vee)^\vee = \mathcal{M}$ (see [11] Chapter II, Exercise 5.1). By definition of locally free module, there exist $e_{j,1}, ..., e_{j,n}$ in $\mathcal{M}^\vee(U_j)$ such that for all open $V \subset U_j$ and all $e \in \mathcal{M}^\vee(V)$ there are unique $a_k \in \mathcal{O}(V), 1 \leq k \leq n$, such that $e = \Sigma_k a_k e_{j,k}|_V$. By the above discussion, there exists an integer N such that $f_j^N e_{j,i} \in \mathcal{M}^\vee(S)$ for all $j \in J$ and $i = 1, ..., n$ and we get a surjective map of sheaves

$$\mathcal{O}^{J\times[n]} \to \mathcal{M}^\vee, E_{j,i} \mapsto f_j^N e_{j,i},$$

where $(E_{j,i})$ is the standard basis for $\mathcal{O}^{J\times[n]}$. By taking the dual of the surjective map above, we have an injective map of sheaves

$$0 \to (\mathcal{M}^\vee)^\vee \to (\mathcal{O}^{J\times[n]})^\vee.$$

In particular we have an injective map between the set of global sections

$$0 \to \mathcal{M}(S) \to \mathbb{Z}^{J\times[n]}.$$

As submodules of free $\mathbb{Z}$-modules of finite rank are free of finite rank, $\mathcal{M}(S)$ is finitely generated. □

2.8 Cohomology groups and Picard groups

Let $\mathcal{O}$ be a sheaf of rings on a topological space S. In this section we give an isomorphism of groups between $\mathrm{H}^1(S, \mathcal{O}^\times)$ and the groups of isomorphism classes of invertible $\mathcal{O}$-modules. References for this section are [11], Chapter II, Section 6 and [10], Chapter V.

2.8.1 Definition. Let S be a topological space, and $\mathcal{O}$ a sheaf of rings on S. Then $\mathrm{Pic}(S, \mathcal{O})$ is the set of isomorphism classes of locally free $\mathcal{O}$-modules of rank one, also called invertible $\mathcal{O}$-modules. The class of an invertible $\mathcal{O}$-module $\mathcal{L}$ is denoted by $[\mathcal{L}]$. If the sheaf $\mathcal{O}$ is clear in the context, for simplicity we write it as $\mathrm{Pic}(S)$. On this set $\mathrm{Pic}(S)$, there is a structure of commutative group: $[\mathcal{L}_1] \cdot [\mathcal{L}_2] = [\mathcal{L}_1 \otimes_{\mathcal{O}} \mathcal{L}_2]$, and $[\mathcal{L}]^{-1} = [\mathcal{L}^\vee]$, where $\mathcal{L}^\vee = \mathbf{Hom}_{\mathcal{O}}(\mathcal{L}, \mathcal{O})$ is the dual of $\mathcal{L}$.

The equivalence of invertible $\mathcal{O}$-modules with $\mathcal{O}^\times$-torsors (where $\mathcal{L}$ corresponds to $\mathbf{Isom}_{\mathcal{O}}(\mathcal{O}, \mathcal{L})$) shows that $\mathrm{Pic}(S, \mathcal{O}) = \mathrm{H}^1(S, \mathcal{O}^\times)$. To see that the group structures between the two sets are the same, we prove that for two invertible $\mathcal{O}$-modules $\mathcal{L}_1, \mathcal{L}_2$, we have an isomorphism of sheaves of sets

$$\bar{\phi}\colon \mathbf{Isom}_{\mathcal{O}}(\mathcal{O}, \mathcal{L}_1) \otimes_{\mathcal{O}^\times} \mathbf{Isom}_{\mathcal{O}}(\mathcal{O}, \mathcal{L}_2) \simeq \mathbf{Isom}_{\mathcal{O}}(\mathcal{O}, \mathcal{L}_1 \otimes_{\mathcal{O}} \mathcal{L}_2).$$

Indeed, for any open subset U of S such that $\mathcal{L}_1|_U$ and $\mathcal{L}_2|_U$ are isomorphic to $\mathcal{O}|_U$, we can send $(f_1, f_2) \in \mathbf{Isom}_{\mathcal{O}}(\mathcal{O}, \mathcal{L}_1) \times \mathbf{Isom}_{\mathcal{O}}(\mathcal{O}, \mathcal{L}_2)|_U$ to $f_1 \otimes f_2 \in \mathbf{Isom}_{\mathcal{O}}(\mathcal{O}, \mathcal{L}_1 \otimes_{\mathcal{O}} \mathcal{L}_2)|_U$, where for any $V \subset U$ and $a \in \mathcal{O}(V)$: $(f_1 \otimes f_2)(a) = f_1(a) \otimes f_2(a)$. This morphism factors through

$$q\colon \mathbf{Isom}_{\mathcal{O}}(\mathcal{O}, \mathcal{L}_1) \times \mathbf{Isom}_{\mathcal{O}}(\mathcal{O}, \mathcal{L}_2)|_U \to \mathbf{Isom}_{\mathcal{O}}(\mathcal{O}, \mathcal{L}_1) \otimes_{\mathcal{O}^\times} \mathbf{Isom}_{\mathcal{O}}(\mathcal{O}, \mathcal{L}_2)|_U,$$

because for any $g \in \mathcal{O}(U)^\times$ we have

$$(f_1 \cdot g \otimes g^{-1} \cdot f_2)(a) = f_1(a) \cdot g \otimes g^{-1} \cdot f_2(a) = f_1(a) \otimes f_2(a).$$

The morphism $\bar{\phi}$ is an isomorphism of sheaves of sets, since locally all the sheaves are isomorphic to $\mathcal{O}$.

2.8.2 Definition. Let A be a ring. We define the *Picard group* $\mathrm{Pic}(A)$ of a ring A as $\mathrm{Pic}(\mathrm{Spec}(A), \mathcal{O}_{\mathrm{Spec}(A)})$, where we give the Zariski topology on $\mathrm{Spec}(A)$.

This is the same as the class group of invertible fractional ideals when A is an order in a number field (finite field extension of $\mathbb{Q}$). For such A, $\mathrm{Pic}(A)$ is a finite group, and it measures how much invertible ideals are not principal, and, if A is the ring of integers, $\mathrm{Pic}(A)$ is the obstruction to unique factorization in A.

For $\mathcal{G}$ a sheaf of (not necessarily commutative) groups, we will see that the set $\mathrm{H}^1(S, \mathcal{G})$ also classifies cohomologous 1-cocycles on the topological space S.

2.8.3 Definition. Let S be a topological space, and $\mathcal{G}$ a sheaf of (not necessarily commutative) groups. Suppose we have $\mathcal{U} = (U_i)_{i\in I}$ an open covering of S. A 1-*cocycle for* $\mathcal{U}$ *with values in* $\mathcal{G}$ is a family $g := (g_{ij})_{(i,j)\in I\times I}$, with $g_{ij} \in \mathcal{G}(U_i \cap U_j)$, such that in the triple intersection $U_i \cap U_j \cap U_k$ we have $g_{ik} = g_{ij} \cdot g_{jk}$. Two cocycles g and g' are *cohomologous*, denoted $g \sim g'$, if there is a family $(h_i)_{i\in I}$, with $h_i \in \mathcal{G}(U_i)$, such that in the intersection $U_i \cap U_j$ we have $g'_{ij} = h_i \cdot g_{ij} \cdot h_j^{-1}$. The set 1-cocycles modulo the equivalence relation of being cohomologous is denoted $\check{\mathrm{H}}^1(\mathcal{U}, \mathcal{G})$. It is not in general a group, but it does have a distinguished element represented by 1-cocycle $g = (g_{ij})_{(i,j)\in I\times I}$ with $g_{ij} = 1$ for all i, j.

A second open covering $\mathcal{V} = (V_j)_{j\in J}$ of S is called a *refinement* of $\mathcal{U}$ if there is a map of sets $\phi\colon J \to I$ such that for all $j \in J$, $V_j \subset U_{\phi(j)}$. This induces a restriction map from $\check{\mathrm{H}}^1(\mathcal{U}, \mathcal{G})$ to $\check{\mathrm{H}}^1(\mathcal{V}, \mathcal{G})$. We may pass to the colimit over all open coverings, and so we obtain the first *Čech cohomology set*

$$\check{\mathrm{H}}^1(S, \mathcal{G}) = \mathrm{colim}_{\mathcal{U}}\, \check{\mathrm{H}}^1(\mathcal{U}, \mathcal{G}).$$

Now given a left-$\mathcal{G}$-torsor $\mathcal{T}$, and an open covering $\mathcal{U} = (U_i S)_{i\in I}$ of S that trivialises $\mathcal{T}$, that is, there exists a family $(s_i \in \mathcal{T}(U_i))_{i\in I}$. Because $\mathcal{T}$ is a $\mathcal{G}$-torsor, then in the intersection $U_i \cap U_j$ we have a unique $g_{ij} \in \mathcal{G}(U_{ij})$

such that $s_i = g_{ij} \cdot s_j$. The family $g = (g_{ij})_{(i,j) \in I \times I}$ is a 1-cocycle, because in the triple intersection $U_i \cap U_j \cap U_k$ we have

$$g_{ij} \cdot g_{jk} \cdot s_k = g_{ij} \cdot s_j = s_i = g_{ik} \cdot s_k.$$

Moreover, if we replace s_i with $s'_i = h_i \cdot s_i$ with $h_i \in \mathcal{G}(U_i)$, we get the cohomologous cocycle $(g'_{ij}) = (h_i \cdot g_{ij} \cdot h_j^{-1})$. Thus for each $\mathcal{G}$-torsor $\mathcal{T}$, we associate a class of 1-cocycle $c(\mathcal{T})$ in $\check{\mathrm{H}}^1(\mathcal{U}, \mathcal{G})$. So we have the following proposition that relates the first cohomology set to the first Čech cohomology set, but we will not prove it.

2.8.4 Proposition. *Let S be a topological space and $\mathcal{G}$ a sheaf of groups on S. The map $\mathcal{T} \mapsto c(\mathcal{T})$ induces a bijection from $\mathrm{H}^1(S, \mathcal{G})$ to $\check{\mathrm{H}}^1(S, \mathcal{G})$.*

Proof. See [10], Proposition 5.1.1. □

For sheaves of abelian groups, in general we define cohomology of sheaves by taking the derived functors of the global section functor. See [11], Chapter III.

2.8.5 Definition. Let S be a topological space. For $i \in \mathbb{Z}_{\geq 0}$, we define a functor

$$Ab(S) \to Ab : \mathcal{F} \mapsto \mathrm{H}^i(S, \mathcal{F}),$$

as the i^{th}-right derived functor of the (left exact) global sections functor

$$Ab(S) \to Ab : \mathcal{F} \mapsto F(S).$$

If $\mathcal{F}$ is a sheaf of abelian groups on S, then the abelian group $\mathrm{H}^i(S, \mathcal{F})$ is called the i^{th} *cohomology group* of $\mathcal{F}$. For $i = 1$, this is compatible with our earlier Definition 2.5.5 (see [21, Tag 02FN]).

Moreover, for any exact sequence of sheaves of abelian groups on S

$$0 \to \mathcal{F} \to \mathcal{G} \to \mathcal{H} \to 0,$$

we get a long exact sequence of abelian groups

$$0 \to \mathrm{H}^0(S, \mathcal{F}) \to \mathrm{H}^0(S, \mathcal{G}) \to \mathrm{H}^0(S, \mathcal{H}) \to \mathrm{H}^1(S, \mathcal{F}) \to \dots.$$

We have the following theorem that relates the first Čech cohomology groups with the first cohomology groups defined by taking the derived functors of the global sections functor.

2.8.6 Theorem. *Let S be a topological space and $\mathcal{F}$ be a sheaf of abelian groups. Then we have a natural isomophism*

$$\check{\mathrm{H}}^1(S, \mathcal{F}) \to \mathrm{H}^1(S, \mathcal{F}).$$

Proof. See [11], Chapter III, Exercise 4.4. □

So our notation of $\mathrm{H}^1(S, \mathcal{F})$ as the first derived functor of the global section functor on S or as the set of isomorphism classes of $\mathcal{F}$-torsors on S is justified for a sheaf of abelian groups $\mathcal{F}$. We cite also a vanishing theorem of Grothendieck from [11], Chapter III, Theorem 2.7 that we will use later.

2.8.7 Theorem. *Let S be a noetherian topological space of dimension n. Then for all $i > n$ and all sheaves of abelian groups $\mathcal{F}$ on S, we have $\mathrm{H}^i(S, \mathcal{F}) = 0$.*

2.9 Bilinear forms and symmetries

We recall the definition of bilinear forms on free modules and study some properties of symmetries, that will be used to prove the transitivity of the action of the special orthogonal group on spheres. The material of this section can be found in [15].

2.9.1 Definition. Let R be a domain, K its fraction field, n a positive integer, and M a locally free R-module of rank n. A *bilinear form* b *on* M is a function $b : M \times M \to R$ such that for every x, y, z in M and for every r in R, we have

$$\begin{aligned} b(x+y,z) &= b(x,z)+b(y,z), \\ b(x,y+z) &= b(x,y)+b(x,z), \\ b(rx,y) &= rb(x,y) = b(x,ry). \end{aligned}$$

A pair of (M, b) is called a *module with bilinear form*, for simplifying the notation we will write it as M if the bilinear form b is clear in the context. An *orientation* of M is an isomorphism $d\colon R \to \wedge^n M$ of R-modules, where the last symbol is the top exterior power of M over R. One writes an oriented module with a bilinear form as a triple (M, b, d). An *isomorphism between two oriented modules with bilinear forms* (M, b, d) and (M', b', d') is a bijective linear map $f : M \to M'$ such that for all $x, y \in M$, we have $b'(f(x), f(y)) = b(x, y)$, and $\wedge^n(f) \circ d = d'$.

A bilinear form b is called *symmetric* if for every x, y in M we have $b(x, y) = b(y, x)$. A symmetric bilinear form b will be called *perfect* (also called *regular*) if the following strong non-degeneracy condition is satisfied: for each R-linear map $\phi\colon M \to R$, there exists a unique element x in M such that the homomorphism $y \mapsto b(x, y)$ from M to R is equal to ϕ. In other words, the map $M \to \mathrm{Hom}_R(M, R)$ sending x to $y \mapsto b(x, y)$ is a bijection. We use the notation $M^\vee$ for the dual $\mathrm{Hom}_R(M, R)$ of M.

Two elements x and y in M with a symmetric bilinear form b are called *orthogonal* if $b(x, y) = 0$. Note that for a module M with perfect symmetric bilinear b, an element x in M is orthogonal to every element y in M if and only if $x = 0$. Let $(e_1, \dots, e_n)$ be a basis of M, we define the *Gram matrix* $B = (b(e_i, e_j))_{i,j}$ with respect to this basis. The bilinear form b is perfect if and only if the matrix B is invertible (it has a 2-sided inverse).

2.9.2 Definition. Let R be a domain, K its fraction field, n a positive integer, and (M, b) a free R-module of rank n with symmetric bilinear form. Assume that 2 is not zero in R. Let $v \in M$ such that $b(v, v)$ divides 2, equivalently $2/b(v, v)$ is in R. We define the *symmetry about the hyperplane perpendicular to* v by the formula:

$$s_v \colon M \to M, x \mapsto s_v(x) := x - 2\frac{b(x, v)}{b(v, v)}v.$$

We have several elementary properties of symmetries:

- For $x \in M$ such that $b(x, v) = 0$, we have $s_v(x) = x$.
- We have $s_v^2 = \mathrm{id}$.
- For any $k \in R$, $s_v(kv) = -kv$.
- For $v, w \in M$ such that $b(w, w) = b(v, v)$ and $b(w - v, w)$ invertible in R, we get $s_{w-v}(w) = v$. Indeed, $b(w - v, w - v)/2 = b(w - v, w)$, so the symmetry is well defined and $s_{w-v}(w) = w - 2\frac{b(w,w-v)}{b(w-v,w-v)}(w - v) = v$.
- Suppose $v \in M$ such that $b(v, v)$ divides 2. For all $x, y \in M$ we have $b(s_v(x), s_v(y)) = b(x, y)$. We compute it directly, let $k_1 := 2\frac{b(x,v)}{b(v,v)}$ and $k_2 := 2\frac{b(y,v)}{b(v,v)}$,

$$\begin{aligned} &b(s_v(x), s_v(y)) = b(x - k_1 v, y - k_2 v)\\ &= b(x, y) + k_1 k_2 b(v, v) - k_2 b(x, v) - k_1 b(y, v)\\ &= b(x, y) + (2/b(v, v))(2b(x, v)b(y, v) - b(y, v)b(x, v) - b(x, v)b(y, v))\\ &= b(x, y). \end{aligned}$$

Now assume that the ring R is either $\mathbb{Z}, \mathbb{Q}$ or $\mathbb{R}$. Then a bilinear form b is called *positive definite* if for any x in M we have $b(x,x) \geq 0$ and $b(x,x) = 0$ if and only if $x = 0$.

Now let n be a positive integer and $\mathbb{R}^n$ be the $\mathbb{R}$-vector space consisting of all n-tuples $x = (x_1, \ldots, x_n)$ of real numbers. We can equip $\mathbb{R}^n$ with the *standard* symmetric bilinear form, i.e., the inner product: $x \cdot y = \sum_{i=1}^{n} x_i y_i$ for $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_n)$ in $\mathbb{R}^n$. The pair $\mathbb{R}^n$ with the inner product is called *the standard euclidean inner product space.* Note that any n-dimensional vector space V over $\mathbb{R}$ with a positive definite symmetric bilinear form b is isomorphic to the standard euclidean inner product space $\mathbb{R}^n$. This is because we can map an orthonormal basis of V, that is obtained from the Gram-Schmidt process, to the standard basis of $\mathbb{R}^n$.

Let n be a positive integer and L be a free $\mathbb{Z}$-module of rank n with positive definite symmetric bilinear form b. We can embed L canonically in $V := L \otimes_{\mathbb{Z}} \mathbb{R}$ which is a n-dimensional $\mathbb{R}$ vector space with the bilinear form $b_{\mathbb{R}}$. It is a positive definite symmetric bilinear form on V. The above discussion shows that L can be embedded into $\mathbb{R}^n$ so that b is the restriction of the standard inner product.

2.9.3 Definition. A *lattice* L is a free $\mathbb{Z}$-module of finite rank together with a positive definite symmetric bilinear form b on $L \otimes_{\mathbb{Z}} \mathbb{R}$. It is *integral* if $b(L \times L)$ is contained in $\mathbb{Z}$.

Let V be a n-dimensional vector space over $\mathbb{R}$ and b an inner product on V. A unit n-dimensional cube in V is a parallelepiped spanned by an orthonormal basis of V. We let the volume of it be 1. It induces a measure on V that does not depend the choice of the orthonormal basis. Let L be a lattice in V. Suppose that $(v_1, \ldots, v_n)$ is a $\mathbb{Z}$-basis of L. Let $(e_1, \ldots, e_n)$ be an orthonormal basis of V. Suppose for every i, we have $v_i = \Sigma a_{ij} e_j$. Let us set $a = (a_{ij})$. The volume of the quotient torus V/L is defined as the volume of the parallelepiped generated by the basis $(v_1, \ldots, v_n)$ (this does not depend on the choice of $\mathbb{Z}$-basis of L). It is equal to

$$\mathrm{Vol}(V/L) = |\det(a)| .$$

The volume is also equal to the square root of the determinant of the Gram matrix $B = (b(v_i, v_j))_{i,j} = a \cdot a^t$. The *discriminant* of the lattice L is defined as the determinant of the gram matrix B.

2.9.4 Minkowski's theorem

Recall that a subset $X \subset \mathbb{R}^n$ is *convex* if x, y in X implies that $\lambda x + (1-\lambda)y$ in X for all real numbers λ in the interval $0 \leq \lambda \leq 1$. A subset X of $\mathbb{R}^n$ is *symmetric about* 0, if x in X implies $-x$ in X. Now we can state the theorem of Minkowski.

2.9.4.1 Theorem. (Minkowski) *Let X be a bounded, convex and symmetric about 0 subset of $\mathbb{R}^n$. If the volume of X is greater than 2^n times the volume of $\mathbb{R}^n/L$, then X contains a non-zero point of L.*

Proof. See [15] Chapter II, Section 1.3. □

As a consequence of this we will show in 3.3 that $\mathrm{H}^1(\mathrm{Spec}(\mathbb{Z}), \mathrm{SO}_3) = \{1\}$, where SO_3 is the sheaf induced by the special orthogonal group with respect to the standard inner product.

2.10 Descent

Sometimes it happens that a certain construction can be carried out only after étale base change, or in general faithfully flat base change. Then one can try to use descent theory in order to go back to the original situation one started with. Although this is a general result, we will see in Chapter 3 an explicit example. A reference for this section is [3]. Some references for the definitions of étale, flat and faithfully flat maps are [13] and [21].

Let $R \to R'$ be a faithfully flat ring homomorphism. We have homomorphisms of R-algebras $p_1 \colon R' \to R' \otimes_R R', p_2 \colon R' \to R' \otimes_R R'$ defined by $p_1(r) = r \otimes 1$ and $p_2(r) = 1 \otimes r$. We have the following lemmas that we will use later.

2.10.1 Lemma. *Let $f \colon R \to R'$ be a faithfully flat morphism of rings. Then, for any R-module M, the canonical diagram*

$$\begin{tikzcd} M \arrow[r] & M \otimes_R R' \arrow[r, shift left, "\mathrm{id}\otimes p_1"] \arrow[r, shift right, "\mathrm{id}\otimes p_2"'] & M \otimes_R R' \otimes_R R' \end{tikzcd}$$

is an equalizer.

Proof. We may apply a faithfully flat base change over R, say with R', since exactness does not change by doing that. Thereby we can assume that $f \colon R \to R'$ admits a section $e \colon R' \to R$, that is $e \circ f = 1$. So all the maps in the above diagram have sections. Suppose $\Sigma_i m_i \otimes r'_i \in M \otimes_R R'$ is in the equalizer. We have $\Sigma_i m_i \otimes 1 \otimes r'_i = \Sigma_i m_i \otimes r'_i \otimes 1$ in $M \otimes_R R' \otimes_R R'$. Then applying the section $M \otimes R' \otimes R' \to M \otimes R', m \otimes r'_1 \otimes r'_2 \mapsto m \otimes r'_1 e(r'_2)$ gives $\Sigma_i m_i \otimes r'_i = \Sigma_i m_i \otimes e(r'_i) = \Sigma_i e(r'_i) m_i \otimes 1$. The last equality holds since $e(r'_i)$ is an element of R. Thus $\Sigma_i m_i \otimes r'_i$ is in M. □

2.10.2 Lemma. *Let R be a ring and $R \to R'$ be a faithfully flat morphism. Suppose A and B are R-algebras (or R'-modules) and $\phi \colon A \otimes_R R' \to B \otimes_R R'$*

is an R'-algebra (or R'-module) morphism. We get the following diagram:

$$\begin{tikzcd}
A \arrow[d] & & B \arrow[d] & , \\
A \otimes_R R' \arrow[rr, "\phi"] \arrow[d, shift right, "\mathrm{id}\otimes p_1"'] \arrow[d, shift left, "\mathrm{id}\otimes p_2"] & & B \otimes_R R' \arrow[d, shift right, "\mathrm{id}\otimes p_1"'] \arrow[d, shift left, "\mathrm{id}\otimes p_2"] & \\
A \otimes_R R' \otimes_R R' \arrow[rr, shift left, "\phi_1"] \arrow[rr, shift right, "\phi_2"'] & & B \otimes_R R' \otimes_R R' &
\end{tikzcd}$$

where for each $i = 1, 2, \phi_i \circ (\mathrm{id} \otimes p_i) = (\mathrm{id} \otimes p_i) \circ \phi$. Then ϕ is defined over R, that is there exists $\psi : A \to B$ such that $\phi = \psi \otimes \mathrm{id}$, if and only if $\phi_1 = \phi_2$. Moreover in that case, if ϕ is an isomorphism, then ψ is also an isomorphism.

Proof. It is clear that the condition is necessary since $(\psi\otimes\mathrm{id})\otimes\mathrm{id} = \psi\otimes\mathrm{id}\otimes\mathrm{id}$. Suppose $\phi_1 = \phi_2$. Let $a \in A$, by Lemma 2.10.1, we have

$$(\mathrm{id} \otimes p_1)(\phi(a)) = \phi_1((\mathrm{id} \otimes p_1)(a)) = \phi_2((\mathrm{id} \otimes p_2)(a)) = (\mathrm{id} \otimes p_2)(\phi(a)).$$

So $\phi(a)$ is in B, and we define $\psi := \phi|_A \colon A \to B$ the restriction of ϕ in A. For $a \otimes r' \in A \otimes_R R'$, we have

$$\phi(a \otimes r') = \phi((a \otimes 1).(1 \otimes r')) = (1 \otimes r')\phi(a \otimes 1) = (1 \otimes r')\psi(a) = \psi(a) \otimes r',$$

and we get $\phi = \psi \otimes \mathrm{id}$. Now if ϕ is an isomorphism, in particular it is injective, so ψ is also an injective map.

Suppose $a \in A \otimes_R R'$ such that $\phi(a) \in B$. Then we have, again by Lemma 2.10.1, we have $(\mathrm{id} \otimes p_1)(\phi(a)) = (\mathrm{id} \otimes p_2)(\phi(a))$, or equivalently $\phi_1((\mathrm{id} \otimes p_1)(a) - (\mathrm{id} \otimes p_2)(a)) = 0$. Because ϕ_1 is an isomorphism, then $(\mathrm{id} \otimes p_1)(a) = (\mathrm{id} \otimes p_2)(a)$, or $a \in A$. Thus together with the surjectivity of ϕ, we conclude that ψ is also surjective. □

2.11 Schemes

The reader is advised to skip this section and only read it if necessary. A reference for the results of this section is Chapters 2–4 of [13].

We define schemes here. For that we need a suitable category of spaces with sheaves of rings on them. The appropriate notion is the category of locally ringed spaces.

2.11.1 Definition. A *locally ringed space* is a pair $(S, \mathcal{O}_S)$ consisting of a topological space S and a sheaf of rings $\mathcal{O}_S$ on S such that for every $s \in S$, the stalk $\mathcal{O}_{S,s}$ of $\mathcal{O}_S$ at s (see Definition 2.2.7) is a local ring. Let $\mathfrak{m}_s$ be the maximal ideal of $\mathcal{O}_{S,s}$; we call $\mathcal{O}_{S,s}/\mathfrak{m}_s$ the *residue field of S at s*, and we denote it $k(s)$. A *morphism* of locally ringed spaces from $(S, \mathcal{O}_S)$ to $(T, \mathcal{O}_T)$ is a pair $(f, f^\#)$ of a continuous map $f\colon S \to T$ and a map $f^\#\colon \mathcal{O}_T \to f_*\mathcal{O}_S$ of sheaves of rings on T such that for every $s \in S$, the stalk map $f_s^\#\colon \mathcal{O}_{T,f(s)} \to \mathcal{O}_{S,s}$ is a local homomorphism, that is $f_s^\#(\mathfrak{m}_{f(s)}) \subset \mathfrak{m}_s$. The stalk map is obtained as follows: As V ranges over all open neighborhoods of $f(s), f^{-1}(V)$ ranges over a subset of the neighborhoods of s. We take filtering colimits and we obtain a map

$$\mathcal{O}_{T,f(s)} = \mathrm{colim}_V\, \mathcal{O}_T(V) \longrightarrow \mathrm{colim}_V\, \mathcal{O}_S(f^{-1}(V)),$$

and the latter limit maps to the stalk $\mathcal{O}_{S,s}$.

Locally ringed spaces and morphisms of them form a category. Thus a morphism $(f, f^\#)$ is an isomorphism if and only if the map f is a homeomorphism of the underlying topological spaces, and $f^\#$ is an isomorphism of sheaves. A morphism $(f, f^\#)$ from $(S, \mathcal{O}_S)$ to $(T, \mathcal{O}_T)$ is an *open immersion* (resp. *closed immersion*) if f is a topological open immersion (resp. closed immersion) and if for every $s \in S$, $f_s^\#$ is an isomorphism (resp. if $f_s^\#$ is surjective).

2.11.2 Definition. We define an *affine scheme* to be a locally ringed space isomorphic to some $(\mathrm{Spec}(A), \mathcal{O}_{\mathrm{Spec}(A)})$ constructed above. A *scheme* is a ringed topological space $(S, \mathcal{O}_S)$ admitting an open covering $\{U_i\}_i$ such that $(U_i, \mathcal{O}_S|_{U_i})$ is an affine scheme for every i. By abuse of notation, we will denote it simply by $\mathrm{Spec}(A)$ or S.

2.11.3 Example. Let k be a field. Let $S = \mathbb{A}^1_k = \mathrm{Spec}(k[x])$ be *the affine line.* Every open subset U of S is of the form $D(p)$, where $p \in k[x]$. We have $\mathcal{O}_S(U) = k[x, 1/p]$.

2.11.4 Lemma. *Let A be a ring and $S = \mathrm{Spec}(A)$ be an affine scheme. Let f be an element of A. Then the principal open subset $D(f)$, endowed with the structure of a ringed topological space induced by that of S, is an affine scheme isomorphic as a ringed topological space to* $\mathrm{Spec}(A_f)$*.*

Proof. See [13] Chapter 2, Lemma 3.7. □

Now let S be a scheme and U any open subset of S. We have $S = \bigcup_i U_i$, where U_i is open and affine. We know that $U_i \cap U \subset U_i$ is a union of principal open subsets of U_i, each of these principal open subsets being an affine scheme. So $U_i \cap U$ is a scheme, and the ringed topological space $(U, \mathcal{O}_S|U)$ is also a scheme. We call $(U, \mathcal{O}_S|U)$ an *open subscheme* of S.

Recall that a ring A is said to be *Noetherian* if every ideal in A is finitely generated. Note that if A is Noetherian, then the polynomial ring $A[x]$ is Noetherian. The quotient ring A/I with any ideal I of A is also Noetherian. In particular for a field k, a finitely-generated algebra $k[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$ is a Noetherian ring. We refer to [1] for a proof. We have a typical example of a non-Noetherian ring such as the polynomial ring $k[x_1, \ldots]$ over a field k with infinitely many variables. Note that this ring is a domain but non-Noetherian.

2.11.5 Definition. A scheme S is said to be *Noetherian* if it is a finite union of affine opens U_i such that $(\mathcal{O}_S|_{U_i})(U_i)$ is a Noetherian ring for every i. We say that a scheme is *locally Noetherian* if every point has an open neighborhood that is a Noetherian scheme.

Let S be a scheme. We have that S is a locally Noetherian scheme if and only if any affine open subscheme of S is a Noetherian scheme. For any point $s \in S$, the local ring $\mathcal{O}_{S,s}$ is also Noetherian. Most schemes that we will consider in this thesis are Noetherian or locally Noetherian.

2.11.6 Definition. Let S and T be schemes. A *morphism of schemes* $f\colon S \to T$ is a morphism of locally ringed spaces. An *open or closed immersion of schemes* is an open or closed immersion of locally ringed spaces.

A *closed subscheme* of S is a closed subset Z of S endowed with the structure $(Z, \mathcal{O}_Z)$ of a scheme and with a closed immersion $(j, j^\#)\colon (Z, \mathcal{O}_Z) \to (S, \mathcal{O}_S)$, where $j\colon Z \to S$ is the canonical injection. A *subscheme* of a scheme S is a closed subscheme of an open subscheme of S.

2.11.7 Remark. Any open subset of a scheme S is (uniquely, via restriction) an open subscheme. A closed subset of a scheme S can have many closed subscheme structures. Indeed when $S = \mathrm{Spec}(A)$ is affine, there is a bijection between the set of closed subschemes of S with the set of ideals of A. In particular 2 ideals I, J of A will give the same closed subset of S, as a topological space, if the radical $\sqrt{I}$ of I is equal to the radical $\sqrt{J}$ of J.

Let $\phi\colon A \to B$ be a ring homomorphism, $S := \mathrm{Spec}(B)$, and $T := \mathrm{Spec}(A)$. Then we have a map of sets $f_\phi := \mathrm{Spec}(\phi)\colon S \to T$ defined by $s \mapsto \phi^{-1}(s)$ for every $s \in S$. The map f_ϕ is continuous. Indeed, if $D(g) \subset T$ for some $g \in A$, then $f_\phi^{-1}(D(g)) = D(\phi(g))$. This implies the preimage of any open subset in T is also open in S. The map ϕ induces a ring homomorphism $\mathcal{O}_T(D(g)) = A_g \to B_{\phi(g)} = (f_\phi)_*\mathcal{O}_S(D(g))$. This homomorphism is compatible with the restrictions; we therefore have a morphism of sheaves $f_\phi^\# : \mathcal{O}_T \to (f_\phi)_*\mathcal{O}_S$ since the $D(g)$ form a base. Moreover, for every $s \in S$, the canonical homomorphism $A_{\phi^{-1}(s)} \to B_s$ induced by ϕ is a local homomorphism and coincides with $(f_\phi^\#)_s$. Therefore $(f_\phi, f_\phi^\#)$ is a morphism of locally ringed spaces. In particular by construction, we have $f_\phi^\#(T) = \phi$.

Now let consider $\mathrm{Mor}(S, T)$ the set of morphisms of affine schemes from S to T. We denote also $\mathrm{Hom}_{rings}(A, B)$ the set of ring homomorphisms from A to B. We have a canonical map $\rho : \mathrm{Mor}(S, T) \to \mathrm{Hom}_{rings}(\mathcal{O}_T(T), \mathcal{O}_S(S))$, which to $(f, f^\#)$ associates $f^\#(T)\colon \mathcal{O}_T(T) \to f_*(\mathcal{O}_S)(T) = \mathcal{O}_S(S)$.

2.11.8 Proposition. *Let A, B be rings and $S = \mathrm{Spec}(B), T = \mathrm{Spec}(A)$ be affine schemes. Then the canonical map*

$$\rho : \mathrm{Mor}(S, T) \to \mathrm{Hom}_{rings}(\mathcal{O}_T(T), \mathcal{O}_S(S))$$

is a bijection.

Proof. Let $f \in \mathrm{Mor}(S, T)$ and $\phi = \rho(f) = f^\#(T)$. The discussion above gives a morphism of schemes $f_\phi\colon S \to T$. It suffices to show that $f = f_\phi$. For any $s \in S$, we have the map $\phi\colon A \to B$ induces the local homomorphism $f_s^\# : A_{f(s)} \to B_s$, thus we have $\phi(A - f(s)) \subset B - s$. Hence $\phi^{-1}(s) \subset f(s)$. Moreover because $f_s^\#$ is a local homomorphism, that implies $\phi^{-1}(s) = f(s)$. Therefore f and f_ϕ coincide set-theoretically, and $f_s^\# = f_{\phi,s}^\#$ for every $s \in S$. Two maps of sheaves that have the same values on the stalks are the same map, or $f^\# = f_\phi^\#$. □

2.11.9 Example. Let A be a ring, I be an ideal of A, and $g \in A$. Then the morphism of schemes $i\colon \mathrm{Spec}(A/I) \to \mathrm{Spec}(A)$, induced by the canonical surjection $A \to A/I$ is a closed immersion of schemes whose image is $Z(I)$. On the other hand, the localization homomorphism $\phi : A \to A_g$ gives an open immersion $f_\phi\colon \mathrm{Spec}(A_g) \to \mathrm{Spec}(A)$, where we identify $\mathrm{Spec}(A_g)$ with the open subset $D(g)$ of $\mathrm{Spec}(A)$, endowed with the structure of locally ringed space induced by that of $\mathrm{Spec}(A)$ as in Lemma 2.11.4.

2.11.10 Definition. Let S be a scheme and $T \to S$ be an S-scheme. For any scheme X, let us denote $S(X) := \mathrm{Mor}(X, S)$ the set of morphisms of schemes from $T \to S$. Also for any S-scheme Y, we denote let $T_S(Y) := \mathrm{Mor}_S(Y, T)$ be the set of morphisms of S-schemes from Y to T. Sometimes we omit the subscript S in $T_S(Y)$ for the notation of $\mathrm{Mor}_S(Y, T)$.

2.11.11 Definition. Let S be a scheme, and let X, Y be two S-schemes. The *fibered product of* X, Y *over* S is an S-scheme $X \times_S Y$, together with two morphisms of S-schemes

$$p\colon X \times_S Y \to X \quad q\colon X \times_S Y \to Y,$$

verifying the following universal property: if $f\colon Z \to X$, $g\colon Z \to Y$ are two morphisms of S-schemes, then there exists a unique morphism of S-schemes $(f, g)\colon Z \to X \times_S Y$ such that $p \circ (f, g) = f$ and $q \circ (f, g) = g$.

The fibered product of two S-schemes X, Y exists (see [13] Chapter 3 for a proof).

2.11.12 Definition. Let $f\colon S \to T$ be a morphism of schemes, and let $t \in T$ be a point. Let $\kappa(t)$ be the residue field of t, and let $\mathrm{Spec}(\kappa(t)) \to T$ be the natural morphism. Then we define the *fibre* of the morphism f over the point t to be the scheme

$$S_t = S \times_T \mathrm{Spec}(\kappa(t)).$$

It is a scheme over $\operatorname{Spec}(\kappa(t))$, and its underlying topological space is homeomorphic to the subspace $f^{-1}(t)$ of S. When we consider a scheme S over $\operatorname{Spec}(\mathbb{Z})$, taking the fibre over the generic point gives a scheme $S_{\mathbb{Q}}$ over $\mathbb{Q}$, while taking the fibre over a closed point (p), corresponding to a prime number p, gives a scheme $S_{\mathbb{F}_p}$ over the finite field $\mathbb{F}_p$. We say that S_p arises by *reduction* mod p of the scheme S.

If B is an algebra over the ring A, we say that B is *finitely presented* if it is the quotient of a polynomial ring $A[x_1, \cdots, x_n]$ over A by a finitely generated ideal. If A is Noetherian, every finitely generated algebra is finitely presented.

2.11.13 Definition. A morphism of schemes $f\colon S \to T$ is *locally of finite presentation* (*locally of finite type*) if for any $s \in S$ there are affine neighborhoods U of s in S and V of $f(s)$ in T such that $f(U) \subset V$ and $\mathcal{O}_S(U)$ is finitely presented (finitely generated) over $\mathcal{O}_T(V)$.

Note that if T is locally Noetherian, then f is locally of finite presentation if and only if it is locally of finite type.

2.11.14 Definition. A morphism of schemes $S \to T$ is *quasi-compact* if the inverse image in S of each quasi-compact open subset of T is quasi-compact.

An affine scheme is quasi-compact, hence a scheme is quasi-compact if and only if it is the finite union of open affine subschemes. Thus we have $f\colon S \to T$ is quasi-compact if and only if there exists a covering $T = \bigcup_i T_i$ by open affine subschemes, such that the inverse image in S of each T_i is a finite union of open affine subschemes.

2.11.15 Definition. A morphism of schemes $f\colon S \to T$ is *of finite type* if it is locally of finite type and quasi-compact. It is called *quasi-finite* if it is of finite type and has finite fibers, that is, $f^{-1}(t)$ is discrete (and hence finite) for all $t \in T$.

Let us turn to flat morphisms.

2.11.16 Definition. A morphism of schemes $f\colon S \to T$ is *flat* if for any $s \in S$, the local ring $\mathcal{O}_{S,s}$ is flat as a module over $\mathcal{O}_{T,f(s)}$. And it is called *faithfully flat* if it is flat and surjective (as a map of sets). It is called *fppf* if it is flat and locally of finite presentation.

2.11.17 Theorem. (Chevalley) *Let S, T be locally Noetherian schemes. A morphism $f\colon S \to T$ that is flat and locally of finite type is open.*

Proof. See [14], Theorem 2.12. □

Let A and B be Noetherian rings. A homomorphism $f\colon A \to B$ of finite type is *unramified* at $s \in \operatorname{Spec}(B)$ if and only if $t := f^{-1}(s) \in \operatorname{Spec}(A)$ generates the maximal ideal in B_s and $\kappa(s)$ is a finite separable field extension of $\kappa(t)$. This terminology agrees with that in number theory.

2.11.18 Definition. A morphism of locally Noetherian schemes $f\colon S \to T$ that is of finite type is said to be *unramified at $s \in S$* if $\mathcal{O}_{S,s}/\mathfrak{m}_t\mathcal{O}_{S,s}$ is a finite separable field extension of $\kappa(t)$, where $t := f(s)$. A morphism $f\colon S \to T$ is *unramified* if it is unramified at all $s \in S$.

We have a nice fiberwise criterion for a finite type morphism $f\colon S \to T$ between locally Noetherian schemes to be unramified. That is f is unramified if and only if for all $t \in T$, the fiber $S_t \to \operatorname{Spec}(\kappa(t))$ over t is unramified. Being unramified over a field, here over $\kappa(t)$, means that S_t is a sum (finite sum when f is of finite type) $\coprod_i \operatorname{Spec}(\kappa_i)$, where the κ_i are finite separable extensions of $\kappa(t)$.

2.11.19 Definition. A morphism of locally Noetherian schemes (or Noetherian rings) $f\colon S \to T$ is said to be *étale* if it is flat and unramified.

Let $f\colon U \to S$, $g\colon T \to U$ be étale morphisms. If $f \circ g\colon T \to S$ and f are étale, then so also is g. Now suppose that $R' = R[x_1, \ldots, x_n]/(P_1, \ldots, P_n)$ is a finite type R-algebra where R is Noetherian. Here P_i are polynomials in $R[x_1, \ldots, x_n]$. Then $R \to R'$ is called an *étale morphism* if the determinant of the Jacobian matrix $(\partial P_i/\partial x_j)$ is a unit in R'. We refer to [14], Chapter I for a more thorough exposition of the notion of étale morphism.

2.12 Grothendieck (pre)topologies and sites

The reader is advised to skip this section and only read it if necessary. Some references for this section are [21, Tag 00UZ] and [16]. Following Poonen, we quote Vistoli:

> Before the notion of a topology on a set was invented, people studied metric spaces, and their open and closed subsets. Then somebody noticed that many properties of metric spaces could be defined without reference to the metric: for many purposes, just knowing which subsets were open was enough. This led to the definition of a topology on a set, in which an arbitrary collection of subsets could be decreed to be the open sets, provided the collection satisfied some axioms (modelled after the theorems about open sets in metric spaces).
>
> Grothendieck took this one step further by observing that sometimes one does not even need to know the open subsets: for many purposes (for instance, for the concept of sheaf), it suffices to have a notion of open covering in an arbitrary category. This led

to the notion of a Grothendieck topology (which is usually not a topology in the usual sense). Just as an open set in a topological space need not be open relative to any metric, an open covering in a Grothendieck topology need not consist of actual open subsets! This relaxation of the notion of open covering is necessary to obtain a sufficiently fine topology on a scheme.

2.12.1 Definition. Let $\mathcal{A}$ be a category together with, for each object U of $\mathcal{A}$, a distinguished set of families of maps $(U_i \to U)_i$, called the *open coverings* of U. A *Grothendieck (pre)topology* on $\mathcal{A}$ is a set τ of open coverings that satisfies the following axioms:

- For any U in $\mathcal{A}$, the family $(U \xrightarrow{\text{id}} U)$ consisting of a single map is an open covering of U, or it belongs to τ.

- An open covering of an open covering is an open covering: If $(U_i \to U)_i$ belongs to τ, and $(V_{ij} \to U_i)_j$ belongs to τ for each i, then $(V_{ij} \to U)_{ij}$ belongs to τ.

- A base extension of an open covering is an open covering: If $(U_i \to U)_i$ belongs to τ, and $V \to U$ is a morphism in $\mathcal{A}$, then the fiber products $V \times_U U_i \to V$ exist for all i and $(V \times_U U_i \to V)_i$ belongs to τ.

Note that the SGA 4 definition of *Grothendieck topology* is in terms of sieves that we will not discuss here. A Grothendieck pretopology gives rise to a Grothendieck topology, and all the Grothendieck topologies we will use here arise this way. So from now on, we will abuse terminology and call a pretopology a topology.

2.12.2 Definition. Let $\mathcal{A}$ be a category and τ a Grothendieck topology on $\mathcal{A}$. A pair $(\mathcal{A}, \tau)$ is called a *site*.

We now list some sites. In the remainder of this section, S will be a scheme. To give a site first we need to have a category, and then the system of coverings with above axioms in that category. A family of S-morphisms $(\phi_i \colon U_i \to U)_i$ of S-schemes will be said to be *surjective* if $U = \bigcup_i \phi_i(U_i)$.

First let us define the list $\mathcal{P}$ of properties of morphisms:

- surjective (as a map of sets), open immersion, locally of finite presentation, locally of finite type, of finite presentation, of finite type, quasi-finite, quasi-compact, flat, fppf, unramified, étale.

Then the following proposition will be used to show that some families of morphisms satisfy the axioms of the coverings.

2.12.3 Proposition. *Let P be in the list $\mathcal{P}$.*

- *If $S \to T$ is a morphism that is P, $T \to W$ is also a morphism with property P, then the composition $S \to W$ is also P.*

- *Let $f \colon S \to T$ be a morphism of schemes, and let $f' \colon S' \to T'$ be its base extension by a morphism $S' \to S$. If f is P, then f' is also P.*

Proof. See [16], Appendix C. □

The small Zariski site Let S be a scheme. We consider it as a topological space, and we take the category $\mathcal{A} = \text{Open}(S)$ as in the Definition 2.1.1. Let the Grothendieck topology τ be the collection of surjective families $(U_i \to U)$ of open immersions. So here U is an open subset of S. We write S_{Zar} the (small) Zariski site.

The big Zariski site Let S be a scheme. We consider the category $\mathcal{A} = Sch/S$ of all S-schemes. Let the Grothendieck topology τ be the collection of surjective families $(U_i \to U)$ of S-morphisms, such that $U_i \to U$

is an open immersion for any i. Here U is any S-scheme, not necessarily an open subset of S.

The small étale site Let S be a scheme. We take $\mathcal{A}$ to be the category $\mathbf{Et}_S$ of schemes U equipped with an étale morphism $U \to S$, and in which morphisms are S-morphisms. These morphisms will automatically be étale (see 2.11). The Grothendieck topology τ is the collection of surjective families $(U_i \to U)$ of (étale) morphisms in $\mathcal{A}$. We write S_{et} the (small) étale site.

The (big) fppf site Let S be a scheme. We take $\mathcal{A}$ be the category Sch/S of all S-schemes. An open covering is a surjective family $(U_i \to U)$ of S-morphisms such that $\coprod_i U_i \to U$ is fppf. This gives the Grothendieck topology τ on $\mathcal{A}$, and we denote S_{fppf} the (big) fppf site.

2.13 Group schemes

The reader is advised to skip this section and only read it if necessary. Some references for this section are [22], [16], and [3]. We follow [16] and [22] quite closely.

Let $\mathcal{A}$ be a category with finite products: i.e., for any natural number n and for any objects $G_1, \ldots, G_n$ of $\mathcal{A}$, there exists an object G (denoted by $G_1 \times \cdots \times G_n$) equipped with morphisms $p_i \colon G \to G_i$, such that any other object H equipped with a morphism to each G_i, that is $h_i \colon H \to G_i$, admits a unique morphism to G, that is $h \colon H \to G$, such that for each i, the composition $p_i \circ h$ is equal to h_i. For example, for S a scheme, in the category of schemes over S the fiber product over S gives finite products (see also Definition 2.11.11).

2.13.1 Remark. For $n = 0$, an empty product is the same thing as a final object of $\mathcal{A}$, denoted by 1.

2.13.2 Definition. A *group object* in the category $\mathcal{A}$ is an object G equipped with morphisms $m\colon G \times G \to G$ (multiplication), $i\colon G \to G$ (inverse), and $e\colon 1 \to G$ (identity) satisfying group axiom as follows:

- (associativity) $m(m \times \mathrm{id}) = (\mathrm{id} \times m)m$,

- (identity) $m(\mathrm{id} \times e) = m(e \times \mathrm{id}) = \mathrm{id}$, and

- (inverse) $m(\mathrm{id}, i) = m(i, \mathrm{id}) = e$.

2.13.3 Example.

- A group object in the category of sets is a group.

- A group object in the category of topological spaces with continuous maps is a topological group.

- A group object in the category of smooth manifolds with smooth maps is a Lie group.

2.13.4 Definition. Let S be a scheme. A *group scheme* G over S is a group object in the category of S-schemes.

Using Yoneda's lemma (see [21, Tag 001L]) one can obtain an equivalent definition of group scheme that is perhaps closer to geometric intuition as follows. Let G be an S-scheme. Equipping G with the structure of a group scheme over S is equivalent to equipping the set $G(T)$ with a group structure for each S-scheme T such that for any S-morphism $T' \to T$, the map of sets $G(T) \to G(T')$ is a group homomorphism.

2.13.5 Definition. Let S be a scheme. A *homomorphism of group schemes* $f\colon G \to H$ over S is an S-morphism respecting the multiplication morphisms m_G and m_H, that is making the diagram

$$\begin{tikzcd}
G \times_S G \arrow[r, "m_G"] \arrow[d, "f\times f"'] & G \arrow[d, "f"] \\
H \times_S H \arrow[r, "m_H"] & H
\end{tikzcd}$$

commute.

2.13.6 Definition. Let S be a scheme. A *subgroup scheme* of a group scheme $G \to S$ is subscheme $H \to S$ of $G \to S$ such that for every $T \to S$ we have $H(T)$ is a subgroup of $G(T)$.

Homomorphisms of group schemes, kernels of morphisms and group scheme actions can be described also by Yoneda's lemma. For $f\colon G \to H$ a homomorphism of group schemes, by Yoneda's lemma

$$\ker(f)(T) = \ker(G(T) \to H(T))$$

for each S-scheme T. To give a left action of an S-group scheme G on an S-scheme X is equivalent to give a collection of compatible group actions $G(T) \times X(T) \to X(T)$ for each S-scheme T. Different properties can be described in terms of the functor of points, for instance, a subgroup scheme H of G is normal if and only if $H(T)$ is a normal subgroup of $G(T)$ for every S-scheme T.

2.13.7 Example. An elliptic curve over a number field K is a group scheme of finite type over $\mathrm{Spec}(K)$.

2.13.8 Affine group schemes

Throughout this subsection let R be a ring. A group scheme over R is called *affine* if it is affine as a scheme. The anti-equivalence between affine R-schemes and R-algebras gives us a description of affine group schemes over R in terms of R-algebras.

Let us see some examples to make clear what we want to discuss. For any R-algebra A, we define a group $G(A) := \mathrm{SL}_2(A)$ (the set of 2×2 matrices with entries in A and determinant 1), with multiplication. If $\phi : A \to B$ is an R-algebras homomorphism, then

$$\text{for any } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(A), \text{ we have } \begin{pmatrix} \phi(a) & \phi(b) \\ \phi(c) & \phi(d) \end{pmatrix} \text{ in } \mathrm{SL}_2(B),$$

because $\phi(a)\phi(d) - \phi(b)\phi(c) = \phi(ad - bc) = \phi(1) = 1$. So we get a group homomorphism $G(A) \to G(B)$. If moreover we have a morphism of R-algebras $\psi : B \to C$, then the map induced by $\psi \circ \phi$ is the composite $G(A) \to G(B) \to G(C)$. Finally, the identity map on A induces the identity map on $G(A)$. These mean that G is a functor from the category of R-algebras to the category of groups.

For A an R-algebra, the set $\mathrm{SL}_2(A)$ is the set of quadruples (a, b, c, d) in A^4 satisfying the polynomial equation $ad - bc = 1$. Hence we have a bijection

$$\mathrm{Hom}_R(R[X_{11}, X_{12}, X_{21}, X_{22}]/(X_{11}X_{22} - X_{12}X_{21} - 1), A) \to \mathrm{SL}_2(A),$$

sending ϕ to $(\phi(X_{11}), \phi(X_{12}), \phi(X_{21}), \phi(X_{22}))$. These bijections are functorial in A, therefore they are an isomorphism of functors

$$\mathrm{Hom}_R(R[X_{11}, X_{12}, X_{21}, X_{22}]/(X_{11}X_{22} - X_{12}X_{21} - 1), -) \to \mathrm{SL}_2(-).$$

In other words, the functor SL_2 composed with the forgetful functor from the category of groups to the category of sets is represented by the R-algebra

$$R[X_{11}, X_{12}, X_{21}, X_{22}]/(X_{11}X_{22} - X_{12}X_{21} - 1).$$

Chapter 3

Cohomological interpretation

3.1 Gauss's theorem

For $d \in \mathbb{Z}$ not a square, $d \equiv 0, 1 \pmod 4$, we let O_d be the subring of $\mathbb{C}$ generated by $u_d := (\sqrt{d}+d)/2$. It consists of the numbers $a+bu_d$ with a and b in $\mathbb{Z}$. It is free as $\mathbb{Z}$-module with basis $(1, u_d)$. The minimal polynomial of u_d is $f_d = x^2 - dx + (d^2 - d)/4$; the discriminant of f_d is d. The ring O_d is called the quadratic order of discriminant d. For such a d, we have the group $\mathrm{Pic}(O_d)$ (see Definition 2.8.2).

Here is Gauss's theorem.

3.1.1 Theorem. (Gauss) *Let n be a positive integer. We define the set $\mathcal{X}_n(\mathbb{Z}) = \{x \in \mathbb{Z}^3 : x_1^2 + x_2^2 + x_3^2 = n$ and $\gcd(x_1, x_2, x_3) = 1\}$. Then:*

$$\#\mathcal{X}_n(\mathbb{Z}) = \begin{cases} 0 \quad \textit{if } n \equiv 0, 4, 7 (8), \\ 48 \cdot \dfrac{\#\,\mathrm{Pic}(O_{-n})}{\#(O_{-n}^\times)} \quad \textit{if } n \equiv 3(8), \\ 24 \cdot \dfrac{\#\,\mathrm{Pic}(O_{-4n})}{\#(O_{-4n}^\times)} \quad \textit{if } n \equiv 1, 2(4). \end{cases}$$

The first case in this theorem is easy to prove. The squares in $\mathbb{Z}/8\mathbb{Z}$ are 0, 1 and 4. If (x_1, x_2, x_3) is in $\mathbb{Z}^3$ and $\gcd(x_1, x_2, x_3) = 1$, then at least one among the x_i is odd, hence $x_1^2 + x_2^2 + x_3^2$ cannot be 0, 4 or 7 in $\mathbb{Z}/8\mathbb{Z}$.

In the next sections, we will apply Theorem 2.6.1 to prove the last two cases of Gauss's result, assuming that there is at least one solution. We will also show the existence of an integer solution in Section 3.4 by using sheaf theory.

3.1.2 Remark. We sketch Gauss's method in a few lines. Let $P = (x, y, z)$ in $\mathbb{Z}^3$ be primitive, with $x^2 + y^2 + z^2 = n$. Then we have the following commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & P^\perp \arrow[r] & \mathbb{Z}^3 \arrow[r, "b_P"] & \mathbb{Z} \arrow[r] & 0 \\
0 \arrow[r] & P^\perp \arrow[r] \arrow[u, "="] & \mathbb{Z} \cdot P \oplus P^\perp \arrow[r] \arrow[u, hook] & n \cdot \mathbb{Z} \arrow[r] \arrow[u, hook] & 0,
\end{tikzcd}$$

where $b_P \colon Q \mapsto \langle Q, P \rangle$. This map has a section $1 \mapsto Q$, where $Q \in \mathbb{Z}^3$ is any point that satisfies $\langle Q, P \rangle = 1$. Then $v := nQ - P$ is in $P^\perp$. Also, $(P^\perp, b, d)$ is a primitive positive definite oriented symmetric bilinear module over $\mathbb{Z}$ of rank 2 and discriminant n (see 2.9 and 3.5.5 for the explanation of the notations and the proof). The lattice $\mathbb{Z} \cdot P \oplus P^\perp$ has the overlattice $\mathbb{Z}^3$ generated by $\mathbb{Z} \cdot P \oplus P^\perp$ and $Q = (1/n)(P + v)$ on which b is integral. We have

$$b((1/n)(P+v), (1/n)(P+v)) = n^{-2} b((P+v), (P+v)) = n^{-2}(n + b(v, v)).$$

So in $P^\perp$, there exists v such that $b(v, v) = -n$ modulo n^2. Conversely, for such a v we get the overlattice generated by $(1/n)(P + v)$ on which b is integral and perfect. A crucial ingredient of the proof of Gauss's theorem is that any (L, b) with L free of rank 3 and b perfect symmetric bilinear positive definite is isomorphic to $\mathbb{Z}^3$ with the standard inner product.

So, in order to find all possible P, one studies the (M, b) of rank 2, primitive, of discriminant n, which have an element $v \in M$ such that $b(v, v) = -n$ modulo n^2. Then the overlattice L of the orthogonal direct sum $\mathbb{Z} \oplus M$ with $(1+0) \in \mathbb{Z} \oplus M$ and $b((1+0),(1+0)) = n$, generated by $(1/n)(1+v)$ is isomorphic to $\mathbb{Z}^3$ with standard inner product and contains the element $(1+0)$ whose image in $\mathbb{Z}^3$ is our desired solution P.

The number of (M, b) that are primitive, positive definite of discriminant n is closely related to the class number of $\mathbb{Z}[\sqrt{-n}]$. Miraculously, the restriction (that is there exists $v \in M$ such that $b(v, v) = -n$ modulo n^2) on M and the number of overlattices cancel out so that the number of solutions P is, up to other subtleties, the same as 48 (the number of isomorphisms) times the class number.

3.2 The sheaf SO_3 acts transitively on spheres

Let $n \in \mathbb{Z}_{\geq 1}$. We want to understand the set of primitive solutions in $\mathbb{Z}^3$ of the equation $x^2 + y^2 + z^2 = n$, where primitive means that $\gcd(x, y, z) = 1$. Theorem 3.1.1 says how many primitive solutions there are. This suffices for the problem of understanding all solutions, because if (x, y, z) is a solution and $d := \gcd(x, y, z) > 1$, then $(x/d, y/d, z/d)$ is a primitive solution of the equation $x^2 + y^2 + z^2 = n/d^2$.

Let us define a sheaf of sets $\mathcal{X}_n$ on $\mathrm{Spec}(\mathbb{Z})$. We have $\mathcal{X}_n(\emptyset)$ is the one point set (see 2.2.2). We define, for each non-empty open $U = D(m)$ (with $m > 0$), the set $\mathcal{X}_n(U)$ as

$$\{(x, y, z) \in \mathbb{Z}[1/m]^3 : x^2 + y^2 + z^2 = n \text{ and } \gcd(x, y, z) = 1 \text{ in } \mathbb{Z}[1/m]\}.$$

Then for $V \subset U$ we have $\mathcal{X}_n(U) \subset \mathcal{X}_n(V)$, these inclusions are our restriction maps, and make $\mathcal{X}_n$ into a presheaf. It is a sheaf. Indeed, let U be a non-empty open subset in $\mathrm{Spec}(\mathbb{Z})$, and $U = \bigcup_{i \in I} U_i$ be an open covering with $U_i = D(m_i)$ for some $m_i \in \mathbb{Z}_{>0}$. Suppose $(f_i) \in \prod_{i \in I} \mathcal{X}_n(U_i)$ satisfies for any $i, j \in I$: $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_i}$ in $\mathcal{X}_n(U_i \cap U_j)$. This means that $f := f_i \in \mathbb{Q}^3$ is well-defined, and the primes that divide the denominators of coordinates of f must be the prime factors of the generator of the ideal generated by $\{m_i\}_{i \in I}$. Hence $f \in \mathcal{X}_n(U)$.

3.2.1 Remark. (For those who know about schemes.) Let X_n be the closed subscheme $Z(x^2 + y^2 + z^2 - n)$ of the 3-dimensional affine space minus the origin $\mathbb{A}^3_{\mathbb{Z}} - Z((z, y, z))$. For U an open subset of $\mathrm{Spec}(\mathbb{Z})$, $\mathcal{X}_n(U) = X_n(U) = \mathrm{Hom}(U, X_n)$. The sheaf property holds because morphisms of locally ringed spaces can be glued uniquely. Above we have given a direct proof that $\mathcal{X}_n$ is a sheaf and actually it has nothing to do with the equations, it works for any equation.

We also want a sheaf of groups acting on $\mathcal{X}_n$. For this we take groups of rotations. For any ring A we define $\mathrm{SO}_3(A)$ as:

$$\mathrm{SO}_3(A) := \{g \in \mathrm{M}_3(A) : g^t \cdot g = 1_3 \text{ and } \det(g) = 1\},$$

where $\mathrm{M}_3(A)$ is the set of 3 by 3 matrices with coefficients in A. In other words, $\mathrm{SO}_3(A)$ is the group of automorphisms of the free A-module A^3 that fix the standard inner product $\langle \cdot, \cdot \rangle : A^3 \to A$; for $x, y \in A^3$, $\langle x, y \rangle = x_1 y_1 + x_2 y_2 + x_3 y_3$, and preserve $d \colon A \to \wedge^3 A^3, 1 \mapsto e_1 \wedge e_2 \wedge e_3$ the standard orientation.

For $U = D(m)$, where $m \neq 0$, we define:

$$\mathcal{G}(U) := \mathrm{SO}_3(\mathcal{O}(U)) = \mathrm{SO}_3(\mathbb{Z}[1/m]).$$

The presheaf $\mathcal{G}$ is a sheaf (argument as for $\mathcal{X}_n$), and it acts on $\mathcal{X}_n$. The following result then makes it possible to apply Theorem 2.6.1.

3.2.2 Theorem. *Let $n \in \mathbb{Z}_{>0}$. The action of $\mathcal{G}$ on $\mathcal{X}_n$ is transitive.*

Proof. Our proof will use symmetries with respect to the inner product $\langle\cdot,\cdot\rangle : \mathbb{Q}^3 \to \mathbb{Q}$, that is for $Q \neq 0$ in $\mathbb{Q}^3$:

$$s_Q \colon \mathbb{Q}^3 \to \mathbb{Q}^3, \quad R \mapsto R - 2\frac{\langle R, Q\rangle}{\langle Q, Q\rangle}Q.$$

Transitivity is a local property on $\operatorname{Spec}(\mathbb{Z})$. That is, we need to show that for each prime number p and all primitive P and Q in $\mathbb{Z}_{(p)}^3$ with $\langle P, P\rangle = n$, and $\langle Q, Q\rangle = n$, there exists a g in $\mathrm{SO}_3(\mathbb{Z}_{(p)})$ such that $gP = Q$.

If $P = Q$, then for $g := 1_3 \in \mathrm{SO}_3(\mathbb{Z}_{(p)})$ we have $g{\cdot}P = Q$. So assume that $P \neq Q$. First suppose that $p = 2$. Consider $v \in \mathbb{Z}^3$ that satisfies $\langle v, P\rangle = 0$ and v is primitive. The set $P^\perp = \{v \in \mathbb{Z}^3 : \langle v, P\rangle = 0\}$ is a free $\mathbb{Z}$-module of rank two, with the property that if v is in $\mathbb{Z}^3$ and $d \in \mathbb{Z}$ with $d \neq 0$ and $dv \in P^\perp$, then $v \in P^\perp$. Therefore we can take a primitive $v \in \mathbb{Z}^3$ such that $\langle v, P\rangle = 0$. At least one of the coordinates of $v \in \mathbb{Z}^3$ is an odd integer, so the residue of $\langle v, v\rangle$ modulo 4 is not equal to 0. Because of that, from the formula of s_v, we get $s_v \colon \mathbb{Z}_{(2)}^3 \to \mathbb{Z}_{(2)}^3$. Also we get that $s_v(P) = P$. Now take w a primitive element in $\mathbb{Z}^3$ such that w is a multiple of the vector $P - Q$ by some number in $\mathbb{Q}$. Then the symmetry $s_w \colon \mathbb{Z}_{(2)}^3 \to \mathbb{Z}_{(2)}^3$ maps the point P to the point Q. So by construction $g := s_w \circ s_v \colon \mathbb{Z}_{(2)}^3 \to \mathbb{Z}_{(2)}^3$ will be in $\mathrm{SO}_3(\mathbb{Z}_{(2)})$ and $(s_w \circ s_v)(P) = s_w(P) = Q$.

Now let p be a prime number not equal to 2. We want to find v and w in $\mathbb{Z}_{(p)}^3$ such that s_v and s_w map $\mathbb{Z}_{(p)}^3$ to itself, and $(s_w \circ s_v)(P) = Q$. The idea is that for any v there is no choice for w: w must be a multiple of $s_v(P) - Q$. So, the conditions on $v \in \mathbb{Z}_{(p)}^3$ are: $\langle v, v\rangle$ is not divisible by p, and $w := s_v(P) - Q \in \mathbb{Z}_{(p)}^3$ has $\langle w, w\rangle$ not divisible by p, that is, their image in $\mathbb{F}_p$ is non-zero. So the existence of a v as desired is a matter of showing that there exists an element v in the $\mathbb{F}_p$-vector space $\mathbb{F}_p^3$ such that $\langle v, v\rangle \neq 0$ and, with $w := s_v(P) - Q$, $\langle w, w\rangle \neq 0$.

Both conditions are *homogeneous* in v: they are satisfied by v if and only if they are satisfied by $\lambda{\cdot}v$ for all λ in $\mathbb{F}_p^\times$. So we study these conditions on $\mathbb{P}^2(\mathbb{F}_p) = (\mathbb{F}_p^3 - \{0\})/\mathbb{F}_p^\times$. The first condition, $\langle v, v\rangle \neq 0$ means that v does not lie on the conic C defined by the homogeneous equation $x_0^2+x_1^2+x_2^2 = 0$. A simple computation shows that the second condition is equivalent to:

$$\frac{\langle P, v\rangle\langle v, Q\rangle}{\langle v, v\rangle} \neq \frac{\langle P, Q\rangle - n}{2}.$$

Note that the left hand side of the last inequality defines a function

$$f\colon \mathbb{P}^2(\mathbb{F}_p) - C(\mathbb{F}_p) \to \mathbb{F}_p, \quad \overline{v} := \mathbb{F}_p^\times{\cdot}v \mapsto \frac{\langle P, v\rangle\langle v, Q\rangle}{\langle v, v\rangle}.$$

It suffices now to show that f is not constant. Now for $\overline{v}$ in $\mathbb{P}^2(\mathbb{F}_p)-C(\mathbb{F}_p)$ we have $f(\overline{v}) = 0$ if and only if $\overline{v}$ is on the (projective) line $P^\perp$ perpendicular to P (its equation is $P_1v_1+P_2v_2+P_3v_3 = 0$), or on the line $Q^\perp$ perpendicular to Q. Each of these has $p+1$ $\mathbb{F}_p$-points, of which at most 2 are on C, hence there are $\overline{v}$ in $\mathbb{P}^2(\mathbb{F}_p) - C(\mathbb{F}_p)$ such that $f(\overline{v}) = 0$. We will now show that there is a $\overline{v}$ in $\mathbb{P}^2(\mathbb{F}_p) - C(\mathbb{F}_p)$ where $f(\overline{v})$ is not zero, by considering all $\overline{v}$ on a suitable line. The issue is that we want a proof that works for all $p \geq 3$, and not have to treat small primes differently. So, consider a line L that contains only one point R that lies on $P^\perp \cup Q^\perp$ (if $P^\perp \neq Q^\perp$ then this means that R is the intersection point of $P^\perp$ and $Q^\perp$). Then $L(\mathbb{F}_p)$ has $p+1$ points, of which one is R and of which at most two are in $C(\mathbb{F}_p)$. Therefore there are at least $p+1-3 = p-2 > 0$ points of $L(\mathbb{F}_p)$ where f is defined and is non-zero. □

To apply Theorem 2.6.1, the next step is to show the existence of an element x in $\mathcal{X}_n(\mathrm{Spec}(\mathbb{Z}))$. Besides that, an important step in proving Gauss's theorem using sheaves is to relate the stabilizer subgroup $\mathcal{H}$ of x in $\mathcal{X}_n(S)$ to the quadratic order O_d with $d = -n$ or $d = -4n$ depending on n

(mod 8) (see Section 3.5.17), and $\mathrm{H}^1(S, \mathcal{H})$ to the Picard group of O_d (see Section 3.7). It turns out that there is an exact sequence on $\mathrm{Spec}(\mathbb{Z}[1/2])$:

$$0 \to \mathcal{O}^{\times}_{\mathrm{Spec}(\mathbb{Z}[1/2])} \to \mathcal{T} \to \mathcal{H}_{\mathrm{Spec}(\mathbb{Z}[1/2])} \to 0,$$

where, for every $m > 0$ in $\mathbb{Z}$, $\mathcal{T}(\mathbb{Z}[1/2m]) = (\mathbb{Z}[1/2m, r]/(r^2+n))^{\times}$. Because we will work on $\mathrm{Spec}(\mathbb{Z}[1/2])$, the following corollary will be necessary.

3.2.3 Corollary. *Let $n \in \mathbb{Z}_{>0}$. The action of $\mathcal{G}$ on $\mathcal{X}_n$ is transitive on* $\mathrm{Spec}(\mathbb{Z}[1/2])$.

But before those two steps we will show that $\mathrm{H}^1(\mathrm{Spec}(\mathbb{Z}), \mathrm{SO}_3) = \{1\}$ and also $\mathrm{H}^1(\mathrm{Spec}(\mathbb{Z}[1/2]), \mathrm{SO}_3) = \{1\}$. We use Minkowski's theorem about lattice points in a bounded, convex and symmetric subset of $\mathbb{R}^n$ and the equivalence between free $\mathbb{Z}$-modules of rank r and locally free $\mathcal{O}_{\mathrm{Spec}(\mathbb{Z})}$-modules of rank r on $\mathrm{Spec}(\mathbb{Z})$.

3.3 Triviality of the first cohomology set of SO_3

For this section S can be either $\mathrm{Spec}(\mathbb{Z})$ or $\mathrm{Spec}(\mathbb{Z}[1/2])$, we will specify it in the statements if necessary. We consider the triple $(\mathcal{O}_S^3, b, d)$, with $b\colon \mathcal{O}_S^3 \times \mathcal{O}_S^3 \to \mathcal{O}_S$ the morphism of sheaves such that for every open subset U of S we have $b(U)$ the standard inner product and $d\colon \mathcal{O} \to \wedge^3\mathcal{O}^3$ the isomorphism of sheaves which is the standard trivialisation of the determinant (sending 1 to $e_1 \wedge e_2 \wedge e_3$). First we show the following lemma.

3.3.1 Lemma. *The inclusion* $\mathrm{SO}_3(\mathbb{Z}_{(2)}) \subset \mathrm{SO}_3(\mathbb{Q})$ *is an equality.*

Proof. We claim that $\mathrm{O}_3(\mathbb{Z}_{(2)}) = \mathrm{O}_3(\mathbb{Q})$. This claim implies the statement that we must prove. The standard basis can be mapped to any orthonormal basis by a composition of symmetries in suitable hyperplanes (recall also the proof of Theorem 3.2.2 where we use symmetries to map any vector to another vector). Thus $\mathrm{O}_3(\mathbb{Q})$ is generated by symmetries. Hence it suffices to show that any symmetry s in $\mathrm{O}_3(\mathbb{Q})$ is in $\mathrm{O}_3(\mathbb{Z}_{(2)})$. But such symmetry is of the form s_v with v a primitive element of $\mathbb{Z}^3$. For such a v, the integer $\langle v, v\rangle$ is not divisible by 4, and hence s_v is in $\mathrm{O}_3(\mathbb{Z}_{(2)})$. □

3.3.2 Remark. The previous lemma can also be proved directly from the equations of SO_3. Let $x, y, z \in \mathbb{Q}$ such that $x^2 + y^2 + z^2 = 1$. Suppose $x = \frac{p}{2^n}, y = \frac{q}{2^l}, z = \frac{r}{2^k}$, where p, q and r are in $\mathbb{Z}_{(2)}$, and $n, l, k \in \mathbb{Z}$. Without loss of generality we may assume that $k \geq l, n$. We have

$$2^{2k-2n}p^2 + 2^{2k-2l}q^2 + r^2 = 2^{2k}.$$

If $k \leq 0$, then x, y, z are in $\mathbb{Z}_{(2)}$. Now if $k > 0$, then the right hand side of the equation is divisible by 4, while the left hand side is congruent to $1, 2$ or 3 (mod 4), which is absurd. Therefore $x, y, z \in \mathbb{Z}_{(2)}$. In particular, for any odd number m, the group $\mathrm{SO}_3(\mathbb{Z}[1/2m])$ is equal to $\mathrm{SO}_3(\mathbb{Z}[1/m])$.

3.3.3 Proposition. *Let S be either* $\mathrm{Spec}(\mathbb{Z})$ *or* $\mathrm{Spec}(\mathbb{Z}[1/2])$, *with its Zariski topology. Then* $\mathrm{H}^1(S, \mathrm{SO}_3)$ *is trivial.*

Proof. A *twist* $(\mathcal{M}, b_{\mathcal{M}}, d_{\mathcal{M}})$ of $(\mathcal{O}_S^3, b, d)$ is a locally free $\mathcal{O}_S$-module $\mathcal{M}$ of rank 3 equipped with $b_{\mathcal{M}} \colon \mathcal{M} \times \mathcal{M} \to \mathcal{O}$ a symmetric bilinear form on $\mathcal{M}$ with values in $\mathcal{O}$ and $d_{\mathcal{M}} \colon \mathcal{M} \to \wedge^3\mathcal{M}$ an isomorphism of $\mathcal{O}$-modules, such that $(\mathcal{M}, b_{\mathcal{M}}, d_{\mathcal{M}})$ is locally isomorphic to $(\mathcal{O}_S^3, b, d)$. As SO_3 is the automorphism group sheaf of $(\mathbb{Z}^3, b, d)$, then as in Example 2.5.6, $\mathrm{H}^1(S, \mathcal{G})$ is the set of isomorphism classes of twists of $(\mathcal{O}_S^3, b, d)$.

Let $(\mathcal{M}, b_{\mathcal{M}}, d_{\mathcal{M}})$ be a twist of $(\mathcal{O}_S^3, b, d)$. We will show that $(\mathcal{M}, b_{\mathcal{M}}, d_{\mathcal{M}})$ is isomorphic to $(\mathcal{O}_S^3, b, d)$. We start by proving the following lemma to understand the set of global sections of $(\mathcal{M}, b_{\mathcal{M}}, d_{\mathcal{M}})$.

3.3.4 Lemma. *Let S be* Spec$(\mathbb{Z})$ *with its Zariski topology. Let $(\mathcal{O}_S^3, b, d)$ be as above definition, and $(\mathcal{M}, b_{\mathcal{M}}, d_{\mathcal{M}})$ any twist of $(\mathcal{O}_S^3, b, d)$. Then the set of global sections $\mathcal{M}(S)$ is isomorphic to $\mathbb{Z}^3$ as $\mathbb{Z}$-module, and $b_{\mathcal{M}}(S)$ is a positive definite perfect symmetric bilinear form with values in $\mathbb{Z}$.*

Proof. Because of Proposition 2.7.4, we have $\mathcal{M}(S)$ is isomorphic to $\mathbb{Z}^3$ as $\mathbb{Z}$-module.

Taking the stalk at the generic point $\eta := (0) \in S$ for $\mathcal{M}$, we get an isometry $\phi\colon \mathbb{Q}^3 \to \mathcal{M}_\eta$ with respect to the standard inner product form $\langle\cdot,\cdot\rangle$ of $\mathbb{Q}^3$. For every open U of S, we have $\mathcal{M}(U) \subset \mathcal{M}_\eta$ (by Proposition 2.7.4), therefore $b_{\mathcal{M}}$ is a symmetric, positive definite bilinear form. Moreover, the map $b_{\mathcal{M}}$ induces a map $\bar{b}_{\mathcal{M}}$ from $\mathcal{M}$ to $\mathcal{M}^\vee$: for every open U of S and $x \in \mathcal{M}(U)$, if $V \subset U, y \in \mathcal{M}(V)$ then $\bar{b}_{\mathcal{M}}(V)(y) := b(x|_V, y)$. So we have the following exact sequence of sheaves (of $\mathcal{O}$-modules)

$$0 \to \ker(\bar{b}_{\mathcal{M}}) \to \mathcal{M} \to \mathcal{M}^\vee \to \operatorname{coker}(\bar{b}_{\mathcal{M}}) \to 0.$$

Since $(\mathcal{M}, b_{\mathcal{M}}, d_{\mathcal{M}})$ is locally isomorphic to $(\mathcal{O}_S^3, b, d)$ and b is a perfect bilinear form, $\bar{b}_{\mathcal{M}}$ is also an isomorphism of sheaves, and $b_{\mathcal{M}}$ is a perfect bilinear form. In particular, $b_{\mathcal{M}}(S)$ is a positive definite perfect symmetric bilinear form with values in $\mathbb{Z}$. □

Now we can prove the proposition in 2 steps. First we will show the existence of an orthonormal basis for $\mathcal{M}(S)$ with $S = \text{Spec}(\mathbb{Z})$ by using Minkowski's theorem. We refer the reader to see again Section 2.9.

For $S = \mathrm{Spec}(\mathbb{Z})$, we have shown that $M := \mathcal{M}(S)$ is isomorphic to $\mathbb{Z}^3$ as $\mathbb{Z}$-module, and b_M is a positive definite perfect symmetric bilinear form with values in $\mathbb{Z}$. Let m be a shortest non-zero element of M. Suppose that $b_M(m,m) \geq 2$. Then the open ball with radius $\sqrt{2}/2$ in $M_{\mathbb{R}} := M \otimes_{\mathbb{Z}} \mathbb{R}$ maps injectively into $M_{\mathbb{R}}/M$. Hence the volume of $M_{\mathbb{R}}/M$ is at least $(4\pi/3)\cdot(\sqrt{2}/2)^3 = \sqrt{2}\pi/3 > 1$. On the other hand the discriminant of (M, b_M, d_M) is equal to 1 because b_M is perfect and positive definite. Hence there is an element m in M with $b_M(m,m) = 1$. Then $M = \mathbb{Z}m \oplus m^{\perp}$, and continuing our argument with $m^{\perp}$ shows that M has an orthonormal basis. This concludes the proof that $\mathrm{H}^1(\mathrm{Spec}(\mathbb{Z}), \mathrm{SO}_3)$ is trivial.

Let S now be $\mathrm{Spec}(\mathbb{Z}[1/2])$. By Lemma 3.3.1, for any odd number m, the group $\mathrm{SO}_3(\mathbb{Z}[1/2m])$ is equal to $\mathrm{SO}_3(\mathbb{Z}[1/m])$. We take any element $g \in \mathrm{H}^1(\mathrm{Spec}(\mathbb{Z}[1/2]), \mathrm{SO}_3)$. By Proposition 2.8.4, there exists an open covering $(U_i)_{i\in I}$ of S where $U_i = D(2m_i)$ and m_i odd, and a 1-cocycle $(g_{ij} \in \mathrm{SO}_3(U_i \cap U_j))_{i,j\in I\times I}$ such that g is the cohomology class of $(g_{ij})_{i,j\in I\times I}$. Since $\mathrm{SO}_3(\mathbb{Z}[1/2m_im_j]) = \mathrm{SO}_3(\mathbb{Z}[1/m_im_j])$, then $(g_{ij})_{i,j\in I\times I}$ is a 1-cocycle for SO_3 on $\mathrm{Spec}(\mathbb{Z})$ with the cover $(D(m_i))_{i\in I}$. There it is a boundary of a 0-cocycle $h = (h_i)_{i\in I}$. Then $(g_{ij} \in \mathrm{SO}_3(U_i \cap U_j))_{i,j\in I\times I}$ is the boundary of h restricted to $\mathrm{Spec}(\mathbb{Z}[1/2])$. So we have $\mathrm{H}^1(\mathrm{Spec}(\mathbb{Z}[1/2]), \mathrm{SO}_3) = \{1\}$. □

3.4 Existence of integral solutions

We will use sheaf theory to prove the following theorem by Legendre.

3.4.1 Theorem. (Legendre) *Let n be in $\mathbb{N}$.*

1. *If $n \neq 0, 4, 7$ (mod 8), then $\mathcal{X}_n(\mathbb{Z}) \neq \emptyset$.*

2. *If n is not of the form $4^a(8b+7)$ with $a \in \mathbb{N}$ and $b \in \mathbb{Z}_{\geq 0}$, then there exists $(x, y, z) \in \mathbb{Z}^3$ such that $x^2 + y^2 + z^2 = n$.*

To prove this theorem we need several steps.

3.4.2 Existence of a rational solution

First we need the existence of a rational solution, so in this case we can assume that n is square free and $n \neq 0, 4, 7 \pmod 8$. We will use the following theorem by Hasse-Minkowski to get a 'global' solution, that is a solution over the field $\mathbb{Q}$ of rational numbers, from local solutions, that are solutions over all p-adic numbers $\mathbb{Q}_p$ and a solution over the field $\mathbb{R}$ of real numbers.

3.4.3 Theorem. (Hasse-Minkowski) *Let m be a positive integer, and $f\colon \mathbb{Q}^m \to \mathbb{Q}$, $x \mapsto \Sigma_{i \leq j} a_{i,j} x_i x_j$, where $a_{i,j}$ are elements of $\mathbb{Q}$, a quadratic form. In order that $f = 0$ has a nontrivial solution in $\mathbb{Q}^m$, it is necessary and sufficient that, for all prime numbers p, the equation $f = 0$ has a nontrivial solution in $\mathbb{Q}_p^m$, and also the equation $f = 0$ has a nontrivial real solution.*

Proof. See [17], Chapitre IV, Théorème 8. □

To apply Hasse-Minkowski's theorem in our case, we consider the quadratic form

$$f\colon \mathbb{Q}^4 \to \mathbb{Q}, (x, y, z, t) \mapsto x^2 + y^2 + z^2 - nt^2.$$

Over the field $\mathbb{R}$ of real numbers, the equation $f = 0$ clearly has the nontrivial solution $(\sqrt{n}, 0, 0, 1)$. For any prime number p we want to get the solution in $\mathbb{Q}_p$, we apply Hensel's lemma to lift a "smooth" solution over the finite field $\mathbb{F}_p$ to a solution over the ring of p-adic integer $\mathbb{Z}_p$. Here is the statement.

3.4.4 Theorem. (Hensel's lemma) *Let p be a prime number, $\mathbb{Z}_p$ the ring of p-adic integers, and $f \in \mathbb{Z}_p[x_1, \dots, x_m]$ a polynomial. If $f = 0$ has a solution a in $\mathbb{F}_p^m$ and $f'(a) \neq 0$ in $\mathbb{F}_p^m$, where f' is the formal derivative of f, then there exists b in $\mathbb{Z}_p^m$ such that $f(b) = 0$ with $b_i = a_i \mod p\mathbb{Z}_p$.*

Proof. See [20], Chapter 11, Theorem 3.6. □

For every prime number p, it is sufficient to consider the equation

$$x^2 + y^2 + z^2 = n$$

over $\mathbb{Z}_p$. First we work for $p = 2$. Let $x \in \mathbb{Z}_2^\times$, thus $x = 1 + 2a$ for some $a \in \mathbb{Z}_2$, and $x^2 = 1 + 4a(a+1) \in 1 + 8\mathbb{Z}_2$. For any $b \in \mathbb{Z}_2$, the polynomial equation $t(t+1) - 2b = 0$ has a solution in $\mathbb{F}_2$, and its derivative is $1 \neq 0$. Therefore, by Hensel's lemma above, we get an $a \in \mathbb{Z}_2$ such that $(1+2a)^2 = 1 + 8b$. We have proven that $\{x^2 : x \in \mathbb{Z}_2^\times\} = 1 + 8\mathbb{Z}_2$. Since $n \neq 0, 4, 7$, then it is the sum of 3 squares in $\mathbb{Z}_2$ by taking $x, y \in \{0, 1, 2\}$, and $z \in \mathbb{Z}_2^\times$. Hence, we have a nontrivial solution of the quadratic form $x^2 + y^2 + z^2 - nt^2$ in $\mathbb{Q}_2$.

Now let $p > 2$. We want to find a solution of the quadric $x^2+y^2+z^2-n = 0$ over $\mathbb{F}_p$ such that the derivative $(2x, 2y, 2z) \neq (0, 0, 0)$. We fix a non-zero $z \in \mathbb{F}_p$. If we let y vary in $\mathbb{F}_p$, then there are $\frac{p+1}{2}$ different values of $n - z^2 - y^2$. Since there are only $\frac{p-1}{2}$ non-square element in $\mathbb{F}_p$, thus at least one value of $n - z^2 - y^2$ is a square element. By Hensel's lemma, we find a non-trivial solution for the equation $x^2 + y^2 + z^2 - nt^2 = 0$ over $\mathbb{Q}_p$.

3.4.5 Existence of a solution over $\mathbb{Z}_{(p)}$

Having found a solution in $\mathcal{X}_n(\mathbb{Q})$, our next step is to bring the rational solution to any "local" solution, that is for any prime number p, a solution in $\mathcal{X}_n(\mathbb{Z}_{(p)})$.

As in Remark 3.3.1, if $x, y, z \in \mathbb{Q}$ such that $x^2 + y^2 + z^2 = n$, then $x, y, z \in \mathbb{Z}_{(2)}$. Suppose 4 divides n, and $x, y, z \in \mathbb{Z}_{(2)}$ such that $x^2+y^2+z^2 = n$. Then x, y, z are 0 (mod 2). Since we are interested in the set of primitive solutions in $\mathbb{Z}^3$ of the equation $x^2 + y^2 + z^2 = n$, we assume that $n \neq 0, 4, 7$ (mod 8) and we have the $(x, y, z) \in \mathbb{Z}^3_{(2)}$ is in $\mathcal{X}_n(\mathbb{Z}_{(2)})$.

Now let $p \neq 2$ be prime. Let us define for $y \in \mathbb{Q}_p^m$,

$$v(y) = \min\{v(y_i); i = 1, ..., m\}.$$

3.4.6 Lemma. *Let $m > 1$ be an integer, and $x \in \mathbb{Q}_p^m$ such that $\langle x, x\rangle \neq 0$, $\langle x, x\rangle \in \mathbb{Z}_p$ and $v(x) < 0$. Let $i := v(\langle x, x\rangle) - v(x) - 1$. Then for all $u \in \mathbb{Z}_p^m$ such that $v(\langle u, x\rangle) = v(x)$, we have $v(s_{x+p^i u}(x)) > v(x)$. Moreover such u exist, even in $\mathbb{Z}^m_{(p)}$.*

Proof. First we show the existence $u \in \mathbb{Z}_p^m$ such that $v(\langle u, x\rangle) = v(x)$. Let $y = p^{-v(x)}x$. Then $v(y) = 0$. It suffices to show that there exists $u \in \mathbb{Z}_p^m$ such that $v(\langle u, y\rangle) = 0$. This is equivalent to the existence of $\bar{u}$ in $\mathbb{F}_p^m$ such that $\langle \bar{u}, \bar{y}\rangle \neq 0$ (here $\bar{y}$ denotes the reduction mod $p\mathbb{Z}_p$). This is clear since the equation $\langle \bar{u}, \bar{y}\rangle \neq 0$ is the complement of a hyperplane in the affine space $\mathbb{F}_p^m$. Note that such u can be taken in $\mathbb{Z}^m_{(p)}$.

Let $u \in \mathbb{Z}_p^m$ such that $v(\langle u, x\rangle) = v(x)$ and $i := v(\langle x, x\rangle) - v(x) - 1$. We consider the following identity:

$$s_{x+p^i u}(x) = x - \frac{2\langle x, x + p^i u\rangle}{\langle x + p^i u, x + p^i u\rangle}(x + p^i u).$$

We have $\langle x, x + p^i u\rangle = \langle x, x\rangle + p^i\langle x, u\rangle$. The valuation $v(\langle x, x\rangle)$ is greater than $v(p^i\langle x, u\rangle)$ because

$$v(p^i\langle x, u\rangle) = i + v(\langle u, x\rangle) = i + v(x) = v(\langle x, x\rangle) - 1.$$

Then

$$v(\langle x, x+p^i u\rangle) = \min\{v(\langle x, x\rangle), i+v(x)\} = v(\langle x, x\rangle) - 1,$$

and the leading term of $\langle x, x+p^i u\rangle$ is $p^i\langle x, u\rangle$. For the denominator of the fraction we have

$$\langle x+p^i u, x+p^i u\rangle = \langle x, x\rangle + 2p^i\langle x, u\rangle + p^{2i}\langle u, u\rangle.$$

Since $\langle u, u\rangle \in \mathbb{Z}_p$, $i \geq 0$, and $v(x) < 0$ we get

$$v(p^{2i}\langle u, u\rangle) \geq 2i > i + v(x) = v(2p^i\langle x, u\rangle).$$

So the leading term of $\langle x+p^i u, x+p^i u\rangle$ is $2p^i\langle x, u\rangle$. This implies the fraction in the formula of $s_{x+p^i u}(x)$ is in the form $(1+p\epsilon)$ where ϵ in $\mathbb{Z}_p$. Thus $v(s_{x+p^i u}(x)) > v(x)$. □

3.4.7 Proposition. *Let n be a natural number such that $n \neq 0, 4, 7$ (mod 8). Then for every prime number p, the set $\mathcal{X}_n(\mathbb{Z}_{(p)})$ is non-empty.*

Proof. Let $p \neq 2$ be a prime number. By applying Lemma 3.4.6 with $m = 3$ and $x \in \mathbb{Q}^3 \hookrightarrow \mathbb{Q}_p^3$ such that $\langle x, x\rangle = n$ repeatedly, we obtain a point $x = (a, b, c) \in \mathbb{Z}_{(p)}^3$ such that $a^2+b^2+c^2 = n$ and $v(x) \geq 0$. If $v(x) = 0$, then $x \in \mathcal{X}_n(\mathbb{Z}_{(p)})$. Suppose $v(x) > 0$. We write $x = p^{v(x)}x'$ with $x' = (a', b', c') \in \mathbb{Z}_{(p)}^3$. We claim that there exists a primitive point $u \in \mathbb{Z}^3$ such that $v(s_u(x)) = v(x) - 1$. To prove the claim, let $u = (k, l, m)$ be a primitive point in $\mathbb{Z}^3$ such that $\langle \bar{u}, \bar{u}\rangle = 0$ and $\langle \bar{u}, \bar{x'}\rangle \neq 0$ in $\mathbb{F}_p$: take any lift in $\mathbb{Z}^3$ from a point in the conic $x^2+y^2+z^2 = 0$ over $\mathbb{F}_p$, that does not belong the line $a'x + b'y + c'z = 0$. In particular, we can take $0 \leq k, l, m \leq \frac{p-1}{2}$. This choice implies that $k^2+l^2+m^2 < p^2$, so $p^2 \nmid k^2+l^2+m^2$. Now let

s_u be the symmetry with respect to the primitive point u. We have the identity

$$s_u(x) = x - 2\frac{\langle u, x\rangle}{\langle u, u\rangle}u.$$

By the choice of the point u, we have also

$$v\left(2\frac{\langle u, x\rangle}{\langle u, u\rangle}u\right) = v(x) + v\left(2\frac{\langle u, x'\rangle}{\langle u, u\rangle}u\right) = v(x) - 1.$$

In particular we get $v(s_u(x)) = v(x) - 1$. By applying the symmetry s_u repeatedly, we get $v(x) = 0$ and $x \in \mathcal{X}_n(\mathbb{Z}_{(p)})$. □

3.4.8 The proof of Legendre's theorem by sheaf theory

The last step is about how to glue "local" solutions, that is a family of solutions in $\mathcal{X}_n(\mathbb{Z}_{(p)})$ for each prime number p, to a global solution, that is a solution in $\mathcal{X}_n(\mathbb{Z})$. We will use sheaf theory to show it. Let us define for a matrix $A = (a_{ij})_{1\leq i\leq k, 1\leq j\leq m} \in \mathrm{M}_{k\times m}(\mathbb{Q})$,

$$\mathrm{denom}(A) := \mathrm{lcm}(\mathrm{denom}(a_{ij}); 1 \leq i \leq k, 1 \leq j \leq m)\ .$$

Proof. Let S be $\mathrm{Spec}(\mathbb{Z})$ with its Zariski topology. From Proposition 3.4.7, there exist solutions in $\mathcal{X}_n(\mathbb{Z}_{(p)})$, for all prime numbers p. Let p_0 be a prime number and $x_0 \in \mathcal{X}_n(\mathbb{Z}_{(p_0)})$. Let U_0 be the complement in S of the finite set of primes p such that $x_0 \notin \mathcal{X}_n(\mathbb{Z}_{(p)})$. Then $x_0 \in \mathcal{X}_n(U_0)$. Write $S - U_0 = \{p_1, \ldots, p_m\}$ with the p_i distinct. For each $i \in \{1, \ldots, m\}$, let $x_i \in \mathcal{X}_n(\mathbb{Z}_{(p_i)})$.

Since $\mathcal{G}$ acts transitively on $\mathcal{X}_n$, for each $1 \leq i \leq m$ there exists $g_{i0} \in \mathcal{G}(\mathbb{Q})$ such that $x_i = g_{i0} \cdot x_0$. Note that the g_{i0} is unique up to right multiplication by elements in the stabilizer subgroup $\mathcal{G}_{x_0}(\mathbb{Q})$. For $1 \leq i, j \leq m$, we define

$g_{ij} := g_{i0} \cdot g_{j0}^{-1} \in \mathcal{G}(\mathbb{Q})$ that maps x_j to x_i. These g_{ij} satisfy the 1-cochain property, that is for every i, j, k we have $g_{ik} = g_{ij} \cdot g_{jk}$. Let us define a number

$$d := \mathrm{lcm}(\mathrm{denom}(g_{ij}) : 0 \leq i, j \leq m, \mathrm{denom}(x_i) : 0 \leq i \leq m, p_1 p_2 \ldots p_m).$$

For each $1 \leq i \leq m$, let us define $U_i := \{p_i\} \cup \mathrm{Spec}(\mathbb{Z}[1/d])$. These are open subsets of S. Thus we have $S = U_0 \cup U_1 \cup \cdots \cup U_m$, and for all $0 \leq i, j \leq m$, $i \neq j$,

$$U_i \cap U_j = \mathrm{Spec}(\mathbb{Z}[1/d])), g_{ij} \in \mathcal{G}(U_i \cap U_j).$$

As $\mathrm{H}^1(S, \mathcal{G}) = \breve{\mathrm{H}}^1(S, \mathcal{G})$ is trivial, there exist $g_0, g_1, \ldots, g_r$ with $g_i \in \mathcal{G}(U_i)$, such that in the intersection $U_i \cap U_j$ we have $g_{ij} = g_i \cdot g_j^{-1}$.

Now for every $0 \leq i \leq m$, we let $x_i' := g_i^{-1} \cdot x_i$. For each i, by construction of U_i, x_i' is an element of $\mathcal{X}_n(U_i)$. In the intersection $U_i \cap U_j$, we have

$$x_j' = g_j^{-1} \cdot x_j = g_i^{-1} \cdot g_{ij} \cdot x_j = g_i^{-1} \cdot x_i = x_i'.$$

Since $\mathcal{X}_n$ is a sheaf of sets, there exists a unique $x' \in \mathcal{X}_n(S)$ such that $x'|_{U_i} = x_i'$. Thus we find a global solution $x' \in \mathcal{X}_n(S)$ as desired. □

3.4.9 Remark. We refer to [17], Chapitre IV-Appendice or [5] for other proofs of Legendre's theorem about the existence of integral points. The classical proof of this theorem by Dirichlet requires three main lemmas: the quadratic reciprocity law, Dirichlet's theorem on primes in arithmetic progressions, and that every perfect lattice of rank 3 is isomorphic to $\mathbb{Z}^3$ with the standard inner product. Note that the proof of the existence of integral solutions of the sums of 3 squares equation is called Legendre's theorem although most likely Legendre did not prove the quadratic reciprocity law completely, as Gauss did. A conceptual description of the proof given above in more advanced language (see [8]) is as follows. There is an $\mathcal{H}$-gerbe

$[\mathcal{G}\backslash\mathcal{X}_n]$, with $\mathcal{H}$ the stabiliser group (glued from local stabilisers). Then $\mathrm{H}^2(S, \mathcal{H}) = \{1\}$ because the dimension of S is 1. This gives that this gerbe is neutral: $[\mathcal{G}\backslash\mathcal{X}_n](S)$ is not empty. Because $\mathrm{H}^1(S, \mathcal{G}) = \{1\}$ we have $\mathcal{X}_n(S)$ is not empty.

3.5 The stabilizer in Gauss's theorem

Let n be a natural number such that $n \neq 0, 4, 7 \pmod 8$. Let $P = (x, y, z)$ be a primitive solution of the equation in $\mathbb{Z}^3$ (see Theorem 3.4.1). As in the Definition 2.4.1, we define the stabilizer $H := \mathrm{SO}_{3,P}$ of P in the group scheme SO_3. So for any ring A we define:

$$H(A) := \{g \in \mathrm{SO}_3(A) : gP = P\}.$$

In particular for $U = D(m)$, where $m \neq 0$, we define

$$\mathcal{G}_P(U) := H(\mathbb{Z}[1/m]).$$

The presheaf $\mathcal{G}_P$ is a sheaf of subgroups of $\mathcal{G}$.

3.5.1 Remark. For the field of real numbers $\mathbb{R}$, $\mathrm{SO}_{3,P}(\mathbb{R})$ is the group of rotations with axis $\mathbb{R} \cdot P$, therefore it is a circle group. In particular it is commutative.

3.5.2 Lemma. *Let $P, Q \in \mathcal{X}_n(\mathbb{Z})$. Then we have a canonical isomorphism of sheaves $\phi\colon \mathcal{G}_Q \to \mathcal{G}_P$ in the Zariski topology on* $\mathrm{Spec}(\mathbb{Z})$.

Proof. By Corollary 3.2.3, there exists an open covering $(U_i)_{i \in I}$ of $\mathrm{Spec}(\mathbb{Z})$, and a family of elements $(g_i \in \mathcal{G}(U_i))_{i \in I}$ such that for every $i \in I, g_i P = Q$. Then for each i, we have an isomorphism of sheaves of groups

$$\phi_{U_i}\colon \mathcal{G}_P|_{U_i} \to \mathcal{G}_Q|_{U_i}, h \mapsto g_i h g_i^{-1}.$$

On the intersection $U_i \cap U_j$, we have $g_j = g_i \cdot h_{ij}$ in $\mathcal{G}(U_i \cap U_j)$, for a unique $h_{ij} \in \mathcal{G}_P(U_i \cap U_j)$. Because $\mathcal{G}_P(\mathbb{Q})$ is a subgroup of $\mathrm{SO}_{3,P}(\mathbb{R})$, it is commutative. Thus on the intersection $U_i \cap U_j$, the morphism ϕ_{U_i} is equal to ϕ_{U_j}. They glue together and we get the isomorphism of sheaves ϕ. See Theorem 2.6.1 for this argument in a more general situation. □

From the lemma above, the stabilizer of $P \in \mathcal{X}_n(\mathbb{Z})$ in $\mathcal{G}$ does not depend on the choice of the point P as a sheaf in the Zariski topology on $\mathrm{Spec}(\mathbb{Z})$. So let us denote $\mathcal{H} := \mathcal{G}_P$ for the stabilizer of some point $P \in \mathcal{X}_n(\mathbb{Z})$ in $\mathcal{G}$. We will determine $\mathcal{H}$, only over $\mathrm{Spec}(\mathbb{Z}[1/2])$, but it will be enough.

3.5.3 Remark. The sheaf of groups $\mathcal{H}$ does not depend on the choice of the point P, but the embedding of $\mathcal{H}$ into $\mathcal{G}$ does depend on the choice of the point P.

3.5.4 The orthogonal complement $P^\perp$ of P in $\mathbb{Z}^3$

We start by considering $P^\perp := \{Q \in \mathbb{Z}^3 : \langle Q, P \rangle = 0\}$, the orthogonal complement of P. Since $\mathbb{Q} \otimes_{\mathbb{Z}} P^\perp$ is of dimension 2 and $P^\perp$ is torsion free, $P^\perp$ is a free $\mathbb{Z}$-module of rank 2. We equip $P^\perp$ with b, the symmetric bilinear form obtained by restricting that of $\mathbb{Z}^3$, and d, the orientation of $P^\perp$ coming from P and the standard orientation of $\mathbb{Z}^3$

3.5.5 Lemma. *Let $P \in \mathcal{X}_n(\mathbb{Z})$. Then the symmetric bilinear form b on $P^\perp$ obtained by restricting $\langle \cdot, \cdot \rangle$ from $\mathbb{Z}^3$ is positive definite, primitive, and its discriminant is n.*

Proof. The positive definiteness is clear since it is the restriction of a positive definite symmetric bilinear form. Now let us first prove the primitivity of b. Because P is primitive, we have the following exact sequence

$$\begin{tikzcd}
0 \arrow[r] & P^{\perp} \arrow[r] & \mathbb{Z}^3 \arrow[r, "b_P"] & \mathbb{Z} \arrow[r] & 0 \\
0 \arrow[r] & P^{\perp} \arrow[r] \arrow[u, "\wr"'] & \mathbb{Z} \cdot P \oplus P^{\perp} \arrow[r] \arrow[u, hook] & n \cdot \mathbb{Z} \arrow[r] \arrow[u, hook] & 0,
\end{tikzcd}$$

where $b_P \colon Q \mapsto \langle Q, P\rangle$. This map has a section $1 \mapsto Q$, where $Q \in \mathbb{Z}^3$ is any point that satisfies $\langle Q, P\rangle = 1$. We get that $\mathbb{Z}^3/P^{\perp}$ is a free $\mathbb{Z}$ module of rank 1. Any $\mathbb{Z}$-basis (e_1, e_2) of $P^{\perp}$ can be extended to a basis (e_1, e_2, e_3) of $\mathbb{Z}^3$, such that $\langle e_3, P\rangle = 1$. Let $g = (\langle e_i, e_j\rangle)_{i,j}$ be the Gram matrix relative to that basis. As the discriminant of $(\mathbb{Z}^3, \langle \cdot, \cdot \rangle)$ is equal to one, we have $\det(g) = 1$. In particular, at every prime number p, the rank g in $\mathrm{M}_3(\mathbb{F}_p)$ is equal to 3. If follows that not all g_{ij} with $1 \leq i, j \leq 2$ can be zero in $\mathbb{F}_p$. This implies that $(P^{\perp}, b)$ is primitive.

By the snake lemma for the diagram above, we get $\mathbb{Z}^3/(\mathbb{Z} \cdot P \oplus P^{\perp})$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. The submodule $P^{\perp} \oplus \mathbb{Z} \cdot P$ has index n in $\mathbb{Z}^3$, hence $\mathrm{discr}(P^{\perp} \oplus \mathbb{Z} \cdot P, \langle \cdot, \cdot \rangle) = n^2$. As this direct sum is orthogonal, we have

$$n^2 = \mathrm{discr}(P^{\perp} \oplus \mathbb{Z} \cdot P) = \mathrm{discr}(P^{\perp}, b). \, \mathrm{discr}(\mathbb{Z} \cdot P, \langle \cdot, \cdot \rangle) = \mathrm{discr}(P^{\perp}, b) \cdot n.$$

We conclude that $(P^{\perp}, b)$ is $\mathbb{Z}$-module of rank 2 with positive definite primitive symmetric bilinear form of discriminant n. □

3.5.6 Remark. We have the exact sequence $0 \to P^{\perp} \to \mathbb{Z}^3 \xrightarrow{b_P} \mathbb{Z} \to 0$. Because P is primitive, the sequence $0 \to P^{\perp} \to \mathbb{Z}^3 \xrightarrow{b_P} \mathbb{Z} \to 0$ admits a splitting. Let A be a ring. By tensoring with A over $\mathbb{Z}$, thus the sequence $0 \to A \otimes_{\mathbb{Z}} P^{\perp} \to A^3 \xrightarrow{\mathrm{id}_A \otimes b_P} A \to 0$ is exact and

$$\{(a, b, c) \in A^3 : \langle (a, b, c), P\rangle = 0\} = A \otimes_{\mathbb{Z}} P^{\perp}.$$

3.5.7 The embedding of $\mathcal{H}$ in $\mathcal{N}$

Let us consider $N := SO(P^{\perp})$ the automorphism group scheme of $(P^{\perp}, b, d)$. For a ring A, we define $N(A)$ as:

$$N(A) := \mathrm{Aut}(A \otimes (P^{\perp}, b, d)).$$

We define the presheaf of groups $\mathcal{N}$ on $\mathrm{Spec}(\mathbb{Z}[1/2])$: for any non-empty open subset $U = D(2m)$ of $\mathrm{Spec}(\mathbb{Z}[1/2])$, where $m \neq 0$ is odd,

$$\mathcal{N}(U) := N(\mathbb{Z}[1/2m]).$$

The presheaf $\mathcal{N}$ is a sheaf of groups on $\mathrm{Spec}(\mathbb{Z}[1/2])$ (see Section 3.2, in particular Remark 3.2.1).

3.5.8 Remark. We can write equations for N explicitly if we choose a $\mathbb{Z}$-basis for $P^{\perp}$. Let us write

$$\mathbb{Z}^3 = P^{\perp} \oplus \mathbb{Z} \cdot e_3 = (\mathbb{Z} \cdot e_1 \oplus \mathbb{Z} \cdot e_2) \oplus \mathbb{Z} \cdot e_3,$$

where (e_1, e_2) is a basis of $P^{\perp}$ and $\langle e_3, P \rangle = 1$. We denote B for the Gram matrix of the symmetric bilinear form b on $P^{\perp}$ with our chosen basis (e_1, e_2). For a ring A, we get

$$N(A) := \{g \in \mathrm{M}_2(A) : g^t \cdot B \cdot g = B \text{ and } \det(g) = 1\},$$

where $\mathrm{M}_2(A)$ is the set of 2 by 2 matrices with coefficients in A.

Let A be a ring and $g \in H(A)$. For $Q \in P_A^{\perp} := A \otimes_{\mathbb{Z}} P^{\perp}$, we have

$$\langle gQ, P \rangle = \langle Q, g^t P \rangle = \langle Q, P \rangle = 0.$$

Thus $gQ \in P_A^{\perp}$. We have the action of $H(A)$ on $P_A^{\perp}$. It gives a morphism of groups $H(A) \to N(A)$ and a natural morphism of groups schemes $H \to N$.

The element $(1/n)P$ of $\mathbb{Z}[1/2n]^3$ is mapped to 1 in $\mathbb{Z}[1/2n]$ in the exact sequence

$$0 \to P^{\perp}_{\mathbb{Z}[1/2n]} \to \mathbb{Z}[1/2n]^3 \xrightarrow{\mathrm{id}_{\mathbb{Z}[1/2n]}\otimes b_P} \mathbb{Z}[1/2n] \to 0.$$

Therefore $\mathbb{Z}[1/2n]^3$ is the orthogonal direct sum of $P^{\perp}_{\mathbb{Z}[1/2n]}$ and $\mathbb{Z}[1/2n]\cdot P$. Thus over $\mathbb{Z}[1/2n]$, $\mathcal{H} \to \mathcal{N}$ is an isomorphism of sheaves. For the same reason, $\mathbb{Q}^3$ is the orthogonal direct sum of $P^{\perp}_{\mathbb{Q}}$ with $\mathbb{Q}\cdot P$, therefore the injection $\mathcal{H}(\mathbb{Q}) \to \mathcal{N}(\mathbb{Q})$ is an isomorphism of groups. In particular we have an injection $\mathcal{H} \to \mathcal{N}$ on $\mathrm{Spec}(\mathbb{Z}[1/2])$. The next lemma is the first step to make the cokernel of the map $\mathcal{H} \to \mathcal{N}$ in the category $\mathrm{Sh}(\mathrm{Spec}(\mathbb{Z}[1/2]))$ explicit.

3.5.9 Lemma. *Let $p \neq 2$ be a prime dividing n. Then $\mathcal{H}(\mathbb{Z}_{(p)})$ is the set of g in $\mathcal{N}(\mathbb{Z}_{(p)})$ that fix $P_{\mathbb{F}_p}$ in $P^{\perp}_{\mathbb{F}_p}$, where $P_{\mathbb{F}_p}$ denotes the image of P in $\mathbb{F}_p^3$.*

Proof. Since the prime $p \neq 2$ divides n, $\langle P_{\mathbb{F}_p}, P_{\mathbb{F}_p}\rangle = 0$ in $\mathbb{F}_p$. As P is primitive, $P_{\mathbb{F}_p} \neq 0$. Let g be in $\mathcal{N}(\mathbb{Z}_{(p)})$ such that $gP_{\mathbb{F}_p} = P_{\mathbb{F}_p}$. Let v in $P^{\perp}$ be a lift over $\mathbb{Z}$ of an element of $P^{\perp}_{\mathbb{F}_p} - \mathbb{F}_p \cdot P_{\mathbb{F}_p}$ (elements in $P^{\perp}_{\mathbb{F}_p}$ which are not in $\mathbb{F}_p \cdot P_{\mathbb{F}_p}$). Since b is a primitive bilinear form on $P^{\perp}$ (see Lemma 3.5.5), $\langle v, v\rangle \neq 0$ in $\mathbb{F}_p$. Let s_v be the symmetry in $P^{\perp}_{\mathbb{Z}_{(p)}}$ with respect to v. Then $s_v g$ is an automorphism of $(P^{\perp}_{\mathbb{Z}_{(p)}}, b)$ of determinant -1. Then $s_v g$ has eigenvalues 1 and -1. Therefore, $P^{\perp}_{\mathbb{Z}_{(p)}}$ decomposes as an orthogonal direct sum $L^+ \oplus L^-$ of eigenspaces (free $\mathbb{Z}_{(p)}$-modules of rank one) with eigenvalues 1 and -1, respectively. The line $\mathbb{F}_p \cdot P_{\mathbb{F}_p} = L^+_{\mathbb{F}_p}$, hence $\mathbb{F}_p \cdot P_{\mathbb{F}_p} \neq L^-_{\mathbb{F}_p}$. Let w be a basis of L^-, then $\langle w, w\rangle \neq 0$ in $\mathbb{F}_p$ and $s_v g = s_w$. We conclude that $g = s_v s_w$ and, now letting s_v and s_w be symmetries in $\mathbb{Z}^3_{(p)}$, that g is in $\mathcal{H}(\mathbb{Z}_{(p)})$. □

The following lemma describes $N(\mathbb{F}_p)$.

3.5.10 Lemma. *Let $p \neq 2$ be a prime number such that p divides n. Then for a basis (e_1, e_2) of $P_{\mathbb{F}_p}^{\perp}$ with $e_1 = P_{\mathbb{F}_p}$, we have*

$$N(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix} : a, b \in \mathbb{F}_p \text{ and } a^2 = 1 \right\}.$$

Proof. Let (e_1, e_2) be a basis of $P_{\mathbb{F}_p}^{\perp}$ with $e_1 = P_{\mathbb{F}_p}$. Since the bilinear form b on $P^{\perp}$ is primitive, we have $\langle e_2, e_2 \rangle \neq 0$. With respect to this basis, let h be any element of $N(\mathbb{F}_p)$. Let us write it as

$$h = \begin{pmatrix} a & b \\ d & e \end{pmatrix} \in \mathrm{M}_2(\mathbb{F}_p).$$

Then we get the following identities

$$0 = \langle e_1, e_1 \rangle = \langle h.e_1, h.e_1 \rangle = \langle ae_1 + de_2, ae_1 + de_2 \rangle = d^2 \langle e_2, e_2 \rangle,$$

$$0 = \langle e_1, e_2 \rangle = \langle h.e_1, h.e_2 \rangle = \langle ae_1 + de_2, be_1 + ee_2 \rangle = de \langle e_2, e_2 \rangle,$$

$$\langle e_2, e_2 \rangle = \langle h.e_2, h.e_2 \rangle = \langle be_1 + ee_2, be_1 + ee_2 \rangle = e^2 \langle e_2, e_2 \rangle,$$

and $\det(h) = ae - bd = 1$. So we get $d = 0, a = e = \pm 1$ and the conclusion follows. □

Let us define Φ to be the sheaf on $\mathrm{Spec}(\mathbb{Z}[1/2])$, for the Zariski topology, by:

$$\Phi = \bigoplus_{2 \neq p | n} i_{p,*} \mathbb{F}_2,$$

that is, the direct sum over the primes $p \neq 2$ dividing n of the pushforward of the constant sheaf $\mathbb{F}_2$ on $\mathrm{Spec}(\mathbb{F}_p)$ via the embedding i_p of $\mathrm{Spec}(\mathbb{F}_p)$

into Spec($\mathbb{Z}$). For any non-empty open subset $U = D(2m)$ of Spec($\mathbb{Z}[1/2]$), where $m \neq 0$ is odd, we have

$$\Phi(U) = \bigoplus_{2 \neq p | n, p \nmid m} \mathbb{F}_2.$$

We have a surjective morphism of sheaves of groups $\phi' \colon \mathcal{N} \to \Phi$ such that Φ is the cokernel for the injection $\mathcal{H} \to \mathcal{N}$ as follows. For each such $p \neq 2$ dividing n, we have a morphism of groups $\phi'_p \colon \mathcal{N}(\mathbb{Z}_{(p)}) \to \mathbb{F}_2$, that sends g to 0 if $\bar{g}P_{\mathbb{F}_p} = P_{\mathbb{F}_p}$ in $P^{\perp}_{\mathbb{F}_p}$ and to 1 if $\bar{g}P_{\mathbb{F}_p} = -P_{\mathbb{F}_p}$. For any non-empty open subset $U = D(2m)$ of Spec($\mathbb{Z}[1/2]$), where $m \neq 0$ is odd, we define

$$\phi'(U) \colon \mathcal{N}(U) \to \Phi(U), g \mapsto (\phi'_p(g))_{2 \neq p | n, p \nmid m}.$$

By Lemma 3.5.10, ϕ' is a surjective morphism of sheaves. Together with Lemma 3.5.9 and the fact that $\mathcal{H} \to \mathcal{N}$ is an isomorphism of sheaves over $\mathbb{Z}[1/2n]$, we have the following proposition.

3.5.11 Proposition. *The sequence $0 \to \mathcal{H} \to \mathcal{N} \to \Phi \to 0$ of sheaves of $\mathcal{O}_{\mathrm{Spec}(\mathbb{Z}[1/2])}$-modules is exact in the Zariski topology on Spec($\mathbb{Z}[1/2]$).*

3.5.12 The automorphism group scheme of $P^{\perp}$

It is time to say more about $N = \mathrm{SO}(P^{\perp})$ and $\mathcal{N}$ over $\mathbb{Z}[1/2]$. We also let $\mathrm{End}_N(P^{\perp}_{\mathbb{Z}[1/2]})$ be the endomorphism ring of $P^{\perp}_{\mathbb{Z}[1/2]}$ as representation of N. More precisely $\mathrm{End}_N(P^{\perp}_{\mathbb{Z}[1/2]})$ is equal to

$$\{f \colon P^{\perp}_{\mathbb{Z}[1/2]} \to P^{\perp}_{\mathbb{Z}[1/2]} \colon \mathbb{Z}[1/2]\text{-linear, and for every } \mathbb{Z}[1/2]\text{-algebra } A\colon$$
$$\mathrm{id}_A \otimes f \colon A \otimes P^{\perp}_{\mathbb{Z}[1/2]} \to A \otimes P^{\perp}_{\mathbb{Z}[1/2]} \text{ commutes with the } N(A)\text{-action}\}.$$

We will show that $\mathrm{End}_N(P^{\perp}_{\mathbb{Z}[1/2]})$ is isomorphic to

$$O := \mathbb{Z}[1/2, r]/(r^2 + n).$$

In particular $\mathbb{Z}[1/2] \otimes P^{\perp}$ is an O-module. First we have the following lemma.

3.5.13 Lemma. *Locally for the étale topology on* $\mathrm{Spec}(\mathbb{Z}[1/2])$, $(P^{\perp}, b, d)$ *is isomorphic to* $\mathbb{Z}[1/2]^2$ *with the diagonal form* $(1, n)$ *with the orientation* $d' \colon \mathbb{Z}[1/2] \to \wedge^2(\mathbb{Z}[1/2]^2), 1 \mapsto e_1 \wedge e_2$.

Proof. Lemma 3.5.5 gives us some properties of $P^{\perp}$. Let M be a free $\mathbb{Z}$-module of rank 2 and b a symmetric bilinear form on M that is positive definite, primitive, and of discriminant n, and $d : \mathbb{Z} \to \wedge^2(M)$ an isomorphism of $\mathbb{Z}$-modules. We claim that there exist an integer j and étale extensions $\mathbb{Z}[1/2] \to R_i$, for $i = 1, \ldots j$, such that for each i, (M_{R_i}, b, d) is isomorphic to R_i^2 with the diagonal form $(1, n)$ and with $d : 1 \mapsto e_1 \wedge e_2$. Moreover if we write $R' := R_1 \times \cdots \times R_j$, then $\mathrm{Spec}(R') \to \mathrm{Spec}(\mathbb{Z}[1/2])$ is a surjective map and (M, b, d) locally for the étale topology on $\mathrm{Spec}(\mathbb{Z}[1/2])$ is isomorphic to $\mathbb{Z}[1/2]^2$ with the diagonal form $(1, n)$ with the orientation $d' \colon \mathbb{Z}[1/2] \to \wedge^2(\mathbb{Z}[1/2]^2), 1 \mapsto e_1 \wedge e_2$.

We prove the claim. Let g in $\mathrm{M}_2(\mathbb{Z})$ be the Gram matrix of b with respect to some $\mathbb{Z}$-basis of M, and let p be any prime number, with $p \neq 2$. We write

$$g = \begin{pmatrix} k & l \\ l & m \end{pmatrix}.$$

After some elementary operations on the basis, we may and do assume that k is a unit at p. Then over $\mathbb{Z}[1/2k, \sqrt{k}]$ we replace our basis vectors by their multiples with $1/\sqrt{k}$ and $\sqrt{k}$ respectively, and get $k = 1$ in g and still with $\det(g) = n$. Then one other elementary operation on the basis gives a Gram matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix},$$

and then we have $m = n$ because of the determinants. Moreover, because we have only done elementary operations with determinant 1, our isomorphism is compatible with the orientations on both sides. The ring $\mathbb{Z}[1/2k, \sqrt{k}]$ is finite étale over $\mathbb{Z}[1/2k]$ (meaning that $\mathbb{Z}[1/2k, \sqrt{k}]$ is a finitely generated $\mathbb{Z}[1/2k]$-module and it is étale over $\mathbb{Z}[1/2k]$), and $\mathrm{Spec}(\mathbb{Z}[1/2k])$ is an open neighborhood in $\mathrm{Spec}(\mathbb{Z}[1/2])$ of $\mathrm{Spec}(\mathbb{F}_p)$. □

So our next step is to study $(\mathbb{Z}[1/2]^2, (1, n), d')$ and its automorphism group scheme. Recall that we do not suppose that n is square free, hence O is a possibly non-maximal order. For any $\mathbb{Z}[1/2]$-algebra A, we let $O_A := A \otimes_{\mathbb{Z}[1/2]} O$. And we let T be the functor from $\mathbb{Z}[1/2]$-algebras to groups, defined by:

$$T(A) := (O_A)^\times = \left(A[r]/(r^2 + n)\right)^\times .$$

As $\mathbb{Z}[1/2]$-module, O is free with basis $(1, r)$. For A any $\mathbb{Z}[1/2]$-algebra, and a, c in A, the norm of the element $a + cr$ of O_A is $a^2 + nc^2$. The element $a + cr$ is invertible in O_A if and only if $a^2 + nc^2$ is a unit in A. So we have

$$T(A) = \{a + cr : a, c \in A \text{ and } a^2 + nc^2 \in A^\times\}.$$

We call the functor T the *Weil restriction of the multiplicative group with respect to the map* $\mathbb{Z}[1/2] \to O$. We let T_1 denote the kernel of the norm map, that is for any $\mathbb{Z}[1/2]$-algebra A,

$$T_1(A) := \{a + cr \in T(A) : a^2 + nc^2 = 1 \in A^\times\}.$$

In particular for $U = D(m)$, where $m \neq 0$, we define:

$$\mathcal{T}(U) := T(\mathcal{O}(U)) = T(\mathbb{Z}[1/m]), \quad \mathcal{T}_1(U) := T_1(\mathcal{O}(U)) = T_1(\mathbb{Z}[1/m]).$$

The presheaf $\mathcal{T}$ is a sheaf of groups, and $\mathcal{T}_1$ is a sheaf of subgroups of $\mathcal{T}$ (again by the same argument as in Section 3.2). The following lemma shows that T_1 is the automorphism group scheme of $(\mathbb{Z}[1/2]^2, (1, n), d')$.

3.5.14 Lemma. *The functor T_1 is represented by $\mathbb{Z}[1/2, x, y]/(x^2+ny^2-1)$. For every $\mathbb{Z}[1/2]$-algebra A, $T_1(A)$ is the group of those automorphisms of the A-module A^2 that preserve the diagonal form $(1, n)$ and the standard orientation $d\colon 1 \to e_1 \wedge e_2$.*

Proof. The representability is clear. We have a natural action of O_A on itself. The A-basis $(1, r)$ of O_A gives an isomorphism of A-modules $A^2 \to O_A$. For an element $g = a + cr \in T_1(A)$, it acts on A^2. In terms of matrices, we have

$$g = \begin{pmatrix} a & -nc \\ c & a \end{pmatrix}.$$

So we get an action of $T_1(A)$ and of $O_A^\times$ on A^2. We have

$$\begin{aligned} g^t \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} g &= \begin{pmatrix} a & c \\ -nc & a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \begin{pmatrix} a & -nc \\ c & a \end{pmatrix} \\ &= \begin{pmatrix} a^2+nc^2 & 0 \\ 0 & n(a^2+nc^2) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}. \end{aligned}$$

Moreover the condition $\det(g) = a^2+nc^2 = 1$ means that it is an orientation preserving matrix.

Now we need to show that for any $g \in \mathrm{M}_2(A)$ that preserves the diagonal form $(1, n)$ and the standard orientation $d\colon 1 \to e_1 \wedge e_2$ is in $T_1(A)$. Let us write

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

The orientation preserving condition is $ad - bc = 1$. Since g preserves the diagonal form $(1, n)$, we get the following identities:

$$a^2 + nc^2 = 1$$
$$ab + ncd = 0$$
$$b^2 + nd^2 = n.$$

The 2 principal opens $D(a)$ and $D(b)$ cover $\operatorname{Spec} A$, because $ad - bc = 1$. Now over $D(a)$, we write $b = -ncd/a$. We substitute it to the identity $ad - bc = 1$ on $D(a)$, and we get

$$1 = ad + (nc^2 d)/a = (a^2 + nc^2)d/a = d/a,$$

which is equivalent to $d = a$ on $D(a)$. Moreover $b = -ncd/a = -nc$ on $D(a)$. Similarly, we do the same computation on $D(b)$ to get $b = -nc$ and $a = d$ in A. □

Before we prove our main result in this section, we will show a lemma that describes the endomorphism ring of $\mathbb{Z}[1/2]^2$ as representation of T_1. Recall that $(1, r)$ gives an isomorphism of $\mathbb{Z}[1/2]$-modules $\mathbb{Z}[1/2]^2 \to O$. This makes $\mathbb{Z}[1/2]^2$ into an O-module.

3.5.15 Lemma. *The endomorphism ring of $\mathbb{Z}[1/2]^2$ as representation of T_1 is O.*

Proof. Let g be any element in the endomorphism ring of $\mathbb{Z}[1/2]^2$ as representation of T_1. Let us write

$$g = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}[1/2]).$$

Then for any $\mathbb{Z}[1/2]$-algebra A, we require that g commutes with r in the ring $O_A = A[1/2, r]/(r^2 + n)$, or equivalently

$$\begin{pmatrix} 0 & -n \\ 1 & 0 \end{pmatrix} g = g \begin{pmatrix} 0 & -n \\ 1 & 0 \end{pmatrix}.$$

Therefore we get $x = t, y = -nz$ in $\mathbb{Z}[1/2]$ or

$$g = \begin{pmatrix} x & -nz \\ z & x \end{pmatrix} = x \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + z \begin{pmatrix} 0 & -n \\ 1 & 0 \end{pmatrix}.$$

So we have proven the lemma. □

3.5.16 Proposition. *We have an isomorphism of $\mathbb{Z}[1/2]$-functors N and T_1. Moreover the ring $\mathrm{End}_N(P^{\perp}_{\mathbb{Z}[1/2]})$ is isomorphic to O.*

Proof. By Lemma 3.5.13 there exist an integer j and étale extensions R_i, $i = 1, \ldots, j$, of $\mathbb{Z}[1/2]$ such that for $R' := R_1 \times \cdots \times R_j$ the morphism $\mathrm{Spec}(R') \to \mathrm{Spec}(\mathbb{Z}[1/2])$ is surjective. By Lemma 3.5.14, T_1 is the automorphism group scheme of $(\mathbb{Z}[1/2]^2, (1, n), e_1 \wedge e_2)$. For each i, $(P^{\perp}_{R_i}, b, d)$ is isomorphic to R_i^2 with the diagonal form $(1, n)$ and $d : 1 \mapsto e_1 \wedge e_2$. Let ϕ_i be an isomorphism from $(P^{\perp}_{R_i}, b, d)$ to $(R_i^2, (1, n), e_1 \wedge e_2)$. Then each ϕ_i induces an isomorphism Φ_i^1 over R_i from $\mathrm{SO}(P^{\perp}_{R_i}) = \mathrm{SO}(P^{\perp}_{\mathbb{Z}[1/2]})_{R_i}$ to $\mathrm{Aut}(R_i^2, b, d) = T_{1,R_i}$ sending $g \mapsto \phi_i \cdot g \cdot \phi_i^{-1}$ and an isomorphism between endomorphism rings Φ_i^2 (also by conjugation). The fact that $T_1(\bar{\mathbb{Q}})$ is commutative (and the definition of the endomorphism ring of $\mathbb{Z}[1/2]^2$ as representation of T_1) implies that these Φ_i^1 (and Φ_i^2) do not depend on the choice of ϕ_i. Therefore, the $(\Phi_i)_i$ are compatible (meaning that for any $1 \leq i, k \leq j$, after base change $\mathbb{Z}[1/2] \to R_i \otimes R_k$ we have $\Phi_i^1 \otimes \mathrm{id}_{R_k} = \Phi_k^1 \otimes \mathrm{id}_{R_i}$) and the same is so for (Φ_i^2). Applying Lemma 2.10.2 for the map $\mathbb{Z}[1/2] \to R'$, we get an isomorphism ϕ from N to T_1, and an isomorphism ϕ_2 from $\mathrm{End}_N(P^{\perp}_{\mathbb{Z}[1/2]})$ to O. □

3.5.17 Determination of $\mathcal{H}$ over $\mathbb{Z}[1/2]$

On the sheaf of groups $\mathcal{T}$, we define a morphism of sheaves σ as the following: for every open subset U of $\mathrm{Spec}(\mathbb{Z}[1/2])$, and for every $a + cr \in \mathcal{T}(U)$

$$\sigma(U)\colon \mathcal{T}(U) \to \mathcal{T}(U), a + cr \mapsto a - cr.$$

We get another 2 morphisms of sheaves on $\mathcal{T}$, denoted by $1-\sigma$ and $1+\sigma$, in which for every open subset U of $\mathrm{Spec}(\mathbb{Z}[1/2])$, and for every $a+cr \in \mathcal{T}(U)$

$$(1-\sigma)(U)(a+cr) = \frac{a+cr}{a-cr}, \quad (1+\sigma)(U)(a+cr) = a^2 + nc^2.$$

Note that $1+\sigma$ is the norm map. The composed map $(1+\sigma)\circ(1-\sigma)$ is a morphism of sheaves from $\mathcal{T}$ to $\mathcal{T}$. On each open subset U of $\mathrm{Spec}(\mathbb{Z}[1/2])$, we have

$$((1+\sigma)\circ(1-\sigma))(U)(a+cr) = 1.$$

So we have the following complex of sheaf of abelian groups on $\mathrm{Spec}(\mathbb{Z}[1/2])$:

$$\mathcal{T} \xrightarrow{1-\sigma} \mathcal{T} \xrightarrow{1+\sigma} \mathcal{T}.$$

The map $(1-\sigma)$ factors through the kernel of the map $(1+\sigma)$, or equivalently the image of $(1-\sigma)$ lies in $\mathcal{T}_1$. Now if $a + uc \in \mathcal{T}(U)$ is in the kernel of the map $(1-\sigma)$, then $a + cr = a - cr$ and $c = 0$, since 2 is invertible. We get

$$\ker(1-\sigma) = (\mathcal{O}^\times_{\mathrm{Spec}(\mathbb{Z}[1/2])} \hookrightarrow \mathcal{T}, a \mapsto a + 0r).$$

In summary we have the following diagram:

$$\begin{tikzcd}
\mathcal{O}^\times_{\mathrm{Spec}(\mathbb{Z}[1/2])} \arrow[r, hook] & \mathcal{T} \arrow[r, "1-\sigma"] \arrow[dr, "1-\sigma"'] & \mathcal{T} \arrow[r, "1+\sigma"] & \mathcal{T}\ . \\
& & \mathcal{T}_1 \arrow[u, hook] &
\end{tikzcd}$$

Recall from 3.5.7, the sheaf of abelian groups Φ on $\operatorname{Spec}(\mathbb{Z}[1/2])$, for the Zariski topology, is defined by:

$$\Phi = \bigoplus_{2 \neq p | n} i_{p,*}\mathbb{F}_2.$$

We have a map of sheaves ϕ from $\mathcal{T}_1 \to \Phi$ as follows: for any prime number $p \neq 2$ that divides n, since $a^2 + nc^2 = 1$, we get $a = \pm 1$ in $\mathbb{F}_p$. We define at each stalk $\mathbb{Z}_{(p)}$, $\phi(a + cr) = 0$ in $(\mathbb{F}_2, +)$ if $a = 1$ in $\mathbb{F}_p$, and $\phi(a + cr) = 1$ in $(\mathbb{F}_2, +)$ otherwise.

Still for any prime number $p \neq 2$ dividing n, if $x + yr \in \mathcal{T}(\mathbb{Z}_{(p)})$, then we have

$$(1 - \sigma)(x + yr) = \frac{x + yr}{x - yr} = \frac{x + yr}{x - yr} \cdot \frac{x + yr}{x + yr} = \frac{x^2 - ny^2 + 2xyr}{x^2 + ny^2}.$$

The image of $(1-\sigma)(x+yr)$ in $T(\mathbb{F}_p)$ is $1 + (2y/x)r$. So we get at each stalk $\mathbb{Z}_{(p)}$, $\phi(1 - \sigma)(x + yr) = 0$ in $(\mathbb{F}_2, +)$. Thus we get a complex of sheaves of abelian groups

$$\mathcal{T} \xrightarrow{1-\sigma} \mathcal{T}_1 \xrightarrow{\phi} \Phi \to 0.$$

3.5.18 Lemma. *Let $\mathcal{T}$, $\mathcal{T}_1$, and Φ be sheaves of abelian groups in the Zariski topology on* $\operatorname{Spec}(\mathbb{Z}[1/2])$ *as above definition. Then the sequence*

$$\mathcal{T} \xrightarrow{1-\sigma} \mathcal{T}_1 \xrightarrow{\phi} \Phi \to 0$$

of sheaves of abelian groups is exact in the Zariski topology on $\operatorname{Spec}(\mathbb{Z}[1/2])$.

Proof. It is sufficient to check the image of the map $1 - \sigma$ at each stalk, that is on $\mathbb{Z}_{(p)}$, where $p \neq 2$ prime number. Let $a + cr$ be in $\mathcal{T}_1(\mathbb{Z}_{(p)})$ such that its image in $\Phi(\mathbb{Z}_{(p)})$ is 0. We want to show that there exists $x + yr \in \mathcal{T}(\mathbb{Z}_{(p)})$ such that

$$(1 - \sigma)(x + yr) = \frac{x + yr}{x - yr} = a + cr,$$

or equivalently,

$$\begin{pmatrix} 1-a & -nc \\ -c & 1+a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Suppose first that we have $p \nmid n$. Since $p \neq 2$, then either $a \neq 1 \pmod p$ or $a \neq -1 \pmod p$. In the first case, $x = nc, y = 1-a$ is a solution of the linear equation above, so

$$(1-\sigma)(nc + (1-a)r) = a + cr,$$

where $nc + (1-a)r$ is an element of $\mathcal{T}(\mathbb{Z}_{(p)})$ because its norm

$$n^2c^2 + n(1-a)^2 = n(nc^2 + 1 - 2a + a^2) = n(2-2a) = 2n(1-a)$$

is invertible in $\mathbb{Z}_{(p)}$. In the second case, $x = 1+a, y = c$ is a solution of the linear equation above, so

$$(1-\sigma)(1 + a + cr) = a + cr,$$

where again $1 + a + cr$ is an element of $\mathcal{T}(\mathbb{Z}_{(p)})$ because its norm

$$(1+a)^2 + nc^2 = 1 + 2a + a^2 + nc^2 = 2(1+a)$$

is invertible in $\mathbb{Z}_{(p)}$.

If p divides n, then from $a^2 + nc^2 = 1$ we have $a = \pm 1$ in $\mathbb{F}_p$. But as $\phi(a + cr) = 0$, then $a = 1$ in $\mathbb{F}_p$. Again $1 + a + cr$ is in $\mathcal{T}(\mathbb{Z}_{(p)})$ and it satisfies $(1-\sigma)(1 + a + cr) = a + cr$. □

Now we are ready to give the determination of the stabilizer subgroup $\mathcal{H}$ over $\mathbb{Z}[1/2]$.

3.5.19 Theorem. *Let n be a natural number such that $n \neq 0, 4, 7$ (mod 8), $\mathcal{H}$ be the stabilizer of some point $P \in \mathcal{X}_n(\mathbb{Z})$ in $\mathcal{G}$, and $\mathcal{T}$ be the Weil* *restriction of the multiplicative group with respect to the map* $\mathbb{Z}[1/2] \to O$*, all in the Zariski topology on* $\mathrm{Spec}(\mathbb{Z}[1/2])$*. Then we have an exact sequence of sheaves of abelian groups in the Zariski topology on* $\mathrm{Spec}(\mathbb{Z}[1/2])$*:*

$$0 \to \mathcal{O}^{\times}_{\mathrm{Spec}(\mathbb{Z}[1/2])} \to \mathcal{T} \to \mathcal{H} \to 0.$$

Proof. From Proposition 3.5.11 and Proposition 3.5.16, the lemma above we get the following diagram of sheaves of abelian groups over $\mathrm{Spec}(\mathbb{Z}[1/2])$:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{H} \arrow[r] & \mathcal{N} \arrow[r, "\phi'"] \arrow[d, "\Phi^1"] & \Phi \arrow[r] \arrow[d, "\mathrm{id}"] & 0 . \\
0 \arrow[r] & \mathcal{T}/\mathcal{O}^{\times} \arrow[r] & \mathcal{T}_1 \arrow[r, "\phi"] & \Phi \arrow[r] & 0
\end{tikzcd}$$

Note that the horizontal diagrams are exact sequence as Proposition 3.5.11 and the lemma above, moreover from Proposition 3.5.16 the map Φ^1 is a canonical isomorphism of sheaves of abelian groups. To prove the theorem, it is sufficient to show that the 2 composed maps, $\mathrm{id} \circ \phi'$ and $\phi \circ \Phi^1$ are equal.

Let $p \neq 2$ be any prime number dividing n. We will show that the 2 composed maps above are equal at the stalk $\mathbb{Z}_{(p)}$. From the proof of Proposition 3.5.16, there exists a surjective étale extension $\mathbb{Z}_{(p)} \to R$ such that we have an isomorphism of modules with symmetric bilinear forms $\phi_1\colon (P_R^{\perp}, b, d) \to (R^2, (1, n), d)$. This isomorphism induce a canonical isomorphism of sheaves of abelian groups $\Phi_1\colon \mathcal{N} \to \mathcal{T}_1, g \mapsto \phi_1 \circ g \circ \phi_1^{-1}$. For any $g \in \mathcal{N}(\mathbb{Z}_{(p)})$, the trace of this endomorphism of modules over the local ring $\mathbb{Z}_{(p)}$, by the definition of trace, is equal to the trace of $\Phi_1(g)$. Considering the traces (mod p), they are either 2 or -2. Following the definitions of the maps $\phi'\colon \mathcal{N} \to \Phi$ and $\phi\colon \mathcal{T}_1 \to \Phi$, we have proved our theorem. □

3.6 The group $\mathrm{H}^1(S, \mathcal{T})$ as Picard group

We will relate $\mathrm{H}^1(S, \mathcal{T}) \simeq \check{\mathrm{H}}^1(S, \mathcal{T})$ to the Picard group $\mathrm{Pic}(O)$ of the quadratic order $O := \mathbb{Z}[1/2, r]/(r^2 + n)$ in order to prove Gauss's theorem in the next section.

First we have a morphism of affine schemes $f\colon \mathrm{Spec}(O) \to \mathrm{Spec}(\mathbb{Z}[1/2])$ induced by the injection $\mathbb{Z}[1/2] \hookrightarrow O$. On $\mathrm{Spec}(\mathbb{Z}[1/2])$, we have a sheaf of abelian group $\mathcal{O}^{\times}_{\mathrm{Spec}(O)}$. Its direct image sheaf $f_*\mathcal{O}^{\times}_{\mathrm{Spec}(O)}$ is isomorphic to $\mathcal{T}$ by definition. We get

$$\check{\mathrm{H}}^1(S, \mathcal{T}) = \check{\mathrm{H}}^1(S, f_*\mathcal{O}^{\times}_{\mathrm{Spec}(O)}).$$

Therefore any element in the group is a $\mathcal{O}^{\times}_{\mathrm{Spec}(O)}$-torsor on $\mathrm{Spec}(O)$ that can be trivialised on covers that come from $\mathrm{Spec}(\mathbb{Z}[1/2])$. More precisely $\check{\mathrm{H}}^1(S, \mathcal{T})$ is the group of invertible O-modules (fractional ideals of O) M with property that for each prime number p, there exists an integer a that is relatively prime to p such that M is free of rank 1 module over $\mathbb{Z}[1/2a, r]/(r^2 + n)$. In other words, we have an injection

$$\bar{f}\colon \check{\mathrm{H}}^1(S, f_*\mathcal{O}^{\times}_{\mathrm{Spec}(O)}) \hookrightarrow \mathrm{Pic}(O).$$

The following lemma, and the fact that O is a free $\mathbb{Z}[1/2]$-module of rank 2, will show that $\bar{f}$ is a bijective map.

3.6.1 Lemma. *Let A be a noetherian ring and B be a finitely generated A-algebra that is also finitely generated as A-module. Let $T = \mathrm{Spec}(B)$ and $S = \mathrm{Spec}(A)$. The morphism $f\colon T \to S$ that is induced by $A \to B$ is finite. Suppose $\mathcal{L} = \tilde{M}$ is an invertible $\mathcal{O}_T$-module. Then for any t in T, $s := f(t)$, there exists an open subset V of T containing t such that $\mathcal{L}_{|V} \simeq \mathcal{O}_{T|V}$ and $V \supseteq f^{-1}(U)$, where U is an open subset of S that contains s.*

Proof. We will begin the proof by proving that if $m_1, ..., m_k$ are maximal ideals of B, then there exists an open subset V containing $\{m_1, ..., m_k\}$ such that $\mathcal{L}_{|V} \simeq \mathcal{O}_{T|V}$.

For each m_i, let V_i be an open subset containing it such that $\mathcal{L}_{|V_i} \simeq \mathcal{O}_{T|V_i}$. We can assume $V_i = D(f_i)$ a principal open subset, for some $f_i \in B$. Now we consider the following

$$\mathcal{L}_{m_i} \otimes_{B_{m_i}} \kappa(m_i) = (M \otimes_B B_{m_i}) \otimes_{B_{m_i}} (B_{m_i}/m_i B_{m_i}) = M \otimes_B B/m_i = M/m_i M.$$

This implies that $M/m_i M$ is 1-dimensional vector space over the residue field $\kappa(m_i)$. So there exists an element $e_i \in M$ such that $M/m_i M = e_i.B/m_i$. By the Chinese reminder theorem, we have

$$B \to \prod_{i=1}^{n} B/m_i \to 0,$$

and after tensoring by M over B, we get

$$M \to \prod_{i=1}^{n} M/m_i M \to 0,$$

and there exists e in M that maps to $(e_i)_{1 \leq i \leq n} \in \prod_{i=1}^{n} M/m_i M$. Because the image of e in $M/m_i M$ generate it over B/m_i, by a version of Nakayama's lemma (see [1], Chapter 2, Proposition 2.8.) we get $e.B_{m_i} = M_{m_i}$, or equivalently $\mathcal{L}_{m_i} = e.\mathcal{O}_{T,m_i}$. So there exist principal open subsets $D(f_i)$ containing m_i such that $\mathcal{L}_{|D(f_i)} = e.\mathcal{O}_{T|D(f_i)}$. Thus we take $V := \cup D(f_i)$ that satisfies $\mathcal{L}_{|V} = e.\mathcal{O}_{T|V}$ as desired.

Next we can change the maximal ideals m_i by prime ideals p_i in the argument, by considering that if V is an open subset containing m_i, then for any prime ideal $p_i \subset m_i$ is also contained in V. Now since f is a finite morphism, the fiber $f^{-1}(s)$ is spectrum of a finite dimensional $\kappa(s)$-vector space, in particular it is finite set in T. Thus there exists $V \supset f^{-1}(s)$ such that $\mathcal{L}_{|V} \simeq \mathcal{O}_{T|V}$. Because finite morphism implies proper morphism (see [11], Chapter II, Exercise 4.1), in particular the map f is closed, so $Z := f(T - V)$ is a closed subset of S. Moreover $s \notin Z$ which means $f^{-1}(U)$, where $U := S - Z$ is an open subset of S and s is an element of U, is contained in V. □

3.7 The proof of Gauss's theorem

Let us recall the situation of Gauss's theorem. Let n be a natural number such that $n \neq 0, 4, 7 \pmod 8$. Let $P = (x, y, z)$ be an element in $\mathcal{X}_n(\mathbb{Z})$, that exists by Legendre's theorem. By Remark 3.3.2, we have $\mathcal{X}_n(\mathbb{Z}[1/2]) = \mathcal{X}_n(\mathbb{Z})$. The sheaf of groups $\mathcal{G}$ acts naturally on $\mathcal{X}_n$. Again note that $\mathcal{G}(\mathbb{Z}[1/2]) = \mathcal{G}(\mathbb{Z})$. The action of $\mathcal{G}$ on $\mathcal{X}_n$ is transitive in the Zariski topology on $\mathrm{Spec}(\mathbb{Z}[1/2])$ (see Corollary 3.2.3). Applying Theorem 2.6.1 gives maps:

$$\mathcal{X}_n(\mathbb{Z}[1/2]) \xrightarrow{c} \mathrm{H}^1(\mathrm{Spec}(\mathbb{Z}[1/2]), \mathcal{H}) \xrightarrow{i} \mathrm{H}^1(\mathrm{Spec}(\mathbb{Z}[1/2]), \mathcal{G}),$$

that satisfy certain properties in the Theorem. Since $\mathrm{H}^1(\mathrm{Spec}(\mathbb{Z}[1/2]), \mathcal{G})$ is trivial (by Proposition 3.3.3), we get a bijection induced by the map c

$$\mathrm{SO}_3(\mathbb{Z})\backslash\mathcal{X}_n(\mathbb{Z}) = \mathrm{SO}_3(\mathbb{Z}[1/2])\backslash\mathcal{X}_n(\mathbb{Z}[1/2]) \to \mathrm{H}^1(\mathrm{Spec}(\mathbb{Z}[1/2]), \mathcal{H}).$$

We know $\mathcal{H}$ over $\mathbb{Z}[1/2]$ (by Theorem 3.5.19), that is we have the following exact sequence

$$0 \to \mathcal{O}^{\times}_{\mathrm{Spec}(\mathbb{Z}[1/2])} \to \mathcal{T} \to \mathcal{H} \to 0,$$

in the Zariski topology on $\mathrm{Spec}(\mathbb{Z}[1/2])$. Taking the long exact sequence of the cohomology groups, we get

$$0 \to \mathbb{Z}[1/2]^{\times} \to O^{\times} \to \mathcal{H}(\mathbb{Z}[1/2]) \to \mathrm{Pic}(\mathbb{Z}[1/2]) \to$$

$\to \mathrm{H}^1(\mathrm{Spec}(\mathbb{Z}[1/2]), \mathcal{T}) \to \mathrm{H}^1(\mathrm{Spec}(\mathbb{Z}[1/2]), \mathcal{H}) \to \mathrm{H}^2(\mathrm{Spec}(\mathbb{Z}[1/2]), \mathcal{O}^\times) \to \dots.$

Since $\mathbb{Z}[1/2]$ is a principal ideal domain, $\mathrm{Pic}(\mathbb{Z}[1/2])$ is a trivial group. By Grothendieck's vanishing theorem (see Theorem 2.8.7), we also get $\mathrm{H}^2(\mathrm{Spec}(\mathbb{Z}[1/2]), \mathcal{O}^\times)$ is trivial. Therefore the map above

$$\mathrm{H}^1(\mathrm{Spec}(\mathbb{Z}[1/2]), \mathcal{T}) \to \mathrm{H}^1(\mathrm{Spec}(\mathbb{Z}[1/2]), \mathcal{H})$$

is an isomorphism. Moreover from Section 3.6, we have

$$\mathrm{Pic}(O) \simeq \mathrm{H}^1(\mathrm{Spec}(\mathbb{Z}[1/2]), \mathcal{T}) \simeq \mathrm{H}^1(\mathrm{Spec}(\mathbb{Z}[1/2]), \mathcal{H}).$$

Indeed, we have proved:

$$\#\mathcal{X}_n(\mathbb{Z}) = \#\mathcal{X}_n(\mathbb{Z}[1/2]) = \frac{\#\mathcal{G}(\mathbb{Z}[1/2])}{\#\mathcal{H}(\mathbb{Z}[1/2])} \# \mathrm{Pic}\big(\mathbb{Z}[1/2, \sqrt{-n}]\big).$$

We can compute directly that $\#\mathrm{O}_3(\mathbb{Z}) = 48, \# \mathrm{SO}_3(\mathbb{Z}) = 24$ as follows:

- Over $\mathbb{Z}$, the solution of the equations $a^2 + b^2 + c^2 = 1$ are coordinate permutations of $(\pm 1, 0, 0)$.

- Because there are 3 columns in $\mathrm{O}_3(\mathbb{Z})$, then there are $3! = 6$ ways to choose the position of 1 such that any two columns are orthogonal. There are $2 \times 2 \times 2 = 8$ ways to choose the sign ± 1. Therefore $\#\mathrm{O}_3(\mathbb{Z}) = 6 \times 8 = 48$.

- For $\mathrm{SO}_3(\mathbb{Z})$, we have one more condition to satisfy that is the determinant of any element of it is equal to 1. So when we are choosing the sign of ± 1 from $2 \times 2 \times 2 = 8$ ways in $\mathrm{O}_3(\mathbb{Z})$, the determinant condition implies that the last choice is fixed, that is there are only 4 ways. Therefore we get $\# \mathrm{SO}_3(\mathbb{Z}) = 24$.

Next, let $n > 3$ and suppose that $P = (x, y, z) \in \mathcal{X}_n(\mathbb{Z})$. We want to show that the stabilizer group $\mathrm{SO}_{3,P}(\mathbb{Z}) := \mathcal{H}(\mathbb{Z}) = \mathcal{H}(\mathbb{Z}[1/2])$ is trivial group. We notice that $x = y = z$ is not possible, since $\gcd(x, y, z) = 1$. Also, it is not possible if two of the coordinates of P are equal to 0, or if one of them is zero but two of them are equal.

- Suppose $g \in \mathcal{H}(\mathbb{Z})$ is not equal to the identity matrix. Assume that it fixes one of the coordinate of P, wlog it fixes z. Then we should have either $(x, y) \mapsto (y, -x)$ or $(x, y) \mapsto (-y, x)$. In both cases, we get $x = y = -x$ or $x = y = 0$ which is not possible.

- Now suppose if $g \in \mathcal{H}(\mathbb{Z})$ maps one of the coordinates of P to its minus, wlog $z \mapsto -z$. In this case $z = 0$ and the possibilities of the maps will be $(x, y) \mapsto (-x, y)$, $(x, y) \mapsto (x, -y)$, $(x, y) \mapsto (y, x)$ or $(x, y) \mapsto (-y, -x)$. From each of the cases, again by the discussion above, it is not possible.

- The last cases will be $g \in \mathcal{H}(\mathbb{Z})$ is a 3-cycle such as
$$g\colon (x, y, z) \mapsto (\pm y, \pm z, \pm x).$$
Again, it implies the $\gcd(x, y, z) > 1$.

The conclusion is that if $n > 3$, then $\mathcal{H}(\mathbb{Z})$ is trivial. For $n = 1$, $\mathcal{H}(\mathbb{Z})$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. For $n = 2$, $\mathcal{H}(\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$ and for $n = 3$, $\mathcal{H}(\mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z}$.

Recall that we defined the ring $O := \mathbb{Z}[1/2, r]/(r^2 + n)$. If n is $1, 2, 5, 6 \pmod 8$ then let $d = -4n$ and $O = O_d[1/2]$, while if n is $3 \pmod 8$ then let $d = -n$ and $O = O_d[1/2]$ and we have a map $\mathrm{Pic}(O_d) \to \mathrm{Pic}(O)$. For $n = 1$ and $n = 2$, the rings $\mathbb{Z}[i] = O_{-4}$ and $\mathbb{Z}[\sqrt{-2}] = O_{-8}$ are PID, so $\mathrm{Pic}(O) = \mathrm{Pic}(O_d)$ because both are trivial. By combining the fact that $O_d^\times$ has order 4 and 2 consecutively for $n = 1$ and $n = 2$, we get Gauss's theorem. When $n = 3$, we have 2 is inert in O_d, so $\mathrm{Pic}(O) = \mathrm{Pic}(O_d)$. The unit group O_d has order 6, so again we get Gauss's theorem.

Suppose now that $n > 3$. The ring O_d need not be integrally closed, so we have to be careful when describing $\mathrm{Pic}(O_d)$ and $\mathrm{Pic}(O_d[1/2])$ in terms of divisors and principal divisors. We note that O_d is integrally closed at 2 because n is not divisible by 4, and that 2 is ramified in O_d if $n = 1, 2, 5, 6 \pmod 8$ and inert if $n = 3 \pmod 8$. So in all cases O_d has a unique maximal ideal m_2 containing 2. This ideal m_2 is invertible and its class in $\mathrm{Pic}(O_d)$ has order 2 if 2 is ramified in O_d (there are no elements of norm 2 in O_d, and $m_2^2 = (2)$), and order 1 if 2 is inert in O_d (then $m_2 = (2)$). We claim that the map $\mathrm{Pic}(O_d) \to \mathrm{Pic}(O_d[1/2])$ is surjective and that its kernel is the subgroup generated by m_2. To see this, we note that every locally free $O_d[1/2]$-module L of rank one has an element l that generates it at the finitely many maximal ideals m_i of O_d that are not invertible: let I be the product of the m_i, and let l be a lift of a generator of L/IL. Then L is isomorphic to the locally free $O_d[1/2]$ module given by the divisor D of l. If $l' \in L$ also generates L at the m_i then $l' = u{\cdot}l$ with u in $\mathbb{Q}(\sqrt{-n})^\times$ such that u and u^{-1} are regular at the m_i. Hence $\mathrm{Pic}(O_d[1/2])$ is the group of Weil divisors of O_d with support outside the m_i, modulo divisors of elements of $\mathbb{Q}(\sqrt{-n})^\times$ whose divisor have support outside the m_i. The extensions of L to a locally free O_d-module then correspond to the divisors $D + a{\cdot}m_2$ with $a \in \mathbb{Z}$.

So for $n > 3$ and the fact that 2 is inert or ramified in O_d for $d = -n$ or $d = -4n$ respectively implies that $\#\,\mathrm{Pic}(O) = \#\,\mathrm{Pic}(O_d)$ for $d = -n$ while $\#\,\mathrm{Pic}(O) = \#\,\mathrm{Pic}(O_d)/2$ for $d = -4n$. We have also Gauss's theorem, since $O_d^\times \simeq \mathbb{Z}/2\mathbb{Z}$. So we have proved that the right hand side of the following formula

$$\begin{aligned}\#\mathcal{X}_n(\mathbb{Z}) = \#\mathcal{X}_n(\mathbb{Z}[1/2]) &= \frac{\#\mathcal{G}(\mathbb{Z}[1/2])}{\#\mathcal{H}(\mathbb{Z}[1/2])}\#\operatorname{Pic}(\mathbb{Z}[1/2, \sqrt{-n}]) \\ &= \frac{\#\mathcal{G}(\mathbb{Z}[1/2])}{\#\mathcal{H}(\mathbb{Z}[1/2])}\#\operatorname{Pic}(O)\end{aligned}$$

is equal to the right hand side of Gauss's theorem 3.1.1.

Chapter 4

Gauss composition on the 2-sphere

4.1 The general situation

Let S be a topological space, $\mathcal{X}$ a sheaf of sets on S, and $\mathcal{G}$ a sheaf of groups on S acting transitively from the left on $\mathcal{X}$. Suppose $\mathcal{X}(S) \neq \emptyset$. For $x \in \mathcal{X}(S)$, we assume that the stabilizer $\mathcal{H} := \mathcal{G}_x$ of x in $\mathcal{G}$ is commutative. From Theorem 2.6.1, then for all y in $\mathcal{X}(S)$, $\mathcal{G}_y$ is canonically isomorphic to $\mathcal{H}$. Moreover we have an "exact" sequence

$$\begin{tikzcd}
\mathcal{H}(S) \arrow[r, hook] & \mathcal{G}(S) \arrow[r] & \mathcal{X}(S) \arrow[r, "c"] & \mathrm{H}^1(S,\mathcal{H}) \arrow[r, "i"] & \mathrm{H}^1(S,\mathcal{G}) \\
 & g \arrow[r, mapsto] & g\cdot x & \mathcal{T} \arrow[r, mapsto] & \mathcal{T}\otimes_{\mathcal{G}_x}\mathcal{G} \\
 & & y \arrow[r, mapsto] & {[{}_y\mathcal{G}_x],} &
\end{tikzcd}$$

where $[{}_y\mathcal{G}_x]$ is the isomorphism class of ${}_y\mathcal{G}_x$. This induces a bijection

$$\mathcal{G}(S) \setminus \mathcal{X}(S) \longrightarrow \ker \left(\mathrm{H}^1(S,\mathcal{H}) \to \mathrm{H}^1(S,\mathcal{G})\right).$$

We assume $\mathrm{H}^1(S,\mathcal{G}) = \{1\}$. Then $\mathcal{G}(S) \setminus \mathcal{X}(S) \xrightarrow{\sim} \mathrm{H}^1(S,\mathcal{H})$. This bijection gives an action of $\mathrm{H}^1(S,\mathcal{H})$ on $\mathcal{G}(S) \setminus \mathcal{X}(S)$ as follows: for $y \in \mathcal{X}(S)$ and $\mathcal{T}$ an $\mathcal{H}$-torsor, there exists $z \in \mathcal{X}(S)$ such that $[{}_y\mathcal{G}_x \otimes_{\mathcal{H}} \mathcal{T}] = [{}_z\mathcal{G}_x]$ and we get the following diagram

$$\begin{tikzcd}
\bar{y} \arrow[r, mapsto] & {[{}_y\mathcal{G}_x]} \arrow[d, mapsto, "\cdot\mathcal{T}"] & . \\
\bar{z} & {[{}_y\mathcal{G}_x \otimes_{\mathcal{H}} \mathcal{T}] = [{}_z\mathcal{G}_x]} \arrow[l, mapsto] &
\end{tikzcd}$$

Moreover we have

$$\bar{y} \overset{[\mathcal{T}]}{\longmapsto} \bar{z} \Leftrightarrow [{}_y\mathcal{G}_x \otimes_{\mathcal{H}} \mathcal{T}] = [{}_z\mathcal{G}_x] \Leftrightarrow [\mathcal{T}] = [{}_z\mathcal{G}_x \otimes_{\mathcal{H}} {}_x\mathcal{G}_y] \Leftrightarrow [\mathcal{T}] = [{}_z\mathcal{G}_y].$$

Here we use Lemma 2.6.2 to have an isomorphism of sheaves (even bitorsors) between ${}_z\mathcal{G}_x \otimes_{\mathcal{H}} {}_x\mathcal{G}_y$ and ${}_z\mathcal{G}_y$. The last equivalence shows that this action does not depend on x.

Now we can explain what we mean by “Gauss composition” in this situation. For x, y, x' in $\mathcal{X}(S)$, there exists a unique $\bar{y}' \in \mathcal{G}(S) \setminus \mathcal{X}(S)$ such that $[{}_y\mathcal{G}_x] = [{}_{y'}\mathcal{G}_{x'}]$. This is a “parallelogram law” in $\mathcal{G}(S) \setminus \mathcal{X}(S)$:

$$\begin{tikzcd}
 & \bar{y'} \ . \\
\bar{x'} \arrow[ur, mapsto, "{[{}_y\mathcal{G}_x]}"] & \bar{y} \arrow[u, mapsto] \\
\bar{x} \arrow[u, mapsto] \arrow[ur, mapsto, "{[{}_y\mathcal{G}_x]}"'] &
\end{tikzcd}$$

4.1.1 A more direct description

Assumptions as above, let x, y, x' are in $\mathcal{X}(S)$. Let $\mathcal{T} := {}_y\mathcal{G}_x$ and view it as a $\mathcal{G}_{x'}$-torsor via the natural isomorphism ${}_{x'}\phi_x\colon \mathcal{G}_x \to \mathcal{G}_{x'}$. Note that the inclusion $\mathcal{T} = {}_y\mathcal{G}_x \hookrightarrow \mathcal{G}$ is not necessarily $\mathcal{G}_{x'}$-equivariant for $\mathcal{G}_{x'} \subset \mathcal{G}$ the inclusion (it is equivariant for $\mathcal{G}_{x'} = \mathcal{G}_x \subset \mathcal{G}$).

We have a map $i\colon \mathcal{T} \to \mathcal{T} \times \mathcal{G}$ as follows: for every open $U \subset S$, and $t \in \mathcal{T}(U)$, $\mathcal{T}(U) \to (\mathcal{T}\times\mathcal{G})(U)\colon t \mapsto (t, e)$, where e is the identity element in $\mathcal{G}(U)$. We define a map $\bar{i} := q \circ i\colon \mathcal{T} \to \mathcal{T} \otimes_{\mathcal{G}_{x'}} \mathcal{G}$, with $q\colon \mathcal{T}\times\mathcal{G} \to \mathcal{T} \otimes_{\mathcal{G}_{x'}} \mathcal{G}$ the quotient map. By the assumption that $\mathrm{H}^1(S, \mathcal{G}) = \{1\}$, there exists $\alpha\colon \mathcal{T} \otimes_{\mathcal{G}_{x'}} \mathcal{G} \to \mathcal{G}$ an isomorphism to the trivial $\mathcal{G}$-torsor. So we get a $\mathcal{G}_{x'} \subset \mathcal{G}$ equivariant embedding $\bar{\alpha} := \alpha \circ \bar{i}\colon \mathcal{T} \hookrightarrow \mathcal{G}$, as in the following diagram

$$\begin{tikzcd}
\mathcal{T} \arrow[r, hook, "\bar{i}"] \arrow[d] & \mathcal{T} \otimes_{\mathcal{G}_{x'}} \mathcal{G} \arrow[d, "\alpha"'] \\
\mathcal{T} \times \mathcal{G} \arrow[ur, "q"] & \mathcal{G}.
\end{tikzcd}$$

This α is unique up to $\alpha' = (\text{automorphism of trivial } \mathcal{G}\text{-torsor}) \circ \alpha$, that is, up to left multiplication by $\mathcal{G}(S)$. We define y' in $\mathcal{X}(S)$ by $y' = (\bar{\alpha}(t)) \cdot x'$ for any $t \in \mathcal{T}(\mathbb{Q})$; this is indeed independent the choice of t. Because of the choice of α, y' is unique up to $\mathcal{G}(S)$.

4.2 Gauss composition: the case of the 2-sphere

We refer the reader to see Section 3.2, Section 3.3, and Section 3.7. We will take a special case (related to Gauss's sum of 3 squares theorem) of the above discussion. Let n be a natural number such that $n \neq 0, 4, 7 \pmod 8$. Let S be $\mathrm{Spec}(\mathbb{Z})$ with its Zariski topology, $\mathcal{X}$ be the sheaf of sets $\mathcal{X}_n$, and

$\mathcal{G}$ be the sheaf of groups $\mathcal{G}$ induced by SO_3. As in the Section 3.3, SO_3 is the automorphism group scheme of $(\mathbb{Z}^3, b, d)$, where $b\colon \mathbb{Z}^3 \times \mathbb{Z}^3 \to \mathbb{Z}$ is the standard inner product and $d\colon \mathbb{Z} \to \wedge^3\mathbb{Z}^3$ is the standard trivialisation of the determinant.

Let x, y, x' be in $\mathcal{X}(S)$ and $\mathcal{T} := {}_y\mathcal{G}_x$ the transporter from x to y. This is a $\mathcal{G}_x$-torsor but we see it as a $\mathcal{G}_{x'}$-torsor via ${}_{x'}\phi_x\colon \mathcal{G}_x \to \mathcal{G}_{x'}$. As explained in Section 4.1.1, trivialising the right $\mathcal{G}$-torsor $\mathcal{T} \otimes_{\mathcal{G}_{x'}} \mathcal{G}$ is the main step in finding y'. First we show that trivialising $\mathcal{T} \otimes_{\mathcal{G}_{x'}} \mathcal{G}$ is the same as finding an isomorphism of triples (M, b, d) between

$$\mathcal{T} \otimes_{\mathcal{G}_{x'}} (\mathbb{Z}^3, b, d) \text{ and } (\mathbb{Z}^3, b, d).$$

Observe that

$$\mathcal{T} \otimes_{\mathcal{G}_{x'}} (\mathbb{Z}^3, b, d) = (\mathcal{T} \otimes_{\mathcal{G}_{x'}} \mathcal{G}) \otimes_{\mathcal{G}} (\mathbb{Z}^3, b, d)$$

is the twist of $(\mathbb{Z}^3, b, d)$ by the right $\mathcal{G}$-torsor $(\mathcal{T} \otimes_{\mathcal{G}_{x'}} \mathcal{G})$. As in Lemma 2.5.4 we have an isomorphism of $\mathcal{G}$-torsors

$$\mathcal{T} \otimes_{\mathcal{G}_{x'}} \mathcal{G} \to \mathbf{Isom}_S((\mathbb{Z}^3, b, d), (\mathcal{T} \otimes_{\mathcal{G}_{x'}} \mathcal{G}) \otimes_{\mathcal{G}} (\mathbb{Z}^3, b, d))$$

which shows that trivialising the right $\mathcal{G}$-torsor $\mathcal{T} \otimes_{\mathcal{G}_{x'}} \mathcal{G}$ is the same as finding an isomorphism between $(\mathbb{Z}^3, b, d)$ and its twist.

So now the main point is: how to describe the lattice $\mathcal{T} \otimes_{\mathcal{G}_{x'}} (\mathbb{Z}^3, b, d)$ explicitly. We do it in 2 steps: first relate ${}_y\mathcal{G}_x$ to a subsheaf of the constant sheaf $\mathcal{G}_x(\mathbb{Q})_S$, and then use the canonical isomorphism between $\mathcal{G}_x$ with $\mathcal{G}_{x'}$ to see ${}_y\mathcal{G}_x$ as a $\mathcal{G}_{x'}$-torsor.

4.2.1 Description in terms of lattices in $\mathbb{Q}^3$

We choose an element $t \in \mathcal{G}_{x,y}(\mathbb{Q})$, this gives a bijection

$${}_y\mathcal{G}_x(\mathbb{Q}) \xrightarrow{\sim} \mathcal{G}_x(\mathbb{Q}), \quad s \mapsto t^{-1}s.$$

Note this is right $\mathcal{G}_x(\mathbb{Q})$-equivariant.

For $U \subset S$ non-empty open, we have ${}_y\mathcal{G}_x(U) \hookrightarrow {}_y\mathcal{G}_x(\mathbb{Q}), \mathcal{G}(U) \hookrightarrow \mathcal{G}(\mathbb{Q})$, etc. where $\mathcal{G}(\mathbb{Q}) = \mathcal{G}_\eta$, the stalk at the generic point. In sheaf language:

$$\mathcal{G} \subset i_{\eta,*}\mathcal{G}_\eta,$$

with $i_\eta \colon \{\eta\} \hookrightarrow S$ the inclusion. So $\mathcal{G}$ is a subsheaf of the constant sheaf $i_{\eta,*}\mathcal{G}_\eta = \mathcal{G}(\mathbb{Q})_S$.

4.2.2 Lemma. *Let $\mathcal{F}$ be either $\mathcal{G}$, ${}_y\mathcal{G}_x$, etc. Then for any $m \neq 0$, we have*

$$\mathcal{F}(\mathbb{Z}[1/m]) = \mathcal{F}(\mathbb{Q}) \cap \mathrm{GL}_3(\mathbb{Z}[1/m]) \quad \textit{in } \mathrm{GL}_3(\mathbb{Q}).$$

Proof. Let m be a non-zero integer. It is sufficient to show that

$$\mathrm{GL}_3(\mathbb{Z}[1/m]) = \{g \in \mathrm{GL}_3(\mathbb{Q}) \colon g \cdot \mathbb{Z}[1/m]^3 = \mathbb{Z}[1/m]^3 \text{ inside } \mathbb{Q}^3\}.$$

If $g \in \{g \in \mathrm{GL}_3(\mathbb{Q}) \colon g \cdot \mathbb{Z}[1/m]^3 = \mathbb{Z}[1/m]^3 \text{ inside } \mathbb{Q}^3\}$, then by considering the images of $(1,0,0)$, $(0,1,0)$, and $(0,0,1)$ by g and by g^{-1}, we get that $g \in \mathrm{GL}_3(\mathbb{Z}[1/m])$. On the other hand, if $g \in \mathrm{GL}_3(\mathbb{Z}[1/m])$, then $g \cdot \mathbb{Z}[1/m]^3 \subset \mathbb{Z}[1/m]^3$. But we have also that $g^{-1} \in \mathrm{GL}_3(\mathbb{Z}[1/m])$, so

$$\mathbb{Z}[1/m]^3 = g^{-1}g \cdot \mathbb{Z}[1/m]^3 \subset g^{-1}\mathbb{Z}[1/m]^3 \subset \mathbb{Z}[1/m]^3.$$

Thus we get an equality $g \cdot \mathbb{Z}[1/m]^3 = \mathbb{Z}[1/m]^3$ inside $\mathbb{Q}^3$. This implies that g is an element of $\mathrm{GL}_3(\mathbb{Q})$ such that $g \cdot \mathbb{Z}[1/m]^3 = \mathbb{Z}[1/m]^3$ inside $\mathbb{Q}^3$. □

Our claim is that $t^{-1}{}_y\mathcal{G}_x \subset \mathcal{G}_x(\mathbb{Q})_S$ is the subsheaf sending the lattice $\mathbb{Z}^3$ to $t^{-1}\mathbb{Z}^3$. We will show it in the following lemma.

4.2.3 Lemma. *For every $m \geq 1$, with $U = \mathrm{Spec}(\mathbb{Z}[1/m])$, we have*

$$t^{-1}{}_y\mathcal{G}_x(\mathbb{Z}[1/m]) = \{g \in \mathcal{G}_x(\mathbb{Q}) \colon g \cdot \mathbb{Z}[1/m]^3 = t^{-1}\mathbb{Z}[1/m]^3 \textit{ inside } \mathbb{Q}^3\}.$$

Proof. To show it, let $s \in \mathcal{G}_{x,y}(\mathbb{Q})$. Then by previous lemma, we have

$$s \in \mathcal{G}_{x,y}(\mathbb{Z}[1/m]) \iff s\mathbb{Z}[1/m]^3 = \mathbb{Z}[1/m]^3 \iff t^{-1}s\mathbb{Z}[1/m]^3 = t^{-1}\mathbb{Z}[1/m]^3.$$

□

In other words: we have "encoded" ${}_y\mathcal{G}_x$ in terms of t and the pair of lattices $\mathbb{Z}^3$ and $t^{-1}\mathbb{Z}^3$, both containing x, both perfect for b the standard inner product, and for d a trivialisation of determinant. We denote it as

$$t^{-1}{}_y\mathcal{G}_x = {}_{t^{-1}\mathbb{Z}^3}\mathcal{G}_x(\mathbb{Q})_{\mathbb{Z}^3}.$$

We realise ${}_y\mathcal{G}_x$ as $\mathcal{G}_{x'}$-torsor, but we need some new object that we denote: ${}_{x'}\mathcal{G}_x t^{-1}\mathbb{Z}^3$. We define it as a sheaf on S, induced by some sublattice in $\mathbb{Q}^3$. The notation makes sense: for any $m \geq 1$, $g_1, g_2 \in {}_{x'}\mathcal{G}_x(\mathbb{Z}[1/m])$, there exists $h \in \mathcal{G}_x(\mathbb{Z}[1/m])$ such that $g_2 = g_1 h$, and since $tht^{-1} \in \mathcal{G}_y(\mathbb{Z}[1/m])$, we have $tht^{-1}\mathbb{Z}[1/m]^3 = \mathbb{Z}[1/m]^3$, or equivalently we get

$$g_1 t^{-1}\mathbb{Z}[1/m]^3 = g_1 h t^{-1}\mathbb{Z}[1/m]^3 = g_2 t^{-1}\mathbb{Z}[1/m]^3.$$

The set of global sections of ${}_{x'}\mathcal{G}_x t^{-1}\mathbb{Z}^3$ is a lattice. It can be recovered from the intersection of all ${}_{x'}\mathcal{G}_x(\mathbb{Z}_{(p)})t^{-1}\mathbb{Z}^3_{(p)}$, where p is running through all prime numbers.

So we have $\mathbb{Z}^3$ and $t^{-1}\mathbb{Z}^3$, both containing x, perfect for b and d. Let us denote

$$L := (\mathbb{Z}^3, b, d) \quad \text{and} \quad M := ({}_{x'}\mathcal{G}_x t^{-1}\mathbb{Z}^3, b, d). \tag{4.1}$$

Now we have also L and M, both containing x', and both perfect for b and d.

4.2.4 Proposition. *Let L and M be as in (4.1). Then ${}_y\mathcal{G}_x$ as $\mathcal{G}_{x'}$-torsor is isomorphic to ${}_M\mathcal{G}_{x'}(\mathbb{Q})_L$.*

Proof. Inside $\mathcal{G}(\mathbb{Q})_S$, we have an isomorphism

$$t^{-1}\cdot \colon {}_y\mathcal{G}_x \xrightarrow{\sim} t^{-1}{}_y\mathcal{G}_x.$$

Lemma 4.2.3 gives us the following identity $t^{-1}{}_y\mathcal{G}_x = {}_{t^{-1}L}\mathcal{G}_x(\mathbb{Q})_L$. We have the canonical isomorphism ${}_{x'}\phi_x \colon \mathcal{G}_x \to \mathcal{G}_{x'}, h \mapsto shs^{-1}$ given by any $s \in {}_{x'}\mathcal{G}_x(\mathbb{Q})$. It induces an isomorphism ${}_{x'}\phi_x \colon \mathcal{G}_x(\mathbb{Q})_S \xrightarrow{\sim} \mathcal{G}_{x'}(\mathbb{Q})_S$. So we have the following diagram:

$$\begin{tikzcd}
\mathcal{G}_x(\mathbb{Q})_S \arrow[r, "\sim"] & \mathcal{G}_{x'}(\mathbb{Q})_S \\
{}_{t^{-1}L}\mathcal{G}_x(\mathbb{Q})_L \arrow[u, hook] & {}_M\mathcal{G}_{x'}(\mathbb{Q})_L \arrow[u, hook]
\end{tikzcd}$$

To prove the proposition, it is sufficient to show that

$$ {}_{x'}\phi_x({}_{t^{-1}L}\mathcal{G}_x(\mathbb{Q})_L) = {}_M\mathcal{G}_{x'}(\mathbb{Q})_L. \tag{4.2}$$

At every prime number p, we have $M_{(p)} = {}_{x'}\mathcal{G}_x(\mathbb{Z}_{(p)})t^{-1}\mathbb{Z}^3_{(p)}$. In particular for any $s \in {}_{x'}\mathcal{G}_x(\mathbb{Z}_{(p)})$, we also have $M_{(p)} = st^{-1}L_{(p)}$. Thus we get, for any $s \in {}_{x'}\mathcal{G}_x(\mathbb{Z}_{(p)})$,

$$\begin{aligned}
{}_{x'}\phi_x({}_{t^{-1}L}\mathcal{G}_x(\mathbb{Q})_L)_{(p)} &= {}_{x'}\phi_x({}_{t^{-1}L_{(p)}}\mathcal{G}_x(\mathbb{Q})_{L_{(p)}}) \\
&= s\cdot({}_{t^{-1}L_{(p)}}\mathcal{G}_x(\mathbb{Q})_{L_{(p)}})\cdot s^{-1} = {}_{M_{(p)}}\mathcal{G}_{x'}(\mathbb{Q})_{sL_{(p)}}.
\end{aligned}$$

As $sL_{(p)} = L_{(p)}$, we get an isomorphism $({}_{x'}\phi_x \circ (t^{-1}\cdot)) \colon {}_y\mathcal{G}_x \to {}_M\mathcal{G}_{x'}(\mathbb{Q})_L$ as desired. □

Now we are ready to give an explicit description of ${}_y\mathcal{G}_x \otimes_{\mathcal{G}_{x'}} L$ as a sublattice of $\mathbb{Q}^3$ which turns out to be M. We have the following sequence of isomorphisms:

$$\begin{aligned}
{}_y\mathcal{G}_x \otimes_{\mathcal{G}_{x'}} L \longrightarrow & t^{-1}{}_y\mathcal{G}_x \otimes_{\mathcal{G}_{x'}} L = {}_{t^{-1}L}\mathcal{G}_x(\mathbb{Q})_L \otimes_{{}_L\mathcal{G}_{x'}(\mathbb{Q})_L} L \longrightarrow \\
& {}_M\mathcal{G}_{x'}(\mathbb{Q})_L \otimes_{{}_L\mathcal{G}_{x'}(\mathbb{Q})_L} L \longrightarrow M \subset \mathbb{Q}^3,
\end{aligned} \tag{4.3}$$

where the first arrow is $t^{-1}\cdot \otimes \mathrm{id}$, the second arrow is ${}_{x'}\phi_x \otimes \mathrm{id}$ (we are using (4.2)), and third arrow is given by the map $(g, v) \mapsto gv$.

Suppose we have an isomorphism of triples (M, b, d), $\phi\colon M \xrightarrow{\sim} L$. It is an element of $\mathcal{G}(\mathbb{Q})$. Then it induces a $\mathcal{G}_{x'}$-equivariant embedding ${}_y\mathcal{G}_x$ in $\mathcal{G}$ as $\mathcal{G}_{x'}$-torsor as follows

$$\bar{i}\colon {}_M\mathcal{G}_{x'}(\mathbb{Q})_L \to {}_L\mathcal{G}(\mathbb{Q})_L = \mathcal{G}, \quad g \mapsto \phi \circ g. \tag{4.4}$$

For any $g \in {}_M\mathcal{G}_{x'}(\mathbb{Q})_L(\mathbb{Q})$, we get

$$y' = (\bar{i}(g))(x'). \tag{4.5}$$

4.2.5 Summary of the method

Let n be a natural number such that $n \neq 0, 4, 7 \pmod 8$ and let S be $\mathrm{Spec}(\mathbb{Z})$ with its Zariski topology. Let $\mathcal{X}$ be the sheaf of sets $\mathcal{X}_n$, and $\mathcal{G}$ be the sheaf of groups $\mathcal{G}$ induced by SO_3 as before. Let also x, y, x' be in $\mathcal{X}(S)$. We want to find the unique $\bar{y}' \in \mathcal{G}(S) \setminus \mathcal{X}(S)$ such that $[{}_y\mathcal{G}_x] = [{}_{y'}\mathcal{G}_{x'}]$.

We have that ${}_y\mathcal{G}_x \subset \mathcal{G}$ is a right $\mathcal{G}_x$-torsor, and we want to view it as $\mathcal{G}_{x'}$-torsor. It is not (necessarily) embedded equivariantly in $\mathcal{G}$ for the inclusion $\mathcal{G}_{x'} \subset \mathcal{G}$. But:

$${}_y\mathcal{G}_x \hookrightarrow {}_y\mathcal{G}_x \otimes_{\mathcal{G}_{x'}} \mathcal{G} \xrightarrow{\sim} \mathcal{G}$$

is an equivariant map for the inclusion $\mathcal{G}_{x'} \subset \mathcal{G}$. So any trivialisation of ${}_y\mathcal{G}_x \otimes_{\mathcal{G}_{x'}} \mathcal{G}$ as right $\mathcal{G}$-torsor embeds ${}_y\mathcal{G}_x$ in $\mathcal{G}$ as $\mathcal{G}_{x'}$-torsor. Let $\bar{i}\colon {}_y\mathcal{G}_x \to \mathcal{G}$ be such an embedding, then $y' := (\bar{i}g) \cdot x'$ for any $g \in {}_y\mathcal{G}_x(\mathbb{Q})$.

Now in terms of lattices. Let $L := \mathbb{Z}^3$ be the standard lattice with the standard inner product form b and a trivialisation of the determinant d. Let

t be an element of ${}_y\mathcal{G}_x(\mathbb{Q})$. Then ${}_y\mathcal{G}_x(\mathbb{Q}) \xrightarrow{\sim} \mathcal{G}_x(\mathbb{Q}), g \mapsto t^{-1}g$. This gives

$$\begin{tikzcd}
{}_y\mathcal{G}_x \arrow[r, hook] \arrow[dr, "\sim"'] & \mathcal{G}_x(\mathbb{Q})_S \\
 & {}_{t^{-1}L}\mathcal{G}_x(\mathbb{Q})_L \arrow[u, hook]
\end{tikzcd}$$

Let $M := {}_{x'}\mathcal{G}_x t^{-1}\mathbb{Z}^3$. Note that ${}_{x'}\mathcal{G}_x L = L$. Then from Proposition 4.2.4, ${}_y\mathcal{G}_x$ as $\mathcal{G}_{x'}$-torsor is ${}_M\mathcal{G}_{x'}(\mathbb{Q})_L$. Moreover ${}_y\mathcal{G}_x \otimes_{\mathcal{G}_{x'}} L$ is equal to M inside $\mathbb{Q}^3$ (4.3). Suppose $\phi\colon M \xrightarrow{\sim} L$ is an element of $\mathcal{G}(\mathbb{Q})$. Then it induces a $\mathcal{G}_{x'}$-equivariant embedding ${}_y\mathcal{G}_x$ in $\mathcal{G}$ as $\mathcal{G}_{x'}$-torsor

$$\bar{i}\colon {}_M\mathcal{G}_{x'}(\mathbb{Q})_L \to {}_L\mathcal{G}(\mathbb{Q})_L = \mathcal{G}, \quad g \mapsto \phi \circ g.$$

Thus for any $g \in {}_M\mathcal{G}_{x'}(\mathbb{Q})_L(\mathbb{Q})$, we get $y' = (\bar{i}(g))(x')$.

4.3 Finding an orthonormal basis for M explicitly

In this section, we keep the same notation as in the previous section. The main concern of this section is, given the natural number n, 3 elements $x, y, x' \in \mathcal{X}_n(\mathbb{Z})$, and some element $t \in {}_y\mathcal{G}_x(\mathbb{Q})$, to find explicitly an orthonormal basis for $M = {}_{x'}\mathcal{G}_x t^{-1}\mathbb{Z}^3$. Note that it is a perfect lattice for b and d that contains x'.

For any element g in $\mathrm{SO}_3(\mathbb{Q})$, we denote $d(g) := \mathrm{denom}(g)$, the lcm of the denominators of $g_{ij} \in \mathbb{Q}$. First is the following lemma.

4.3.1 Lemma. *There exists $s \in {}_{x'}\mathcal{G}_x(\mathbb{Q})$ such that $d(s) := \mathrm{denom}(s)$ is coprime with n and $d(t)$.*

Proof. The main ingredient for the proof of this lemma is the proof of Theorem 3.2.2 and the Chinese remainder theorem. As in the proof of Theorem 3.2.2, for each prime $p \neq 2$ that divides $nd(t)$, there exists a vector $v_p \in \mathbb{F}_p^3$ such that $\langle v_p, v_p \rangle$ and $\langle s_{v_p}(x) - x', s_{v_p}(x) - x' \rangle$ are both non-zero in $\mathbb{F}_p$. By applying the Chinese remainder theorem to each coordinate of v_p, there exists $v \in \mathbb{Z}^3$ such that for each p that divides $nd(t)$, v is equal to v_p in $\mathbb{F}_p^3$. We set $w := s_v(x) - x'$ and we get $s := s_w \circ s_v$. □

Now let us choose s as in Lemma 4.3.1. Thus we get

$$M[1/d(s)] = st^{-1}\mathbb{Z}[1/d(s)]^3 \text{ inside } \mathbb{Q}^3, \tag{4.6}$$

and also for every prime number p dividing $d(s)$, there exists $s_p \in {}_{x'}\mathcal{G}_x(\mathbb{Z}_{(p)})$ such that

$$M_{(p)} = s_p t^{-1}\mathbb{Z}_{(p)}^3 \text{ inside } \mathbb{Q}^3. \tag{4.7}$$

For each p dividing $d(s)$, we choose such an s_p. Let $h_p := ss_p^{-1} \in \mathcal{G}_{x'}(\mathbb{Q})$. Note that s_p is an orthogonal matrix with coefficients in $\mathbb{Z}_{(p)}$, its inverse is its transpose, and in particular we get that the valuation $v_p(h_p) = v_p(s)$ (see again Section 3.4 for the definition of the valuation of matrices). Thus we have $d(s)h_p \in \mathrm{M}_3(\mathbb{Z}_{(p)})$.

4.3.2 Lemma. *We have the following inclusions inside* $\mathbb{Q}^3$*:*

$$d(s)st^{-1}\mathbb{Z}^3 \subset M \subset \frac{1}{d(s)}st^{-1}\mathbb{Z}^3.$$

Proof. Since $d(t)$ and $d(s)$ are coprime, we have $M_{(p)} = \mathbb{Z}_{(p)}$ for all p dividing $d(s)$. Moreover we have the following inclusion inside $\mathbb{Q}^3$:

$$d(s)st^{-1}\mathbb{Z}_{(p)}^3 = d(s)h_p(s_pt^{-1}\mathbb{Z}_{(p)}^3) = d(s)h_p\mathbb{Z}_{(p)}^3 \subset \mathbb{Z}_{(p)}^3 = M_{(p)}.$$

Note that we use the fact that $d(s)h_p$ is an endomorphism of $\mathbb{Z}^3_{(p)}$ to get $d(s)h_p\mathbb{Z}^3_{(p)} \subset \mathbb{Z}^3_{(p)}$. Combining with (4.6)

$$st^{-1}\mathbb{Z}[1/d(s)]^3 = M[1/d(s)] \text{ inside } \mathbb{Q}^3,$$

and by taking the intersection of $d(s)st^{-1}\mathbb{Z}^3_{(p)}$ over all prime numbers p dividing $d(s)$, we get

$$d(s)st^{-1}\mathbb{Z}^3 \subset M \text{ inside } \mathbb{Q}^3.$$

For the other inclusion, we use the fact that

$$d(s)h_p^{-1}\mathbb{Z}^3_{(p)} \subset \mathbb{Z}^3_{(p)} \Longleftrightarrow \mathbb{Z}^3_{(p)} \subset \frac{1}{d(s)}h_p\mathbb{Z}^3_{(p)}.$$

Thus inside $\mathbb{Q}^3$ we have

$$M_{(p)} = \mathbb{Z}^3_{(p)} \subset \frac{1}{d(s)}h_p\mathbb{Z}^3_{(p)} = \frac{1}{d(s)}h_p(s_pt^{-1}\mathbb{Z}^3_{(p)}) = \frac{1}{d(s)}st^{-1}\mathbb{Z}^3_{(p)}.$$

□

4.3.3 The quotient of $ts^{-1}M + \mathbb{Z}^3$ by $\mathbb{Z}^3$

Lemma 4.3.2 gives us upper and lower bounds for M in $\mathbb{Q}^3$. But there are many sublattices of $\frac{1}{d(s)}st^{-1}\mathbb{Z}^3$ containing $d(s)st^{-1}\mathbb{Z}^3$. We also have the perfect lattice $(\mathbb{Z}^3, b, d)$ inside $\mathbb{Q}^3$. The following two inclusions are hold

$$d(s)\mathbb{Z}^3 \subset ts^{-1}M \subset \frac{1}{d(s)}\mathbb{Z}^3 \quad \text{and} \quad d(s)\mathbb{Z}^3 \subset \mathbb{Z}^3 \subset \frac{1}{d(s)}\mathbb{Z}^3.$$

Let us consider two important properties of the lattices $ts^{-1}M$ and $\mathbb{Z}^3$. First by the definition of M, we have a natural $\mathcal{G}_{x'}$-action. The element ts^{-1} of $\mathcal{G}(\mathbb{Q})$ maps x' to y. It induces, by conjugation, an isomorphism of sheaves $\mathcal{G}_{x'} \to \mathcal{G}_y$. This implies that $ts^{-1}M$ has a natural $\mathcal{G}_y$-action from the left. Thus both $ts^{-1}M$ and $\mathbb{Z}^3$ have $\mathcal{G}_y$-actions and contain y. Moreover both are perfect lattices for the standard inner product b and a trivialisation of the determinant d. These 2 properties will become our trump cards to determine explicitly $ts^{-1}M$ and also M.

First our strategy is to consider the sum of the two lattices $ts^{-1}M$ and $\mathbb{Z}^3$ inside $\mathbb{Q}^3$. We have

$$\mathbb{Z}^3 \subset (ts^{-1}M + \mathbb{Z}^3) \subset \frac{1}{d(s)}\mathbb{Z}^3.$$

Let p be a prime number dividing $d(s)$. Then $M_{(p)} = \mathbb{Z}^3_{(p)}$ and t is in $\mathcal{G}(\mathbb{Z}_{(p)})$. So we need to understand what $s^{-1}M_{(p)}$ is. We have

$$s^{-1} = s_p^{-1}h_p^{-1}, \tag{4.8}$$

where $h_p^{-1} \in \mathcal{G}_{x'}(\mathbb{Q})$ and $s_p \in {}_{x'}\mathcal{G}_x(\mathbb{Z}_{(p)})$. Thus $v_p(s^{-1}) = v_p(h_p^{-1}) < 0$. Recall that p is relatively prime with n. We know the structure of $\mathcal{G}_{x'}$ as a sheaf even as a group scheme over $\mathbb{Z}[1/2n]$ (see for instance 3.5.7 and 3.5.12). There we have a natural map $H \to N := \mathrm{SO}(x'^{\perp})$ which is an isomorphism over $\mathbb{Z}[1/2n]$. So H is isomorphic to the norm 1 torus $T_1 = \mathrm{Spec}(\mathbb{Z}[1/2n][x,y]/x^2 + ny^2 - 1)$.

4.3.4 Lemma. *We have that $-n$ is square in $\mathbb{F}_p$ or equivalently over $\mathbb{F}_p$ the norm 1 torus $\mathrm{Spec}(\mathbb{F}_p[x,y]/x^2+ny^2-1)$ is split. Over the ring of p-adic integers $\mathbb{Z}_p$, we have that*

$$\mathbb{Z}_p^3 = \mathbb{Z}_p x' \oplus x'^{\perp}_{\mathbb{Z}_p}$$

is an orthogonal direct sum and there exists a basis (v,w) of $x'^{\perp}_{\mathbb{Z}_p}$ with $b(v,v) = b(w,w) = 0$ and $b(v,w) = 1$, such that (x', v, w) are eigenvectors of h_p^{-1} with eigenvalues $1, \lambda, \lambda^{-1} \in \mathbb{Q}_p^{\times}$ respectively and $v_p(\lambda^{-1}) = v_p(h_p^{-1}) < 0$.

Proof. We have $h_p^{-1} \in \mathcal{G}(\mathbb{Q})$ but $h_p^{-1} \notin \mathcal{G}(\mathbb{Z}_{(p)})$. So h_p^{-1} corresponds to a $\mathbb{Q}$-point (a,b) of T_1 that is not in $T_1(\mathbb{Z}_{(p)})$. Thus we have $a^2+nb^2=1$ and $\gamma := -\min(v_p(a), v_p(b))$ is greater than 0. Let us write $a = a'/p^\gamma$ and $b = b'/p^\gamma$, then a' and b' are in $\mathbb{Z}_{(p)}$ and at least one of them is a unit. Then we get

$$1 = a^2+nb^2 = \big(\frac{a'}{p^\gamma}\big)^2 + n\big(\frac{b'}{p^\gamma}\big)^2,$$

and

$$p^{2\gamma} = a'^2 + nb'^2.$$

It follows that a' and b' are both units and that

$$-n = c^2 \quad \text{in } \mathbb{F}_p \text{ with } c = a'b'^{-1}.$$

Now we consider $x'^\perp$ with its bilinear form form b. Let us denote q for the quadratic form that b induces. Since $p \neq 2$, over $\mathbb{F}_p$, the quadratic from q is diagonalisable and with respect to some basis it is $d_1x_1^2 + d_2x_2^2$ with $d_1d_2 = n$. Since $-n = c^2$ in $\mathbb{F}_p$, we have $(c, d_1) \neq 0$ satisfying

$$d_1c^2 + d_2d_1^2 = d_1c^2 + d_1n = d_1c^2 - d_1c^2 = 0,$$

and the form $dx_1^2 + ex_2^2$ has a non-zero zero over $\mathbb{F}_p$. So there exists $v_0 \neq 0$ in $x'^\perp_{\mathbb{F}_p}$ such that $b(v_0, v_0) = 0$. Let w_0 be an element of $x'^\perp_{\mathbb{F}_p}$ such that $x'^\perp_{\mathbb{F}_p} = \mathbb{F}_p \cdot v_0 \oplus \mathbb{F}_p \cdot w_0$. By Hensel's lemma 3.4.4, we lift v_0 and w_0 to primitive elements $v, w' \in x'^\perp_{\mathbb{Z}_p}$ with $b(v,v) = 0$. By Nakayama's lemma, since (v_0, w_0) is a basis of $x'^\perp_{\mathbb{F}_p}$, (v, w') is a basis for $x'^\perp_{\mathbb{Z}_p}$. The Gram matrix B of b on $x'^\perp_{\mathbb{Z}_p}$ with respect to the basis (v, w') is

$$\begin{pmatrix} 0 & t \\ t & u \end{pmatrix} \quad \text{where } t \in \mathbb{Z}_p^\times \text{ and } u \in \mathbb{Z}_p.$$

Since the discriminant of b is n (see Section 3.5.4), that is coprime with p, we have that $\det(B) = t^2 = n \in \mathbb{Z}_p^\times$ up to square of units. By changing w' with $w'' := \frac{1}{t}w'$, we get a new basis (v, w'') of $x'^{\perp}_{\mathbb{Z}_p}$ such that $b(v, w'') = 1$. Again by changing w'' with $w := w'' - \frac{u}{2t^2}v$, the new basis (v, w) satisfies $b(v, w) = 1$ and $b(w, w) = 0$.

Now let us write h_p^{-1} in $\mathrm{SO}(x'^{\perp})(\mathbb{Q}_p)$, with respect to the basis (v, w) of $x'^{\perp}_{\mathbb{Z}_p}$, as

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in \mathrm{M}_2(\mathbb{Q}_p).$$

Then we get the following identities

$$1 = \langle v, w\rangle = \langle h_p^{-1}v, h_p^{-1}w\rangle = \langle a_1v + a_3w, a_2v + a_4w\rangle = a_1a_4 + a_2a_3,$$

$$0 = \langle v, v\rangle = \langle h_p^{-1}v, h_p^{-1}v\rangle = \langle a_1v + a_3w, a_1v + a_3w\rangle = 2a_1a_3,$$

$$0 = \langle w, w\rangle = \langle h_p^{-1}w, h_p^{-1}w\rangle = \langle a_2v + a_4w, a_2v + a_4w\rangle = 2a_2a_4,$$

and $\det(h_p^{-1}) = a_1a_4 - a_2a_3 = 1$. By adding the first equation with the last equation and by using the fact that $p \neq 2$, we have that $a_1a_4 = 1$ in $\mathbb{Q}_p$. Then we have $a_2 = a_3 = 0$. By changing the basis (v, w) with (w, v) if necessary, let us denote $\lambda := a_1$ and $\lambda^{-1} = a_4$ such that $v_p(\lambda) \geq 0 \geq v_p(\lambda^{-1})$. Now let g be the matrix in $\mathrm{GL}_3(\mathbb{Z}_p)$ with the columns x', v, w respectively. We have

$$g \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda^{-1} \end{pmatrix} \cdot g^{-1} = h_p^{-1}. \tag{4.9}$$

The coefficients of h_p^{-1} are $\mathbb{Z}_p$-linear combinations of $1, \lambda$, and λ^{-1}. So $v_p(\lambda^{-1}) \leq v_p(h_p^{-1})$. We multiply both sides of Equation 4.9 with g^{-1} from the left and g from the right and the same argument gives $v_p(\lambda^{-1}) \geq v_p(h_p^{-1})$. So we get that $v_p(\lambda^{-1}) = v_p(h_p^{-1}) < 0$. □

With this lemma we are ready to prove the following proposition that describes the quotient of $(ts^{-1}M + \mathbb{Z}^3)$ by $\mathbb{Z}^3$.

4.3.5 Proposition. *We have that the quotients* $(ts^{-1}M + \mathbb{Z}^3)/\mathbb{Z}^3$ *and* $(ts^{-1}M + \mathbb{Z}^3)/ts^{-1}M$ *are free* $\mathbb{Z}/d(s)\mathbb{Z}$*-modules of rank* 1.

Proof. We work first to prove the case $(ts^{-1}M + \mathbb{Z}^3)/\mathbb{Z}^3$ and the other case is an analog. It is sufficient to show, for each prime number p, that

$$(ts^{-1}M + \mathbb{Z}^3)/\mathbb{Z}^3 \otimes_{\mathbb{Z}} \mathbb{Z}_p = (ts^{-1}\mathbb{Z}_p^3 + \mathbb{Z}_p^3)/\mathbb{Z}_p^3 = (ts_p^{-1}h_p^{-1}\mathbb{Z}_p^3 + \mathbb{Z}_p^3)/\mathbb{Z}_p^3$$

is cyclic of order p^a, where $a = v_p(d(s))$. For p not dividing $d(s)$, it follows from the second inclusion of Lemma 4.3.2.

Now let p divide $d(s)$. As in Lemma 4.3.4 we write $\mathbb{Z}_p^3 = \mathbb{Z}_p x' \oplus \mathbb{Z}_p v \oplus \mathbb{Z}_p w$. Let us denote

$$M_p' = h_p^{-1}\mathbb{Z}_p^3 = \mathbb{Z}_p x' \oplus \mathbb{Z}_p p^a v \oplus \mathbb{Z}_p p^{-a} w.$$

Multiplying with $s_p t^{-1}$ gives an isomorphism

$$(ts_p^{-1}M_p' + \mathbb{Z}_p^3)/\mathbb{Z}_p^3 \xrightarrow{\sim} (M_p' + s_p t^{-1}\mathbb{Z}_p^3)/s_p t^{-1}\mathbb{Z}_p^3.$$

Since t, s_p are integral matrices in $\mathcal{G}(\mathbb{Z}_{(p)})$, we have $s_p t^{-1}\mathbb{Z}_p^3 = \mathbb{Z}_p^3$. So

$$(M_p' + s_p t^{-1}\mathbb{Z}_p^3)/s_p t^{-1}\mathbb{Z}_p^3 = (M_p' + \mathbb{Z}_p^3)/\mathbb{Z}_p^3 = \langle x', v, p^{-a}w\rangle/\langle x', v, w\rangle,$$

which is isomorphic to $(\mathbb{Z}/p^a\mathbb{Z})$. For the other case, we have for p dividing $d(s)$ that $(ts^{-1}M + \mathbb{Z}^3)/ts^{-1}M$ is isomorphic to

$$(M_p' + \mathbb{Z}_p^3)/M_p' = \langle x', v, p^{-a}w\rangle/\langle x', p^a v, p^{-a}w\rangle \simeq (\mathbb{Z}/p^a\mathbb{Z}) \cdot v.$$

□

4.3.6 Explicit computation for $ts^{-1}M + \mathbb{Z}^3 \subset \mathbb{Q}^3$ continued

We have an inclusion and an isomorphism of $\mathbb{Z}/d(s)\mathbb{Z}$-modules

$$(ts^{-1}M + \mathbb{Z}^3)/\mathbb{Z}^3 \subset \left(\frac{1}{d(s)}\mathbb{Z}^3\right)/\mathbb{Z}^3 \xrightarrow[\sim]{\cdot d(s)} (\mathbb{Z}/d(s)\mathbb{Z})^3.$$

By the last proposition $(ts^{-1}M + \mathbb{Z}^3)/\mathbb{Z}^3$ is a free $\mathbb{Z}/d(s)\mathbb{Z}$-module of rank 1, so it is a “line” in $(\mathbb{Z}/d(s)\mathbb{Z})^3$ or equivalently there exists $u \in \mathbb{Z}^3$, unique up to translation by $d(s)\mathbb{Z}^3$ and multiplication by integers coprime with $d(s)$, such that

$$ts^{-1}M + \mathbb{Z}^3 = \mathbb{Z}\frac{u}{d(s)} + \mathbb{Z}^3.$$

Let U^{-1} denote localisation with respect to the multiplicative set U that is generated by $\{p\colon p$ is a prime number and $p \nmid d(s)\}$. Over $\mathbb{Z}_{(p)}$, where p divides $d(s)$, the lattice $M_{(p)}$ is equal to the standard lattice $\mathbb{Z}^3_{(p)}$. Since finite intersections of $M_{(p)}$ over the primes p dividing $d(s)$ commute with localisation, we have $U^{-1}M = U^{-1}\mathbb{Z}^3$. Moreover since quotient and summations of modules commute with localisation, we get

$$\begin{aligned}
d(s)ts^{-1}(\mathbb{Z}/d(s)\mathbb{Z})^3 &= d(s)ts^{-1}U^{-1}(\mathbb{Z}/d(s)\mathbb{Z})^3 \\
&= (d(s)ts^{-1}U^{-1}\mathbb{Z}^3 + d(s)U^{-1}\mathbb{Z}^3)/d(s)U^{-1}\mathbb{Z}^3 \\
&= (d(s)ts^{-1}U^{-1}M + d(s)U^{-1}\mathbb{Z}^3)/d(s)U^{-1}\mathbb{Z}^3 \\
&= U^{-1}\left((d(s)ts^{-1}M + d(s)\mathbb{Z}^3)/d(s)\mathbb{Z}^3\right) \\
&\subset U^{-1}\left(\mathbb{Z}/d(s)\mathbb{Z}\right)^3 = (\mathbb{Z}/d(s)\mathbb{Z})^3.
\end{aligned}$$

So to get the vector u, it is sufficient to compute the image of the morphism of modules

$$d(s)ts^{-1}\colon (\mathbb{Z}/d(s)\mathbb{Z})^3 \to (\mathbb{Z}/d(s)\mathbb{Z})^3. \tag{4.10}$$

Let $\bar{u} \in (\mathbb{Z}/d(s)\mathbb{Z})^3$ be a generator of $d(s)ts^{-1}((\mathbb{Z}/d(s)\mathbb{Z})^3)$ and let (a, b, c) in $\mathbb{Z}^3$ be a lift of $\bar{u}$. Then

$$\frac{1}{d(s)}\begin{pmatrix} a \\ b \\ c \end{pmatrix}, e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

generates $ts^{-1}M + \mathbb{Z}^3$. As $\bar{u}$ is of order $d(s)$, $\gcd(a, b, c)$ is relatively prime with $d(s)$. Let $u := (a, b, c)/\gcd(a, b, c)$. Then $(\frac{u}{d(s)}, e_1, e_2, e_3)$ generates $ts^{-1}M + \mathbb{Z}^3$, since $\overline{\gcd(a, b, c)}$ is a unit in $\mathbb{Z}/d(s)\mathbb{Z}$. Because u is primitive, there exist $v_2, v_3 \in \mathbb{Z}^3$ such that (u, v_2, v_3) is a basis of $\mathbb{Z}^3$. Let $v_1 := \frac{1}{d(s)}u$. Then $\big(v_1, v_2, v_3\big)$ is a basis of $\mathbb{Z}\frac{u}{d(s)} + \mathbb{Z}^3$.

For explicit computation, we want an algorithm to compute a basis of the image of morphism of modules $d(s)ts^{-1}$, given the entries of the matrix $d(s)ts^{-1}$. First $\mathbb{Z}/d(s)\mathbb{Z}$ is a principal ideal ring and gcd's (defined up to units) can be computed efficiently. If we represent elements of $\mathbb{Z}/d(s)\mathbb{Z}$ as elements in $\mathbb{Z}$ in the interval $[0, d(s) - 1]$, then the ideal $(a_1, ..., a_n)$ of $\mathbb{Z}/d(s)\mathbb{Z}$ gives, by pullback to $\mathbb{Z}$, the ideal $(d(s), a_1, ..., a_n)$. Any generator of that gives a generator of the original ideal in $\mathbb{Z}/d(s)\mathbb{Z}$.

We use a well known algorithm, the Smith normal form (see [4] Theorem 2.4.12 for $\mathbb{Z}$-modules but it can be applied in the above situation for $\mathbb{Z}/d(s)\mathbb{Z}$-modules), that uses gcd's to bring any u in say $\mathrm{M}_{n,m}(\mathbb{Z}/d(s)\mathbb{Z})$ by row and column operations into diagonal form where the elements of the diagonal divide the next ones. After applying this algorithm to our matrix, then $d(s)ts^{-1}$ will be of the form $\mathrm{diag}(a, 0, 0)$ for some $a \in (\mathbb{Z}/d(s)\mathbb{Z})^\times$. All row operations together are given by multiplication on the left by an invertible matrix say w. Now we undo the row operations: the first column $\bar{u}$ of $w^{-1}.d(s)ts^{-1}$ is a basis of $d(s)ts^{-1}(\mathbb{Z}/d(s)\mathbb{Z}^3)$. We write $\bar{u} = (\bar{a}, \bar{b}, \bar{c})$ where a, b, c are elements in $\mathbb{Z}$ in the interval $[0, d(s) - 1]$ and let $u = (a', b', c')$

where $d = \gcd(a,b,c), a' = a/d, b' = b/d$, and $c' = c/d$. Here we use the Euclidean algorithm to find $\gcd(a,b,c)$. Then $ts^{-1}M + \mathbb{Z}^3$ is generated by

$$\frac{u}{d(s)},\ e_1 = \begin{pmatrix}1\\0\\0\end{pmatrix}, e_2 = \begin{pmatrix}0\\1\\0\end{pmatrix}, e_3 = \begin{pmatrix}0\\0\\1\end{pmatrix}.$$

To find v_2, v_3 such that (u, v_2, v_3) is a basis for $\mathbb{Z}^3$ we do the following: first let $\alpha, \beta, \gamma \in \mathbb{Z}$ such that $\alpha a' + \beta b' + \gamma c' = 1$ by using the Euclidean algorithm. Then we have the following split exact sequence of $\mathbb{Z}$-modules

$$\ker(l) \hookrightarrow \mathbb{Z}^3 \xrightarrow{l} \mathbb{Z}, \quad v = (x,y,z) \mapsto l(v) := \alpha x + \beta y + \gamma z,$$

with the splitting given by $1 \mapsto (a', b', c')$. We use the algorithm that is an application of the Hermite normal form (see [4] Proposition 2.4.9) to find a basis for $\ker(l)$. We denote this basis as (v_2, v_3). Let $v_1 := \frac{u}{d(s)}$. So we get explicitly a basis (v_1, v_2, v_3) for $ts^{-1}M + \mathbb{Z}^3$.

4.3.7 Getting a basis for $ts^{-1}M$ given one for $ts^{-1}M+\mathbb{Z}^3$

Let us use the same notation: we have a basis (v_1, v_2, v_3) for $ts^{-1}M + \mathbb{Z}^3$ and vectors that generate it

$$\frac{1}{d(s)}u,\ e_1 = \begin{pmatrix}1\\0\\0\end{pmatrix},\ e_2 = \begin{pmatrix}0\\1\\0\end{pmatrix},\ e_3 = \begin{pmatrix}0\\0\\1\end{pmatrix},$$

where $d(s)v_1 = u$. Moreover (u, v_2, v_3) is a basis for $\mathbb{Z}^3$. We have a surjective linear map

$$l_1 \colon (ts^{-1}M + \mathbb{Z}^3) \to \mathbb{Z}$$

defined as: for $v = xv_1 + yv_2 + zv_3 \in ts^{-1}M + \mathbb{Z}^3, l(v) = x$. We also have the composed map $\bar{l_1} = \sigma \circ l_1$, where $\sigma \colon \mathbb{Z} \to \mathbb{Z}/d(s)\mathbb{Z}$ is the quotient map. We have that

$$\begin{aligned}\ker(\bar{l_1}) &= \{v = xv_1 + yv_2 + zv_3 \in ts^{-1}M + \mathbb{Z}^3 : x = 0 \text{ in } \mathbb{Z}/d(s)\mathbb{Z}\} \\ &= \langle d(s)v_1, v_2, v_3 \rangle = \mathbb{Z}^3.\end{aligned}$$

The standard inner product b is perfect on $ts^{-1}M$ and $\mathbb{Z}^3$, in particular it is $\mathbb{Z}$-valued on each of them. We have the following lemma.

4.3.8 Lemma. *The quadratic form q, that is induced by b, on $ts^{-1}M + \mathbb{Z}^3$ has values in $\frac{1}{d(s)}\mathbb{Z}$.*

Proof. Since $ts^{-1}M + \mathbb{Z}^3 = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \mathbb{Z}v_3$, with $d(s)v_1, v_2, v_3 \in \mathbb{Z}^3$, it is sufficient to show that

$$q(v_1) = b(v_1, v_1) = \frac{b(u,u)}{d(s)^2} \in \frac{1}{d(s)}\mathbb{Z}.$$

Therefore it is sufficient to show that $b(u,u) \in d(s)\mathbb{Z}$, which is equivalent to $b(\bar{u}, \bar{u}) = 0$. For each prime p dividing $d(s)$, we have $d(s)ts^{-1} = d(s)ts_p^{-1}h_p^{-1}$ (see Identity 4.8). By Proposition 4.3.5, we get the following diagram

$$\begin{tikzcd}
\mathbb{Z}_p^3/d(s)\mathbb{Z}_p^3 \arrow[dd, "d(s)h_p^{-1}"'] \arrow[dddd, bend right=60, "d(s)ts^{-1}"'] & = & \mathbb{Z}_p\bar{x}' & + & \mathbb{Z}_p\bar{v} & + & \mathbb{Z}_p\bar{w} \\
 & & \bar{x}' \arrow[d, mapsto] & & \bar{v} \arrow[d, mapsto] & & \bar{w} \arrow[d, mapsto] \\
\mathbb{Z}_p^3/d(s)\mathbb{Z}_p^3 \arrow[d, "s_p^{-1}"'] & & 0 \arrow[d, mapsto] & & 0 \arrow[d, mapsto] & & \text{unit} \cdot \bar{w} \arrow[d, mapsto] \\
\mathbb{Z}_p^3/d(s)\mathbb{Z}_p^3 \arrow[d, "t"'] & & 0 \arrow[d, mapsto] & & 0 \arrow[d, mapsto] & & s_p^{-1}\text{unit} \cdot \bar{w} \arrow[d, mapsto] \\
\mathbb{Z}_p^3/d(s)\mathbb{Z}_p^3 & & 0 & & 0 & & ts_p^{-1}\text{unit} \cdot \bar{w}.
\end{tikzcd}$$

Since $\bar{u}$ generates $d(s)ts^{-1}(\mathbb{Z}/d(s)\mathbb{Z})^3$, we have $\bar{u} = \text{unit} \cdot ts_p^{-1}\bar{w}$. Since ts_p^{-1} is an orthogonal matrix for the inner product b and integral at p and because $b(w, w) = 0$ in $\mathbb{Z}_p$, we get

$$b(\bar{u}, \bar{u}) = b(\text{unit} \cdot ts_p^{-1}\bar{w}, \text{unit} \cdot ts_p^{-1}\bar{w}) = \text{unit}^2 \cdot b(\bar{w}, \bar{w}) = 0.$$

□

We define a map

$$\bar{Q}\colon (ts^{-1}M + \mathbb{Z}^3) \to \mathbb{Z}/d(s)\mathbb{Z}, \quad v \mapsto \overline{d(s) \cdot q(v)}.$$

Since b is perfect on $\mathbb{Z}^3$, we have $\bar{Q}(\mathbb{Z}^3) = 0$. For $v = xv_1 + yv_2 + zv_3$ in the lattice $ts^{-1}M + \mathbb{Z}^3$, we have that $d(s)b(v, v)$ is equal to

$$d(s)b(v_1, v_1)x^2 + 2d(s)b(v_1, v_2)xy + 2d(s)b(v_1, v_3)xz + d(s)q(yv_2 + zv_3).$$

Since q has integral values on $\langle v_2, v_3\rangle$, we have $d(s)q(yv_2 + zv_3) \equiv 0$ in $\mathbb{Z}/d(s)\mathbb{Z}$. So we get

$$\bar{Q}(v) = \bar{x}\overline{b(u, xv_1 + 2yv_2 + 2zv_3)}.$$

We define the map $\bar{l_2}\colon (ts^{-1}M + \mathbb{Z}^3) \to \mathbb{Z}/d(s)\mathbb{Z}$ as:

$$v = (x, y, z) \mapsto \bar{l_2}(v) = \overline{b(u, xv_1 + 2yv_2 + 2zv_3)}.$$

It is a linear map such that $\bar{Q} = \bar{x} \cdot \bar{l_2} = \bar{l_1}\bar{l_2}$.

4.3.9 Proposition. *With the above description, we have that*

$$ts^{-1}M = \ker(\bar{l_2}).$$

Proof. First we will show that the map $\bar{l_2}$ is surjective. Let us write $u = (a, b, c)$. Then $\gcd(a, b, c) = 1$. There exist $\alpha, \beta, \gamma \in \mathbb{Z}$ such that $\alpha a + \beta b + \gamma c = 1$ and we choose such a triple. Because $(d(s)v_1, v_2, v_3)$ is a basis of $\mathbb{Z}^3$ and $d(s)$ is odd, we may choose $x, y, z \in \mathbb{Z}^3$ such that

$$\overline{xv_1 + 2yv_2 + 2zv_3} = (\bar{\alpha}, \bar{\beta}, \bar{\gamma}) \in (\mathbb{Z}/d(s)\mathbb{Z})^3.$$

Let us denote $v := xv_1 + 2yv_2 + 2zv_3$. This implies $\bar{l_2}(v) = 1$ in $\mathbb{Z}/d(s)\mathbb{Z}$ and $\bar{l_2}$ is surjective. Thus $\ker(\bar{l_2})$ is a sublattice of $ts^{-1}M + \mathbb{Z}^3$ of index $d(s)$ with cyclic quotient. Note that $\ker(\bar{l_2})$ contains $d(s)\mathbb{Z}^3$. Since both $ts^{-1}M$ and $\ker(\bar{l_2})$ are contained in $\frac{1}{d(s)}\mathbb{Z}^3$ and contain $d(s)\mathbb{Z}^3$, it is sufficient to check whether both are the same $\mathbb{Z}_p$-lattices for each prime p dividing $d(s)$.

Again by Proposition 4.3.5, we have

$$\mathbb{Z}_p^3 = \mathbb{Z}_p x' + \mathbb{Z}_p v + \mathbb{Z}_p w \text{ and } ts^{-1}M_p + \mathbb{Z}_p^3 = \mathbb{Z}_p x' + \mathbb{Z}_p v + \mathbb{Z}_p \frac{w}{d(s)}.$$

With respect to the basis $(x', v, \frac{w}{d(s)})$, for $v = xx' + yv + z\frac{w}{d(s)} \in ts^{-1}M + \mathbb{Z}^3$, we have the following identity:

$$\begin{aligned} d(s)b(v,v) &= \frac{b(w,w)}{d(s)}z^2 + 2b(w,x')zx + 2b(w,v)zy + d(s)q(xx' + yv) \\ &= 2zy + d(s)q(xx' + yv). \end{aligned}$$

The map $\bar{Q}\colon (ts^{-1}M + \mathbb{Z}^3) \to \mathbb{Z}/d(s)\mathbb{Z}$ with respect to this basis is given by $(x, y, z) \mapsto 2\bar{z}\bar{y}$. Moreover we have the two linear maps

$$\bar{l_3}, \bar{l_4}\colon (ts^{-1}M + \mathbb{Z}^3) \to \mathbb{Z}/d(s)\mathbb{Z}, \quad v = (x, y, z) \mapsto \bar{l_3}(v) = \bar{z} \text{ and } \bar{l_4}(v) = 2\bar{y}.$$

So the quadratic form $\bar{Q}\colon (ts^{-1}M_p + \mathbb{Z}_p^3) \to \mathbb{Z}_p/d(s)\mathbb{Z}_p$ can be written as products of linear forms $\bar{Q} = \bar{l_1}\bar{l_2} = \bar{l_3}\bar{l_4}$. Note that $\bar{l_1}$ and $\bar{l_3}$ have the same kernel, that is $\mathbb{Z}_p^3$. By the universal properties of $\ker(\bar{l_1})$ and $\ker(\bar{l_3})$, there exists a unique isomorphism $f\colon \mathbb{Z}_p/d(s)\mathbb{Z}_p \to \mathbb{Z}_p/d(s)\mathbb{Z}_p$ such that we have the following commutative diagram of morphisms of $\mathbb{Z}_p$-modules

$$\begin{tikzcd}
 & \mathbb{Z}_p/d(s)\mathbb{Z}_p \arrow[dd, dotted, "f"] \\
(ts^{-1}M_p + \mathbb{Z}_p^3) \arrow[ur, "\bar{l_1}"] \arrow[dr, "\bar{l_3}"] & \\
 & \mathbb{Z}_p/d(s)\mathbb{Z}_p.
\end{tikzcd}$$

The automorphism group of the cyclic group $\mathbb{Z}_p/d(s)\mathbb{Z}_p$ is its unit group, hence $\bar{l_1} = c \cdot \bar{l_3}$, for some $c \in (\mathbb{Z}_p/d(s)\mathbb{Z}_p)^\times$. Note that the multiplication by $x \in (\mathbb{Z}_p/d(s)\mathbb{Z}_p)[x, y, z]$ gives an injective map

$$(\mathbb{Z}_p/d(s)\mathbb{Z}_p)[x, y, z] \xrightarrow{x\cdot} (\mathbb{Z}_p/d(s)\mathbb{Z}_p)[x, y, z].$$

Thus we get $\bar{l_2} = 1/c \cdot \bar{l_4}$, in particular $\ker(\bar{l_2}) = \ker(\bar{l_4}) = ts^{-1}M_p$. $\square$

Let us now make the computation of a basis of $ts^{-1}M$ explicit. Let

$$d := \gcd(b(u, v_1), 2b(u, v_2), 2b(u, v_3)).$$

We denote

$$a_1 := b(u, v_1)/d, a_2 := 2b(u, v_2)/d, a_3 := 2b(u, v_3)/d.$$

Thus $\gcd(a_1, a_2, a_3) = 1$. Let $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}$ such that $a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3 = 1$. The map $\bar{l_2}$ is surjective, in particular d and $d(s)$ are coprime and d is a unit in $\mathbb{Z}/d(s)\mathbb{Z}$. So for computing $\ker(\bar{l_2})$, we may replace $\bar{l_2}$ by

$$\bar{l_2}\colon (\mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \oplus \mathbb{Z}v_3) \to \mathbb{Z}/d(s)\mathbb{Z}, (x, y, z) \mapsto \overline{a_1x + a_2y + a_3z}.$$

To get a basis for $ts^{-1}M$ we consider the following split exact sequence of $\mathbb{Z}$-modules

$$\ker(l_2) \hookrightarrow (ts^{-1}M + \mathbb{Z}^3) \twoheadrightarrow \mathbb{Z}, v = (x, y, z) \mapsto l_2(v) := a_1x + a_2y + a_3z.$$

By using the splitting map

$$f\colon \mathbb{Z} \to (ts^{-1}M + \mathbb{Z}^3), 1 \mapsto f(1) := \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3$$

of l_2, we get that the $\mathbb{Z}$-module $(ts^{-1}M + \mathbb{Z}^3)$ is isomorphic to the direct sum of $\ker(l_2) \oplus \mathbb{Z} \cdot f(1)$ given by

$$v \in (ts^{-1}M + \mathbb{Z}^3) \mapsto (v - f(l_2(v))) + l_2(v)f(1) \in (\ker(l_2) \oplus \mathbb{Z} \cdot f(1)) .$$

In particular we have

$$\ker(\bar{l_2}) = \ker(l_2) \oplus \mathbb{Z} \cdot d(s)f(1).$$

We use again the algorithm, that is an application of the Hermite normal form (see [4] Proposition 2.4.9), to find a basis for $\ker(l_2)$. We denote this basis as (w_2', w_3'). Let $w_1' := d(s)f(1)$. So we get explicitly a basis (w_1', w_2', w_3') for the lattice $ts^{-1}M$. By multiplying with st^{-1}, we get a basis (w_1, w_2, w_3) for M. By using the LLL-algorithm (see [4] Section 2.6, especially Theorem 2.6.2) for rank 3, we obtain an orthonormal basis for M. So we have an isomorphism of triples (M, b, d), $\phi^{-1}\colon \mathbb{Z}^3 \xrightarrow{\sim} M$, that is an element of $\mathcal{G}(\mathbb{Q})$. Thus $[y'] = \phi^{-1}[x']$.

4.4 Some explicit computation

Let $n = 770 = 2{\cdot}5{\cdot}7{\cdot}11$, the same example that Gauss gives in his Disquisitiones Arithmeticae. The number n can be written as a sum of 3 squares up to $\mathrm{SO}_3(\mathbb{Z})$-action in the following 16 ways:

$$\begin{aligned} 770 &= (\pm 27)^2 + 5^2 + 4^2 = (\pm 25)^2 + 9^2 + 8^2 = (\pm 25)^2 + 12^2 + 1^2 \\ &= (\pm 24)^2 + 13^2 + 5^2 = (\pm 23)^2 + 15^2 + 4^2 = (\pm 20)^2 + 19^2 + 3^2 \\ &= (\pm 20)^2 + 17^2 + 9^2 = (\pm 17)^2 + 16^2 + 15^2. \end{aligned}$$

Let $O = \mathbb{Z}[x]/(x^2 + 770)$ be the ring of integers in $\mathbb{Q}(\sqrt{-770})$. Since $-770 = 2 \pmod 4$, by Gauss, we get $\#\operatorname{Pic}(O) = 32$. Since 2 is ramified in O, we get $\#\operatorname{Pic}(\mathbb{Z}[1/2, \sqrt{-770}]) = 16$. We will show that

$$\operatorname{Pic}(\mathbb{Z}[1/2, \sqrt{-770}]) \cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

We have maximal ideals of O and some relations:

$$\begin{array}{rr} (2, x) =: m_2 & m_2^2 = (4, 2x, -770) = (2, 2x) = (2) \\ (3, x-1) =: m_3 & \\ (3, x+1) = \bar{m}_3 & m_3\bar{m}_3 = (9, 3(x+1), 3(x-1), -771) = (3) \\ (5, x) =: m_5 & m_5^2 = (25, 5x, -770) = (5, 5x) = (5) \\ (7, x) =: m_7 & m_7^2 = (49, 7x, -770) = (7, 7x) = (7) \\ (11, x) =: m_{11} & m_{11}^2 = (121, 11x, -770) = (11, 11x) = (11) \\ & m_2 m_5 m_7 m_{11} = (x). \end{array}$$

First we find the order of m_3. Note that for any $a + bx \in O$, the norm $N(a + bx) = a^2 + 770b^2$ is greater or equal to 770 if $b \neq 0$. We have $N(m_3^4) = 81 < 770$. A generator for the ideal m_3^4, if it exists, is in the form $a \in \mathbb{Z}$ where $a = \pm 9$. Since $(3) = m_3\bar{m}_3$, we have $(3^2) = m_3^4 = m_3^2\bar{m}_3{}^2$. So by the unique factorization into prime ideals in O, $\bar{m}_3 = m_3$, which is absurd. Thus m_3^4 is not principal. We have the following computation:

$$\begin{aligned} m_3^2 &= (9, 3(x-1), (x-1)^2) = (9, x+2) \\ m_3^4 &= (81, x+11) \\ m_3^8 = (6561, x+3251) \supseteq (2(x+3251) - 6561) &= (2x-59). \end{aligned}$$

The inclusion is an equality because both ideals have norm 3^8 and m_3^8 is principal.

4.4.1 Lemma. *Let $n > 0$ be an even square-free integer, $K := \mathbb{Q}(\sqrt{-n})$ and $O = \mathbb{Z}[\sqrt{-n}]$ the ring of integers of K. The discriminant of O is $-4n$. Let $p_1, \ldots, p_k$ be the prime divisors of n. The ramified maximal ideals are $m_i := (p_i, \sqrt{-n})$ where $i = 1, \ldots, k$. Then the classes of $m_1, \ldots, m_k$ generate $\mathrm{Pic}(O)[2]$. We have $\#\,\mathrm{Pic}(O)[2] = 2^{k-1}$ and $m_1 \cdots m_k = \sqrt{-n} \cdot O$.*

Proof. As $\mathbb{Z}[\sqrt{-n}] = \mathbb{Z}[x]/(x^2+n)$, the primes p in $\mathbb{N}$ that ramify in O are precisely the p_i. For each i, $O/m_i = O/(p_i, \sqrt{-n}) = \mathbb{F}_{p_i}$ hence the m_i is the unique maximal ideal containing p_i. All maximal ideals of O other than the m_i are invertible. The m_i are invertible as well, because $m_i^2 = p_i \cdot O$. Hence O is the ring of integers in K. The discriminant of O is the discriminant of $x^2 + n$, hence equal to $-4n$.

Let J be a non-zero ideal of O, such that J^2 is principal.Let σ be the non-trivial automorphism of O. Then in $\mathrm{Pic}(O)$ we have $[J] \cdot [J] = [J] \cdot [\sigma(J)]$ because both J^2 and $J \cdot \sigma(J)$ are principal. Hence there is an a in $K^\times$ such that $\sigma(J) = a \cdot J$. Then $N(J) = N(a \cdot \sigma(J)) = N(a)N(J)$, hence $N(a) = 1$. By Hilbert 90, there is a b in $K^\times$ such that $a = b/\sigma(b)$. That gives $bJ = \sigma(bJ)$. The unique factorisation $bJ = \prod_m m^{n_m}$ then shows that bJ is a principal ideal times an ideal of the form $m_1^{n_1} \cdot m_k^{n_k}$ with the n_i in $\{0, 1\}$.

To finish, it suffices to show that for any proper subset S of $\{1,\ldots,k\}$ the ideals $\prod_{i\in S} m_i$ are non-principal. Suppose $S \subsetneq \{1,\ldots,k\}$ and $a,b\in\mathbb{Z}$ are such that $\prod_{i\in S} m_i = (a+b\sqrt{-n})\cdot O$. Taking norm on both sides, we get $\prod_{i\in S} p_i = a^2+nb^2$ and it is greater or equal to $n = p_1\ldots p_k$ if $b\neq 0$. Hence $b=0$. Then $\prod_{i\in S} p_i = a^2$ shows that S is empty. □

We have $\#\operatorname{Pic}(O) = 32$. We also have the order of m_3 is 8 in $\operatorname{Pic}(O)$ and m_2, m_5, m_7, and m_{11} are all of order 2. So by previous lemma, we get

$$\operatorname{Pic}(O) \cong \mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$$

and also

$$\operatorname{Pic}(\mathbb{Z}[1/2,\sqrt{-770}]) \cong \mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}.$$

4.4.2 An example of Gauss composition for 770

Now we will show some examples of Gauss composition for the 2-sphere for this n. Let $x=(25,9,-8)$, $y=(23,15,4)$, and $x'=(25,12,1)$. We want to find $\bar{y}'\in\mathcal{G}(S)\setminus\mathcal{X}(S)$ such that $[{}_y\mathcal{G}_x] = [{}_{y'}\mathcal{G}_{'x}]$. We obtain an element $t\in {}_yG_x(\mathbb{Q})$ by composing two symmetries: the first one is s_z the symmetry about the hyperplane perpendicular to $z:=(0,0,1)$ and the second one is the symmetry about the hyperplane perpendicular to the vector $y-s_z(x)$. This gives

$$t=\frac{1}{7}\begin{pmatrix}6 & 3 & 2\\ 3 & -2 & -6\\ -2 & 6 & -3\end{pmatrix} \text{ in } {}_yG_x(\mathbb{Z}[1/7]).$$

We obtain an element $s\in {}_{x'}G_x(\mathbb{Q})$ by composing two symmetries: the first one is s_z and the second one is the symmetry about the hyperplane perpendicular to the vector $x' - s_z(x)$. This gives

$$s = \frac{1}{29}\begin{pmatrix} 29 & 0 & 0 \\ 0 & 20 & -21 \\ 0 & 21 & 20 \end{pmatrix} \text{ in } {}_{x'}G_x(\mathbb{Z}[1/29]).$$

It has a pole at 29. Note that 29 is coprime with $n = 770$ and $d(t) = 7$. By Lemma 4.3.2, we have $29\mathbb{Z}^3 \subset ts^{-1}M \subset 29^{-1}\mathbb{Z}^3$. Now we consider the lattice $ts^{-1}M + \mathbb{Z}^3$ inside $\frac{1}{29}\mathbb{Z}^3$. Proposition 4.3.5 shows that $(ts^{-1}M + \mathbb{Z}^3)/\mathbb{Z}^3$ is a free $\mathbb{Z}/29\mathbb{Z}$-module of rank 1. To get a generator $\bar{u}$ of $(ts^{-1}M + \mathbb{Z}^3)/\mathbb{Z}^3$, we consider the image of the morphism of modules (4.10)

$$29ts^{-1} \colon (\mathbb{Z}/29\mathbb{Z})^3 \to (\mathbb{Z}/29\mathbb{Z})^3.$$

It is generated by $\bar{u} = (\bar{1}, \bar{8}, \bar{15}) \in (\mathbb{Z}/29\mathbb{Z})^3$. Let $u = (1, 8, 15)$ be a lifting of $\bar{u}$ in $\mathbb{Z}^3$ with $\gcd(1, 8, 15) = 1$. We extend u to a basis (u, v_2, v_3) of $\mathbb{Z}^3$, where $v_2 = (0, 1, 0)$ and $v_3 = (0, 0, 1)$. So we get a basis for $\mathbb{Z}^3 + ts^{-1}M$:

$$v_1 = (1/29, 8/29, 15/29), \quad v_2 = (0, 1, 0), \quad v_3 = (0, 0, 1).$$

We know that $\mathbb{Z}^3 + ts^{-1}M$ has two sublattices of index 29 on which the inner product is integral: $\mathbb{Z}^3$ and $ts^{-1}M$. We have the quadratic form

$$\bar{Q} \colon (ts^{-1}M + \mathbb{Z}^3) \to \mathbb{Z}/29\mathbb{Z}, (x, y, z) \mapsto x(10x + 16y + z) \pmod{29}.$$

We get

$$ts^{-1}M = \ker((ts^{-1}M + \mathbb{Z}^3) \to \mathbb{Z}/29\mathbb{Z}, (x, y, z) \mapsto 10x + 16y + z \pmod{29}).$$

Over $\mathbb{Z}/29\mathbb{Z}$ we have $\bar{x} = 10\bar{y} - 3\bar{z}$ and $x = 10y - 3z + 29t$ for some $t \in \mathbb{Z}$. So we get

$$ts^{-1}M = \{xv_1 + yv_2 + zv_3 : x = 10y - 3z + 29t, t \in \mathbb{Z}\}.$$

By substituting $x = 10y - 3z + 29t$, we get a basis for $ts^{-1}M$:

$$(10, 109, 150)/29, (-3, -24, -16)/29, (1, 8, 15),$$

and then via multiplication by st^{-1} a basis for M:

$$(-1, 32, -2)/7, (-2, -6, 3)/7, (0, 119, -7)/7.$$

We get the Gram matrix with respect to that basis of M:

$$\begin{pmatrix} 21 & -4 & 78 \\ -4 & 1 & -15 \\ 78 & -15 & 290 \end{pmatrix}.$$

Here is the LLL-algorithm, written in the product of elementary operations:

$$\begin{pmatrix} 1 & 0 & 0 \\ 4 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 15 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 4 & 0 & -7 \\ 1 & 1 & 2 \\ -1 & 0 & 2 \end{pmatrix}.$$

It gives us an (oriented) orthonormal basis for M:

$$(-6, 3, 2)/7, (-2, -6, 3)/7, (3, 2, 6)/7.$$

This gives

$$y' = \frac{1}{7} \begin{pmatrix} -6 & 3 & 2 \\ -2 & -6 & 3 \\ 3 & 2 & 6 \end{pmatrix} \begin{pmatrix} 25 \\ 12 \\ 1 \end{pmatrix} = \begin{pmatrix} -16 \\ -17 \\ 15 \end{pmatrix}.$$

So here we show in the computation how to get explicitly the action of the Picard group on the set of orbits of primitive solutions of sum of 3 squares that the sheaf method gives.

4.4.3 Another example for 770

In the previous subsection we have $x = (25, 9, -8)$, $y = (23, 15, 4)$, and $x' = (25, 12, 1)$ and we find $\bar{y}' \in \mathcal{G}(S) \setminus \mathcal{X}(S)$ such that $\bar{x}' \xmapsto{[{}_yG_x]} \bar{y}'$. Since it is a "parallelogram law", we know that $\bar{y} \xmapsto{[{}_{x'}G_x]} \bar{y}'$. So let us exchange the values of $y \mapsto x'$ and of $x' \mapsto y$ and we do the same computation that shows that it will produce the same y' up to $\mathrm{SO}_3(\mathbb{Z})$-orbit. So now $x = (25, 9, -8)$, $y = (25, 12, 1)$, and $x' = (23, 15, 4)$. Let us take

$$t = \frac{1}{29}\begin{pmatrix} 29 & 0 & 0 \\ 0 & 20 & -21 \\ 0 & 21 & 20 \end{pmatrix} \text{ in } {}_yG_x(\mathbb{Z}[1/29])$$

and

$$s = \frac{1}{7}\begin{pmatrix} 6 & 3 & 2 \\ 3 & -2 & -6 \\ -2 & 6 & -3 \end{pmatrix} \text{ in } {}_{x'}G_x(\mathbb{Z}[1/7]).$$

4.4.4 Remark. Here $d(s) = 7$, which divides 770. It is not coprime with 770 as required in Lemma 4.3.1 and Lemma 4.3.4. But we continue the computation nevertheless and will see that it gives the right y' up to $\mathrm{SO}_3(\mathbb{Z})$-action. This is an indication that $d(s)$ does not need to be coprime with n. This will be investigated later, there is no time now to include it in this thesis. We will use a correct choice of s after this example.

We get $7\mathbb{Z}^3 \subset ts^{-1}M \subset 7^{-1}\mathbb{Z}^3$ and we consider the lattice $ts^{-1}M + \mathbb{Z}^3$ inside $\frac{1}{7}\mathbb{Z}^3$. The image of the morphism of modules

$$7ts^{-1} \colon (\mathbb{Z}/7\mathbb{Z})^3 \to (\mathbb{Z}/7\mathbb{Z})^3$$

is generated by $\bar{u} = (\bar{1}, \bar{3}, \bar{2}) \in (\mathbb{Z}/7\mathbb{Z})^3$. Let $u = (1, 3, 2)$ be a lifting of $\bar{u}$ in $\mathbb{Z}^3$ with $\gcd(1, 3, 2) = 1$. We extend u to a basis (u, v_2, v_3) of $\mathbb{Z}^3$, where

$v_2 = (0,1,0)$ and $v_3 = (0,0,1)$. So we get a basis for $\mathbb{Z}^3 + ts^{-1}M$:

$$v_1 = (1/7, 3/7, 2/7), \quad v_2 = (0,1,0), \quad v_3 = (0,0,1).$$

We have the quadratic form

$$\bar{Q}\colon (ts^{-1}M + \mathbb{Z}^3) \to \mathbb{Z}/7\mathbb{Z}, (x,y,z) \mapsto x(x+3y+2z) \pmod 7.$$

We get

$$ts^{-1}M = \ker((ts^{-1}M + \mathbb{Z}^3) \to \mathbb{Z}/7\mathbb{Z}, (x,y,z) \mapsto x+3y+2z \pmod 7).$$

By substituting $x = -3y - 2z + 7t$, we get a basis for $ts^{-1}M$:

$$(-3,-2,-6)/7, (-2,-6,3)/7, (1,3,2),$$

and by the LLL-algorithm, we get an (oriented) orthonormal basis for $ts^{-1}M$:

$$(-3,-2,6)/7, (-2,-6,3)/7, (-6,3,2)/7.$$

This gives

$$y' = \begin{pmatrix} 25 & 12 & 1 \end{pmatrix} st^{-1}\frac{1}{7}\begin{pmatrix} -3 & -2 & -6 \\ -2 & -6 & 3 \\ 6 & 3 & 2 \end{pmatrix} = \begin{pmatrix} -15 & -17 & -16 \end{pmatrix}.$$

Let us do the same computation with a different choice of s such that $d(s)$ coprime with 770 and $d(t)$. Let $x = (25, 9, -8)$, $y = (25, 12, 1)$, and $x' = (23, 15, 4)$. Let us take

$$t = \frac{1}{29}\begin{pmatrix} 29 & 0 & 0 \\ 0 & 20 & -21 \\ 0 & 21 & 20 \end{pmatrix} \text{ in } {}_yG_x(\mathbb{Z}[1/29]).$$

We obtain an element $s \in {}_{x'}G_x(\mathbb{Q})$ by composing two symmetries: the first one is s_y the symmetry about the hyperplane perpendicular to $y := (0,1,0)$ and the second one is the symmetry about the hyperplane perpendicular to the vector $x' - s_y(x)$. This gives

$$s = \frac{1}{181}\begin{pmatrix} 179 & -24 & 12 \\ 24 & 107 & -144 \\ 12 & 144 & 109 \end{pmatrix} \text{ in } {}_{x'}G_x(\mathbb{Z}[1/181]).$$

We get $181\mathbb{Z}^3 \subset ts^{-1}M \subset 181^{-1}\mathbb{Z}^3$ and we consider the lattice $ts^{-1}M + \mathbb{Z}^3$ inside $\frac{1}{181}\mathbb{Z}^3$. The image of the morphism of modules

$$181ts^{-1} \colon (\mathbb{Z}/181\mathbb{Z})^3 \to (\mathbb{Z}/181\mathbb{Z})^3$$

is generated by $\bar{u} = (\bar{-38}, \bar{1}, \bar{33}) \in (\mathbb{Z}/181\mathbb{Z})^3$. Let $u = (-38, 1, 33)$ be a lifting of $\bar{u}$ in $\mathbb{Z}^3$ with $\gcd(-38, 1, 33) = 1$. We extend u to a basis (u, v_2, v_3) of $\mathbb{Z}^3$, where $v_2 = (1,0,0)$ and $v_3 = (0,0,1)$. So we get a basis for $\mathbb{Z}^3 + ts^{-1}M$:

$$v_1 = (-38/181, 1/181, 33/181), \quad v_2 = (1,0,0), \quad v_3 = (0,0,1).$$

The quadratic form $\bar{Q} \colon (ts^{-1}M + \mathbb{Z}^3) \to \mathbb{Z}/181\mathbb{Z}$ is given by

$$(x,y,z) \mapsto 2/26x(x + 98y - 47z) \pmod{181}.$$

We get

$$ts^{-1}M = \ker((ts^{-1}M + \mathbb{Z}^3) \to \mathbb{Z}/181\mathbb{Z}, (x,y,z) \mapsto x + 98y - 47z \pmod{181})).$$

By substituting $x = 47z - 98y + 181k$, we get a basis for $ts^{-1}M$:

$$(-1786, 47, 1732)/181, (3905, -98, -3234)/181, (-6878, 181, 5973)/181,$$

and then via multiplication by st^{-1} a basis for M:

$$(-298,-64,257)/29,(647,130,-474)/29,(-1142,-233,879)/29.$$

By the LLL-algorithm, we get an (oriented) orthonormal basis for M:

$$(-24,11,-12)/29,(3,24,16)/29,(16,12,-21)/29.$$

This gives

$$y' = \begin{pmatrix} 23 & 15 & 4 \end{pmatrix} \frac{1}{29} \begin{pmatrix} -24 & 3 & 16 \\ 11 & 24 & 12 \\ -12 & 16 & -21 \end{pmatrix} = \begin{pmatrix} -15 & 17 & 16 \end{pmatrix}.$$

Bibliography

[1] M.F. Atiyah and I.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[2] M. Bhargava and B.H. Gross, *Arithmetic invariant theory*, arXiv 4 Aug 2012.

[3] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron Models*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer-Verlag, 1990.

[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, Grad. Texts Math., **138**, Springer-Verlag, 1993.

[5] M. DeLand, *Sum of Three Squares*, `http://www-personal.umich.edu/~madeland/teaching_files/math311/class_files/sum3squares.pdf`.

[6] C. F. Gauss, *Disquisitiones Arithmeticae*, English Edition, Springer-Verlag, 1986.

[7] P. Gille and L. Moret-Bailly, *Actions algébriques de groupes arithmétiques*, in “Torsors, étale homotopy and applications to rational points”, 231–249, London Math. Soc. Lecture Note Ser., 405, Cambridge Univ. Press, Cambridge, 2013, edited by V. Batyrev et A. Skorobogatov.

[8] J. Giraud, *Cohomologie non abélienne*, Die Grundlehren der mathematischen Wissenschaften, Band 179, Springer-Verlag, 1971.

[9] B. H. Gross, *Heights and the Special Values of L-series*, CMS Proceedings, Vol. 7, AMS, 1986, 115-187.

[10] A. Grothendieck, *A General Theory of Fibre Spaces with Structure Sheaf*, Report No. 4, University of Kansas, 1958.

[11] R. Hartshorne, *Algebraic Geometry*, Grad. Texts Math., **52**, Springer, 1977.

[12] F. Hirzebruch and D. Zagier, *Intersection numbers of curves on Hilbert modular surfaces and modular forms of Nebentypus*, Invent. Math. 36, 1976, 57–113.

[13] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford Grad. Texts Math., **6**, 2006.

[14] J.S. Milne, *Étale Cohomology*, Princeton University Press, **33**, 1980.

[15] J. Milnor and D. Husemoller, *Symmetric Bilinear Forms*, Ergebnisse der Mathematik und ihrer Grenzgebiete, **73**, Springer-Verlag, 1973.

[16] B. Poonen, *Rational Points on Varieties*, `http://www.math.mit.edu/poonen/papers/Qpoints.pdf`.

[17] J-P. Serre, *Cours d'arithmétique*, Le Mathématicien, Presses Universitaires de France, 4$^{\text{e}}$ tirage, 2013.

[18] G. Shimura, *Quadratic Diophantine Equations, the Class Number, and the Mass Formula*, Bulletin of the AMS, Volume 43, Number 3, July 2006.

[19] P. Stevenhagen, *Number Rings*, http://websites.math.leidenuniv.nl/algebra/ant.pdf.

[20] The CRing Project Authors, *The CRing Project*, https://math.berkeley.edu/~amathew/chcompletion.pdf.

[21] The Stacks Project Authors, *The Stacks Project*, http://stacks.math.columbia.edu.

[22] W.C. Waterhouse, *Introduction to Affine Group Schemes*, Grad. Texts Math., **66**, Springer-Verlag, 1979.

[23] D. Zagier, *Nombres de classes et formes modulaires de poids 3/2*, C. R. Acad. Sci. Paris Sér. A-B 281, 1975.

Summary

Gauss's theorem on sums of 3 squares relates the number of primitive integer points on the sphere of radius the square root of n with the class number of some quadratic imaginary order. In 2011, Edixhoven sketched a different proof of Gauss's theorem by using an approach from arithmetic geometry. He used the action of the special orthogonal group on the sphere and gave a bijection between the set of $\mathrm{SO}_3(\mathbb{Z})$-orbits of such points, if non-empty, with the set of isomorphism classes of torsors under the stabilizer group. This last set is a group, isomorphic to the group of isomorphism classes of projective rank one modules over the ring $\mathbb{Z}[1/2, \sqrt{-n}]$. This gives an affine space structure on the set of $\mathrm{SO}_3(\mathbb{Z})$-orbits on the sphere.

In Chapter 3 we give a complete proof of Gauss's theorem following Edixhoven's work and a new proof of Legendre's theorem on the existence of a primitive integer solution of the equation $x^2 + y^2 + z^2 = n$ by sheaf theory. In Chapter 4 we make the action given by the sheaf method of the Picard group on the set of $\mathrm{SO}_3(\mathbb{Z})$-orbits on the sphere explicit, in terms of $\mathrm{SO}_3(\mathbb{Q})$.

Samenvatting

De stelling van Gauss over sommen van 3 kwadraten relateert het aantal primitieve gehele punten op de bol van straal de vierkantswortel van n aan het klassengetal van een bepaalde imaginaire kwadratisch orde. In 2011 schetste Edixhoven een ander bewijs van deze stelling van Gauss met behulp van aritmetische meetkunde. Hij gebruikte de actie van de speciale orthogonale groep op de bol en gaf een bijectie tussen de verzameling van $\mathrm{SO}_3(\mathbb{Z})$-banen van dergelijke punten, als die niet leeg is, met de verzameling van isomorfie klassen van torsors onder de stabilisator groep. Deze laatste verzameling is een groep, isomorf met de groep van isomorfie klassen van projectieve rang één modulen over de ring $\mathbb{Z}[1/2, \sqrt{-n}]$. Dit geeft een affiene ruimte structuur op de verzameling van $\mathrm{SO}_3(\mathbb{Z})$-banen op de bol.

In Hoofdstuk 3 geven we een volledig bewijs van de stelling van Gauss zoals geschetst door Edixhoven, en een nieuw bewijs van Legendre's stelling over het bestaan van een primitieve gehele oplossing van de vergelijking $x^2 + y^2 + z^2 = n$ met schoven theorie. In hoofdstuk 4 maken we de werking gegeven door de schoven theorie van de Picard groep op de verzameling van $\mathrm{SO}_3(\mathbb{Z})$-banen op de bol expliciet, in termen van $\mathrm{SO}_3(\mathbb{Q})$.

Résumé

Le théorème de Gauss sur les sommes de 3 carrés relie le nombre de points entiers primitifs sur la sphère de rayon la racine carrée de n au nombre de classes d'un ordre quadratique imaginaire. En 2011, Edixhoven a esquissé une preuve du théoreme de Gauss en utilisant une approche de la géométrie arithmétique. Il a utilisé l'action du groupe orthogonal spécial sur la sphère et a donné une bijection entre l'ensemble des $\mathrm{SO}_3(\mathbb{Z})$-orbites de tels points, si non vide, avec l'ensemble des classes d'isomorphisme de torseurs sous le stabilisateur. Ce dernier ensemble est un groupe, isomorphe au groupe des classes d'isomorphisme de modules projectifs de rang 1 sur l'anneau $\mathbb{Z}[1/2, \sqrt{-n}]$, ce qui donne une structure d'espace affine sur l'ensemble des $\mathrm{SO}_3(\mathbb{Z})$-orbites sur la sphère.

Au chapitre 3 de cette thèse, nous donnons une démonstration complète du théorème de Gauss suivant les travaux d'Edixhoven. Nous donnons aussi une nouvelle preuve du théorème de Legendre sur l'existence d'une solution entière primitive de l'équation $x^2 + y^2 + z^2 = n$ en utilisant la théorie des faisceaux. Nous montrons au chapitre 4 comment obtenir explicitement l'action, donnée par la méthode des faisceaux, du groupe des classes sur l'ensemble des $\mathrm{SO}_3(\mathbb{Z})$-orbites sur la sphère en termes de $\mathrm{SO}_3(\mathbb{Q})$.

Acknowledgments

I express my gratitude to Aad van der Vaart, Hendrik Lenstra, Don Zagier, and Philippe Gille for their assessments of this thesis, and the last three of them for their nice suggestions to improve the quality of this work and for taking part in the defence. I also thank Elisa Lorenzo Garcia and Lenny Taelman for taking part in the defence.

I thank all my teachers for teaching me mathematics, how to do mathematics, and how to enjoy it. In the ALGANT program, my deepest thanks especially go to Bas Edixhoven and Qing Liu. I thank Christopher Niesen who has helped me a lot during my study in the ALGANT program.

I am grateful to my friends from the International church of Leiden, my graduate program, and my badminton club BC Leiden, especially: Pastor Andy/Helen, Paulina+Jérome+Pippa, Inge, Aaron, Erika, Stine, Liu+joy, Yuven, Bas+his family, Angelica, Jochem+Rongfang+Isa, Leah, Jesse, and Annemarie. They are like a family to me these days. Last but not least, I thank my family for their encouragements and support during difficult times.

Curriculum Vitae

Albert Gunawan was born on February 26, 1988 in Temanggung, Indonesia, where he also attended SMA N1 Temanggung high school. During this period he participated in some mathematical competitions, that enabled him to pursue the bachelor program of mathematics in Gadjah Mada University from 2006-2010.

In 2010 he was offered an Algant Masters scholarship to study at the Universiteit Leiden and the Université de Bordeaux. He studied in Leiden for the first year and spent his second year in Bordeaux. As a second year masters student he asked Prof. Qing Liu to supervise his masters thesis. He received his masters degree from the Algant program in the Summer of 2012.

In November 2011 he learned about the Algant-Doc program and of the topic of this thesis from Prof. Bas Edixhoven during a short visit to Bordeaux. He was admitted into the Algant-Doc joint PhD program starting September 2012 under the supervision of Bas Edixhoven and Qing Liu.