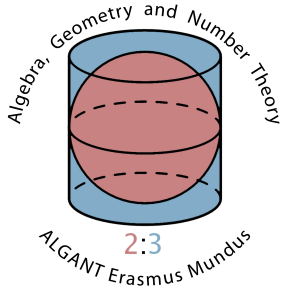


ERASMUS MUNDUS MASTER ALGANT

Universiteit Leiden

MASTER THESIS

On Gauss's 3 squares theorem by Bas Edixhoven

Author:
Albert GUNAWAN

Supervisor:
Prof. Qing LIU

July 10, 2012

Contents

1 Introduction

The area of arithmetic geometry is motivated by studying the questions in number theory through algebraic geometry, a viewpoint which was hinted at in the 19th century and which has been brought to fruition very successfully this century. Due to the variety of the techniques and theory required, it is an area which maintains deep interconnections with other branches of mathematics such as algebra, analysis and topology.

Arithmetics geometry has witnessed a lot of important results in past decades. Some of the better known examples include the proofs of the Mordell conjecture, Fermat's last Theorem and the modularity conjecture. With its powerful tools, arithmetic geometry also open possibilities to prove "old" theorem in number theory using new methods that possibly will simplify the proof and make better understanding of it.

There is one celebrated theorem by Gauss on quadratic forms in 3 variable that gives the number of integer solutions of the equation $x^2 + y^2 + z^2 = n$ for $n \geq 1$. Gauss formulated the solution it in terms of equivalence classes of quadratic forms. The proof that Gauss used is not easy to follow. Trying to understand Gauss's proof, Bas Edixhoven had an idea in terms of SO_3 as group scheme over $\mathbb{Z}$ and transporters between solutions. He relates the H^1 of the stabilizer to the relevant class group uses exact sequences of cohomology. It gives us elegant result and all the understanding that one could want. Recent development of the same approaches can be seen in the work of Shimura in the article *Quadratic diophantine equations, the class number, and the mass formula* [3]. Also recent work by Bhargava and Gross in their paper of *Arithmetic invariant theory* [4].

We start now with the definition of group scheme, follow with cohomology tools that we will use in the proof.

2 Group schemes

2.1 Group schemes

Group objects. Let C be a category with finite products: i.e., for any $n \geq 0$ and for any objects $G_1, \ldots, G_n$ of C, there is an objects G equipped with a morphism to each G_i such that any other object H equipped with a morphism to each G_i admits a unique morphism to G compatible with the morphisms $G \to G_i$. For $n = 0$, an empty product is the same thing as a terminal object of C, denoted by 1.

A group object in C is an object G equipped with morphisms $m : G \times G \to G$ (multiplication), $i : G \to G$ (inverse), and $e : 1 \to G$ (identity) satisfying group axiom as follows:

- Associativity

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{m \times id} & G \times G \\ \downarrow{\scriptstyle id \times m} & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{m} & G \end{array}$$

- Identity (left and right)

$$\begin{array}{ccc} 1 \times G & \xrightarrow{e \times id} & G \times G \\ & \searrow^{\simeq} & \downarrow{\scriptstyle m} \\ & & G \end{array}$$

and

$$\begin{array}{ccc} G \times 1 & \xrightarrow{id \times e} & G \times G \\ & \searrow^{\simeq} & \downarrow{\scriptstyle m} \\ & & G \end{array}$$

- Inverse (left and right)

$$\begin{array}{ccc} G & \xrightarrow{(i,id)} & G \times G \\ \downarrow & & \downarrow{\scriptstyle m} \\ 1 & \xrightarrow{e} & G \end{array}$$

and

$$\begin{array}{ccc} G & \xrightarrow{(id,i)} & G \times G \\ \downarrow & & \downarrow m \\ 1 & \xrightarrow{e} & G \end{array}$$

Example 2.1.1

- *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.*

Definition 2.1.2 *A* group scheme *G over a scheme S is a group object in the category of S-schemes.*

In the category of S-schemes, products are fiber products over S, and the terminal object is the S-scheme S. So, for example, a homomorphism of group schemes $G \to H$ over S is an S-morphism respecting the multiplication morphisms m_G and m_H, that is, an S-morphism $\phi : G \to H$ making

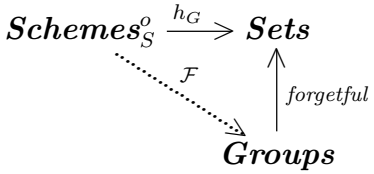
$$\begin{array}{ccc} G \times_S G & \xrightarrow{m_G} & G \\ {\scriptstyle (\phi,\phi)}\downarrow & & \downarrow{\scriptstyle \phi} \\ H \times_S H & \xrightarrow{m_H} & H \end{array}$$

commute.

Definition 2.1.3 *A* subgroup scheme *of a group scheme G is a group scheme H that is also a closed subscheme of G, and for which the inclusion $H \to G$ is a homomorphism.*

Using Yoneda's lemma one can obtain an equivalent definition of group scheme that is perhaps closer to geometric intuition:

Proposition 2.1.4 *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. Equivalently, making G group scheme over S is equivalent to giving a functor $\mathcal{F} : \boldsymbol{Schemes}_S^o \to \boldsymbol{Groups}$ completing the commutative diagram*



Homomorphisms of group schemes and group scheme actions can be described similarly. For example, giving a right action of a group scheme G on an S-scheme X is equivalent to giving a collection of compatible group actions $X(T) \times G(T) \to X(T)$ (in the category of sets), one for each S-scheme T.

Various properties are also conveniently 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.

Example 2.1.5

- *Let G be a group, and let S be a scheme. For each $\sigma \in G$, let S_σ be a copy of S. Then $\coprod_{\sigma \in G} S_\sigma$ can be made a group scheme over S, by letting m map $S_\sigma \times_S S_\tau$ isomorphically to $S_{\sigma\tau}$ for each $\sigma, \tau \in G$. This is called a constant group scheme.*

- *An elliptic curve over a field k is a group scheme of finite type over k.*

2.2 Affine group schemes

Definition. Throughout this subsection let k be a ring, R be any commutative k-algebra with unity. A group in the category of schemes over k is called a group scheme over k. When the underlying scheme is affine, it is called an affine group scheme over k. Because the affine schemes form a full subcategory of the category of all schemes, so we have following:

Definition 2.2.1 *An* affine group scheme $G = SpecA \to S = Speck$ *is a group object in the category of affine scheme over k.*

By Proposition 2.1.4 we have a functor from the category of affine schemes over k to the category of set that gives a group structure on

$$G(R) = \mathrm{Mor}(\mathrm{Spec}R,\ \mathrm{Spec}A) \simeq \mathrm{Hom}_k(A,R).$$

Let us see some examples to make it clear. Define a group $G(R)$=$SL_2(R)$ under multiplication by the set of 2×2 matrices with entries in R and determinant 1 (unity in R), for each k-algebra R. Now if $\phi : R \to S$ is an k-algebra homomorphism, it induces in every case a group homomorphism $G(R) \to G(S)$; for instance $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in $SL_2(R)$, then $\begin{pmatrix} \phi(a) & \phi(b) \\ \phi(c) & \phi(d) \end{pmatrix}$ is in $SL_2(S)$, since its determinant is $\phi(a)\phi(d)-\phi(b)\phi(c) = \phi(ad-bc) = \phi(1) = 1$. If we then take some $\psi : S \to T$, the map induced by $\psi \circ \phi$ is the composite $G(R) \to G(S) \to G(T)$. Finally and most trivially, the identity map on R induces the identity map on $G(R)$. These are summed up by saying that G is a functor from the category of k-algebras to the category of groups.

In most cases, we will consider functors G that defined by finitely many polynomial equations with coefficient in k. For example here, $SL_2(R)$ are given by quadruples a, b, c, d in R satisfying the equation $ad - bc = 1$. Now we try to recover A, take a polynomial ring over k with one indeterminate for each variable in the equations. Divide by the ideal generated by the relations which the equations express. Here

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

Let $G(R)$ be given by the solutions of the equations in R. Any k-algebra homomorphism $\phi : A \to R$ will take our "general" solution to a solution in R corresponding to an element of $G(R)$. Since ϕ is determined by where it sends the indeterminates, we have an injection of $\mathrm{Hom}_k(A, R)$ into $G(R)$. But since the solution is as general as possible, this is actually bijective. Thus for this A we have a natural correspondence between $G(R)$=$SL_2(R)$ and $\mathrm{Hom}_k(A, R)$.

If there is such A for our functor G, we call G is representable or one says that A represent G. This is one of equivalent definition of affine group scheme over k as a representable functor from the category of k-algebras to the category of groups.

Theorem 2.2.2 *Let E and F be functors represented by k-algebras A and B. The natural maps between functors $E \to F$ correspond to k-algebra homomorphisms $B \to A$.*

Proof Let $\phi : B \to A$ be given. An element in $E(R)$ corresponds to a homomorphis $A \to R$, and the composition $B \to A \to R$ then defines an element in $F(R)$. This clearly gives a natural map $E \to F$.

Conversely, let $\Psi : E \to F$ be a natural map. Inside $E(A)$ is our "most general possible" solution, coressponding to the identity map $\mathrm{id}_A : A \to A$. Applying Ψ to it, we get an element of $F(A)$, that is, a homomorphism $\phi : B \to A$. Since any element in any $E(R)$ comes from a homomorphism $A \to R$, and

$$\begin{array}{ccc} E(A) & \to & E(R) \\ \downarrow & & \downarrow \\ F(A) & \to & F(R) \end{array}$$

commutes, we obtain Ψ is precisely the map defined from ϕ in the first step.

Hopf algebras. Our definition of affine group scheme is of mixed nature: we have an algebra A together with group structure on the corresponding functor. Using theorem 2.2.2 we can turn that structure into something involving A.

We will need two small facts about representability. First, the functor E assigning just one point to every k-algebra R is represented by k itself. Second, suppose that E and F are represented by A and B; then the product

$$(E \times_k F)(R) = \{\langle e, f\rangle |\ e \in E(R),\ f \in F(R)\}$$

is represented by $A \otimes_k B$. Indeed, this merely says that homomorphisms $A \otimes_k B \to R$ correspond to pairs of homomorphisms $A, B \to R$, which is a familiar property of tensor products. We can even generalize slightly. Suppose we have some G represented by C and natural maps $E \to G, F \to G$ corresponding to $C \to A, C \to B$. Then the fiber product

$$(E \times_G F)(R) = \{\langle e, f\rangle | e \text{ and } f \text{ have the same image in } G(R)\ \}$$

is represented by $A \otimes_C B$.

Then the morphism m, i, and e correspond to R-algebra homomorphisms with their own names,

- comultiplication

$$\triangle : A \to A \otimes_k A$$

- counit (augmentation)
$$\epsilon : A \to k$$
- coinverse (antipode)
$$S : A \to A$$

such that the diagrams

$$\begin{array}{ccc} A \otimes_k A \otimes_k A & \xleftarrow{\triangle \otimes id} & A \otimes_k A \\ \uparrow{\scriptstyle id \otimes \triangle} & & \uparrow{\scriptstyle \triangle} \\ A \otimes_k A & \xleftarrow{\triangle} & A \end{array}$$

,

$$\begin{array}{ccc} k \otimes_k A & \xleftarrow{\epsilon \otimes id} & A \otimes_k A \\ \uparrow{\scriptstyle \simeq} & & \uparrow{\scriptstyle \triangle} \\ A & \xleftarrow{=} & A \end{array}$$

and

$$\begin{array}{ccc} A & \xleftarrow{(S,id)} & A \otimes_k A \\ \uparrow & & \uparrow{\scriptstyle \triangle} \\ k & \xleftarrow{\epsilon} & A \end{array}$$

commute. A k-algebra A with specified maps $\triangle, \epsilon, S$ satisfying these conditions we will call a Hopf algebra.

Base change/extension of scalars. We originally chose our base ring k somewhat arbitrarily, requiring only that the defining equations make sense in k. Suppose now that we take a ring homomorphism $k \to k'$; this could be mean expanding k, or it could mean reading the equations modulo some ideal. Any k'-algebra S becomes a k-algebra by $k \to k' \to S$, and k'-algebra homomorphisms are k-algebra homomorphisms for this structure. Any functor F on the category of k-algebras can thus be evaluated on such S and gives us a functor $F_{k'}$ on the category of k'-algebras.

Suppose now that F is represented by the k-algebra A, so the elements of $F(R)$ correspond to k-algebra maps $A \to R$. If S is a k'-algebra, it is

a standard fact that $\mathrm{Hom}_{k'}(A \otimes_k k', S) \simeq \mathrm{Hom}_k(A, S)$. Thus base change goes over to tensor product, and $F_{k'}$ is represented by $A' = A \otimes_k k'$. If for instance A is $k[a,b,c,d]/(ad-bc-1)$, then A' is $k'[a,b,c,d]/(ad-bc-1)$, and in general A' is the algebra over k' coming from the same equations as A.

Affine subgroup and homomorphisms. A homomorphism of affine group schemes is a natural map $G \to H$ for which each $G(R) \to H(R)$ is a homomorphism. Let $\phi : H' \to G$ be a homomorphism. If the corresponding algebra map $B' \leftarrow A$ is surjective, we call ϕ a closed embedding. It is an isomorphism of H' onto a closed subgroup H of G represented by a ring B (isomorphic to B') which is a quotient of A with some ideal I of A. Moreover if $H'(R)$ is a subgroup of $G(R)$ for any k-algebra R, we say that H' is affine subgroup of G.

Kernel of homomorphisms. We will see a special case of affine subgroup that is occured from homomorphisms of affine group schemes. If $\phi : G \to H$ is any homomorphism, then $N(R) = \ker[G(R) \to H(R)]$ is a group functor, the kernel of ϕ. The elements of $N(R)$ can be described as the pairs in $G(R) \times \{e\}$ having the same image in $H(R)$; that is, $N = G \times_H 1$. Hence if G and H are represented by A and B, we know that N will be represented by $A \otimes_B k$.

2.3 Some important examples of affine group schemes

Throughout this subsection let k be a ring, R be any commutative k-algebra with unity.

Additive group. Let $\mathbb{G}_a$ be the functor sending a k-algebra R to itself considered as an additive group, i.e., $\mathbb{G}_a(R) = (R, +)$. Then $\mathbb{G}_a$ is represented just by the polynomial ring $A = k[X]$. Here $\triangle, \epsilon$, and S worked out as follows: Let $g, h : A \to R$ be homomorphisms with $g(X) = r$ and $h(X) = s$. We need $\triangle : A \to A \otimes_k A$ such that $(g,h)\triangle : A \to A \otimes_k A \to R$ sends X to $r + s$. Clearly $\triangle(X) = X \otimes_k 1 + 1 \otimes_k X$ has this property, and it must then be the map we want, since the correspondence is bijective. Similarly the map $\epsilon : A \to k$ must make $A \to k \to R$ give the identity element 0 of $\mathbb{G}_a(R)$; hence $\epsilon(X) = 0$. Finally, when $g(X) = r$, we must have $g \circ S(X) = -r$; hence $S(X) = -X$.

Multiplicative group. Let $\mathbb{G}_m$ be the functor $R \to R^\times$. Each $a \in R^\times$ has a unique inverse, and so $\mathbb{G}_m(R) \simeq \{(a,b) \in R^2 | ab = 1\}$. Therefore $\mathbb{G}_m$

is represented by $A = k[X,Y]/(XY-1)$, which may sometimes write as $k[X,1/X]$. The structure for $\mathbb{G}_m$ is equally simple: on $A = k[X,1/X]$ we have $\triangle(X) = X \otimes_k X$ and $\epsilon(X) = 1$ and $S(X) = 1/X$.

Root of unity. For an integer $n \geq 1$, the functor $R \to \mu_n(R) = \{r \in R | r^n = 1\}$ sending any k-algebra R to a subgroup of multiplicative group $\mathbb{G}_m$. Moreover it is an affine group scheme represented by $A = k[X]/(X^n - 1)$. We can see also μ_n as a kernel of homomorphism of affine groups $[n] : \mathbb{G}_m \to \mathbb{G}_m$ given in coordinates by $t \mapsto t^n$. Here $A = k[X,1/X]$ and $B = k[Y,1/Y]$, and the homomorphism sends Y to X^n.

Special linear group. For $n \times n$ matrices M and N with entries in a k-algebra R, we have from Cramer's rule

$$\det(MN) = \det(M).\det(N) \qquad \text{adj}(M).\text{M} = \det(M).I = M.\text{adj}(M)$$

where I denotes the identity matrix. Therefore, there is a functor SL_n sending a k-algebra R to the group of $n \times n$ matrices of determinant 1 with entries in R. Moreover, SL_n is represented by

$$A = k[X_{11}, X_{12}, \ldots, X_{nn}]/(\det(X_{ij})\text{-}1).$$

General linear group. Similar arguments above show that the $n \times n$ matrices with entries in a k-algebra R and with determinant a unit in R form a group $GL_n(R)$, and that $R \to GL_n(R)$ is a functor represented by

$$A = k[X_{11}, X_{12}, \ldots, X_{nn}, Y]/(\det(X_{ij})Y\text{-}1).$$

Orthogonal and special orthogonal group. Let V be a finitely generated free k-module with rank n, and let φ be a nondegenerate symmetric bilinear form $V \times V \to k$. We then put $\varphi[x] = \varphi(x,x)$ for $x \in V$, thus using the same letter φ for the quadratic form and the corresponding symmetric form. By a quadratic Diophantine equation we mean an equation of the type $\varphi[x] = q$ with a given $q \in k^\times$. In particular, in the classical case with $k = \mathbb{Q}$ and $V = \mathbb{Q}^n$, we usually assume that φ is $\mathbb{Z}$-valued on $\mathbb{Z}^n$ and $q \in \mathbb{Z}$. We define the orthogonal group $O_n(\varphi)$ and the special orthogonal group $SO_n(\varphi)$ by

$$O_n(\varphi)(R) = \{\alpha \in GL_V(R) \mid \varphi(\alpha v, \alpha w) = \varphi(v,w) \text{ for all } v, w \in R \otimes_k V\},$$
$$SO_n(\varphi)(R) = O_n(\varphi)(R) \cap SL_V(R).$$

The choice of a basis for V defines a functor $O_n(\varphi)$ and $SO_n(\varphi)$ that are represented by quotient of $A = k[X_{11}, X_{12}, \ldots, X_{nn}, Y]$ by the ideal generated by the polynomials

$$\Sigma_{j,k} c_{jk} X_{ji} X_{kl} - c_{il}, \qquad i, l = 1, \cdots, n$$

also $\det(X_{ij})Y$-1, and by quotient of $B = k[X_{11}, X_{12}, \ldots, X_{nn}]$ by the ideal generated by the polynomials

$$\Sigma_{j,k} c_{jk} X_{ji} X_{kl} - c_{il}, \qquad i, l = 1, \cdots, n$$

also $\det(X_{ij})$-1 respectively. Where $C = (c_{il})$ is the gramm matrix of the bilinear form. Or equivalently we have

$$O_n(\varphi)(R) = \{T \in GL_n(R) \mid T^t.C.T = C\},$$
$$SO_n(\varphi)(R) = \{T \in GL_n(R) \mid T^t.C.T = C, \det(T) = 1\}.$$

Finite constant group scheme. Let G be a finite group. The functor assigning G to every algebra cannot be defined by a family of equations, but something close to it can be. Let A be k^G, the functions from G to k. Let e_σ has value 1 on σ and 0 on the other elements; then $\{e_\sigma\}$ is a basis of A. As a ring A is just $k \times \cdots \times k$: we have $e_\sigma^2 = e\sigma$ and $e_\sigma e_\tau = 0$ and $\Sigma e_\sigma = 1$. Suppose now R is a k-algebra with no idempotents except 0 and 1. Then a homomorphism $\phi : A \to R$ must send one e_σ to 1 and the others to 0. Thus these homomorphisms correspond to elements of G.

Defining $\triangle(e_\rho) = \Sigma_{\rho=\sigma\tau}\ (e_\sigma \otimes e_\tau)$ gives us a structure on A for which the induced multiplication of the homomorphisms above matches up with the multiplication in G. For coassociativity, note that $\triangle$ is simply the map from k^G to $k^{G\times G} \simeq k^G \otimes k^G$ induced by $m : G \times G \to G$. Letting $S(e_\sigma)$ be $e_{(\sigma^{-1})}$, with $\epsilon(e_\sigma)$ equal to 1 when σ is the unit and 0 otherwise, we in fact get a Hopf algebra. The group scheme thus defined is called the constant group scheme for G, again denoted by G if no confusion is likely.

2.4 Weil restriction/Restriction of the base ring

Let k' be a k algebra, where again k is a commutative ring. For an affine k'-group G, we want to construct an affine k-group denoted by $\mathrm{Res}_{k'/k}(G)$ whose arithmetic over k mimics the arithmetic of G over k'. In particular we want a bijection $\mathrm{Res}_{k'/k}(G)(k) \simeq G(k')$. We will use a functor to reach our goal, i.e. we let $(G)_{k'/k}$ denote the functor

$$R \to G(k' \otimes_k R)\colon \mathrm{Alg}_k \to \mathrm{Grp}.$$

Proposition 2.4.1 *Assume that k' is finitely generated and free as a k-module. For all affine k'-groups G, the functor $(G)_{k'/k}$ is an affine k-group; moreover, for all affine k-groups H and affine k'-groups G, there are canonical isomorphisms*

$$Hom_k(H,(G)_{k'/k}) \simeq Hom_{k'}(H_{k'},G),$$

natural in both H and G.

In other words, $G \to (G)_{k'/k}$ is a functor from affine k'-groups to affine k-groups which is right adjoint to the functor "extension of the base ring" $k \to k'$. The affine group $(G)_{k'/k}$ is said to have been obtained from G by (Weil) restriction of scalars or by restriction of the base ring, and $(G)_{k'/k}$ is called the Weil restriction of G.

Proof We first explain the existence of a right adjoint for functors to sets. From a functor $F\colon \mathrm{Alg}_k \to \mathrm{Set}$ we obtain a functor $F_{k'}\colon \mathrm{Alg}_{k'} \to \mathrm{Set}$ by setting $F_{k'}(R)=F(R)$. On the other hand, from a functor $F'\colon \mathrm{Alg}_{k'} \to \mathrm{Set}$ we obtain a functor $(F')_{k'/k}\colon \mathrm{Alg}_k \to \mathrm{Set}$ by setting $(F')_{k'/k}(R)=F'(k' \otimes R)$. Let ϕ be a natural transformation $\phi : F_{k'} \to F'$. The homomorphism

$$F(R) \xrightarrow{F(r \mapsto 1 \otimes r)} F(k' \otimes R) \xrightarrow{\phi(k \otimes R)} F'(k' \otimes R) = (F')_{k'/k}(R)$$

are natural in the k-algebra R, and so their composite is a natural transformation $F \to (F')_{k'/k}$. Thus we have a morphism

$$\mathrm{Hom}\ (F_{k'}, F') \to \mathrm{Hom}\ (F,(F')_{k'/k}).$$

This has an obvious inverse. Given $F \to (F')_{k'/k}$, we need a map $F_{k'} \to F'$. Let R be a k'-algebra, and let R_0 be R regarded as a k-algebra. The given k-algebra map $k' \to R$ and the identity map $R_0 \to R$ define a map $k' \otimes_k R_0 \to R$ (of k'-algebras). Hence we have a map

$$F(R_0) \to F'(k' \otimes_k R_0) \to F'(R),$$

and $F(R_0)=F_{k'}(R)$. Thus we get a bijection.

We have shown that the extension of scalars functor $F \to F_{k'}$ has a right adjoint $F' \to (F')_{k'/k}$:

$$\mathrm{Hom}(F_{k'}, F') \simeq \mathrm{Hom}(F, (F')_{k'/k}).$$

Lemma 2.4.2 *Assume that k' is finitely generated and free as a k-module. If $F : Alg_{k'} \to Set$ is represented by a k-algebra, then so also is $(F')_{k'/k}$.*

Proof Let $k' = ke_1 \oplus \cdots \oplus ke_d$, $e_i \in k'$. Consider first the case that $F = \mathbb{A}^n$, so that $F(R)=R^n$ for all k'-algebras R. For any k-algebra R,

$$R' = k' \otimes R \simeq Re_1 \oplus \cdots \oplus Re_d,$$

and so there is a bijection

$$(a_i)_{1\le i\le n} \mapsto (b_{ij})_{\substack{1\le i\le n\\ 1\le j\le d}} : (R')^n \to R^{nd}$$

which sends (a_i) to the family (b_{ij}) defined by the equations

$$a_i = \sum_{j=1}^{d} b_{ij}e_j, \qquad i = 1, \dots, n.$$

The bijection is natural in R, and shows that $(F)_{k'/k} \simeq \mathbb{A}^{nd}$ (the isomorphism depends only on the choice of the basis $e_1, \dots, e_d$).

Now suppose that F is the subfunctor of $\mathbb{A}^n$ defined by a polynomial $f(X_1, \dots, X_n) \in k'[X_1, \dots, X_n]$. On substituting

$$X_i = \sum_{j=1}^{d} Y_{ij}e_j$$

into f, we obtain a polynomial $g(Y_{11}, Y_{12}, \dots, Y_{nd})$ with the property that

$$f(a_1, \dots, a_n) = 0 \iff g(b_{11}, b_{12}, \dots, b_{nd}) = 0.$$

The polynomial G has coefficients in k', but we can write it (uniquely) as a sum

$$g = g_1e_1 + \cdots + g_de_d, \qquad g_i \in k[Y_{11}.Y_{12}, \dots, Y_{nd}].$$

Clearly,

$$g(b_{11}, b_{12}, \dots, b_{nd}) = 0 \iff g_i(b_{11}, b_{12}, \dots, b_{nd}) = 0 \quad \text{for } i = 1, \dots, d,$$

and so $(F)_{k'/k}$ is isomorphic to the subfunctor of $\mathbb{A}^{nd}$ defined by the polynomials $g_1, \dots, g_d$.

This arguments extends in an obvious way to the case that F is the subfunctor of $\mathbb{A}^n$ defined by a finite set of polynomials, and even to the case that it is a subfunctor of an infinite dimensional affine space defined by infinitely many polynomials.

If G is a functor $\mathrm{Alg}_{k'} \to \mathrm{Grp}$, then $(G)_{k'/k}$ is a functor $\mathrm{Alg}_k \to \mathrm{Grp}$. This lemma also shows that if G is an affine group or an affine algebraic group, then so also is $(G)_{k'/k}$, and the functor $G' \to (G)_{k'/k}$ is right adjoint to the functor "extension of scalars".

Later we will compute Weil restriction for multiplicative group $\mathbb{G}_m$. To make the computation easier, we need to recall what is norm map between algebras.

Norm maps. Let $k \subset k'$ be an extension of rings such that k' is free of finite rank n as an k-algebra. This means that there exist $e_1, \ldots, e_n \in k'$ that form an k-basis for k'

$$k' = k.x_1 \oplus k.x_2 \oplus \cdots \oplus k.x_n.$$

For $x \in k'$, let $M_x : k' \to k'$ denote the k-linear multiplication map $y \mapsto x.y$. If we choose an k-basis for k', this map can be described by an $n \times n$-matrix with coefficients in k. We define the norm from k' to k by

$$N_{k'/k}(x) = \det M_x.$$

It is immediate from this definition that the norm map is a multiplication map.

Example 2.4.3 *Let $O = \mathbb{Z}[1/2, r]/(r^2 + n)$, recall that we do not suppose that n is square free, hence O is a possibly non-maximal order. We let T denote the groupscheme over $\mathbb{Z}[1/2]$ obtained by restriction of scalars from O to $\mathbb{Z}[1/2]$ applied to $\mathbb{G}_{m,O}$ (the multiplicative group scheme $\mathbb{G}_m$ over Spec O):*

$$T = Res_{O/\mathbb{Z}[1/2]}\mathbb{G}_{m,O}.$$

As a $\mathbb{Z}[1/2]$-algebra, O is free with basis $(1, r)$. Now for any $\mathbb{Z}[1/2]$-algebra R, we have:

$$T(R) = Res_{O/\mathbb{Z}[1/2]}\mathbb{G}_{m,O}(R) = \mathbb{G}_{m,O}(O \otimes_{\mathbb{Z}[1/2]} R) = \mathbb{G}_{m,O}(R \oplus R.r) = (R \oplus R.r)^*.$$

For $a, b \in R$, the norm of the element $a + br$ of $R \oplus R.r$ is $a^2 + nb^2$, and $a + br$ is invertible in $R \oplus R.r$ if and only if $a^2 + nb^2$ is a unit in R. Hence T is the spectrum of $\mathbb{Z}[1/2, a, b, 1/(a^2 + nb^2)]$, with group law given by the multiplication in O. Furthermore the norm map $T(R) = (R \oplus R.r)^* \to R^* = \mathbb{G}_{m,\mathbb{Z}[1/2]}(R)$

induces a morphism of group scheme (because norm map is multiplicative so functorialy it is commute with product of the groups):

$$Norm : T \to \mathbb{G}_{m,\mathbb{Z}[1/2]}.$$

We let T_1 *denote the kernel of this norm morphism:*

$$T_1 = ker(Norm : T \to \mathbb{G}_{m,\mathbb{Z}[1/2]}).$$

Likewise, T_1 *is the spectrum of* $\mathbb{Z}[1/2, a, b]/(a^2 + nb^2 - 1)$.

3 Étale topology and cohomology

3.1 Étale morphisms

Throughout this subsection otherwise it is stated, our rings are Noetherian and that our schemes are locally Noetherian.

An étale morphism is the analogue in algebraic geometry of a local isomorphism of manifolds in differential geometry, a covering of Riemann surfaces with no branch point in complex analysis, and an unramified extension in algebraic number theory.

Flat morphism. Recall that a homomorphism of rings $A \to B$ is flat if the functor $M \to B \otimes_A M$ from A-modules to B-modules is exact. One also says that B is a flat A-algebra. To check that $f : A \to B$ is flat, it suffices to check that the local homomorphism $A_{f^{-1}(m)} \to B_m$ is flat for every maximal ideal m in B. For such a morphism, the family of fibers X_y for $y \in Y$, is in some sense a "continuous family".

If A is an integral domain, then $x \mapsto ax : A \to A$ is injective for all nonzero a. Therefore, so also is $x \mapsto ax : B \to B$ for any flat A-algebra B, and it follows that $A \to B$ is injective.

A morphism $\varphi : Y \to X$ of schemes is flat if the local homomorphisms $O_{X,\varphi(y)} \to O_{Y,y}$ are flat for all $y \in Y$. The remark following the definition of flatness shows that it suffices to check this for the closed points $y \in Y$.

Example 3.1.1 *The structural morphism $A \to$ Speck of an algebraic variety over a field k is flat. Indeed, any algebra over a field is flat over the field.*

Example 3.1.2 *Let Z be a closed subscheme of X. Then the inclusion $Z \hookrightarrow X$ will be flat if and only if Z is also open in X (and so is a connected component of X).*

Proposition 3.1.3 *The following properties are true:*

- *Open immersions are flat morphisms.*
- *Flat morphisms are stable under base change.*
- *The composition of flat morphisms is flat.*
- *The fibered product of two flat morphisms is flat.*

- *Let $A \to B$ be a ring homomorphism. Then Spec$B \to$ Spec$A$ is flat if and only if $A \to B$ is flat.*

Proof See [5] section 4.3, proposition 3.3. for the proof.

A flat homomorphism $A \to B$ is *faithfully flat* if it is satisfies one of the following equivalent conditions:

- if an A-module M is nonzero, then $B \otimes_A M$ is nonzero;
- if a sequence of A-modules $M' \to M \to M''$ is not exact, then neither is $B \otimes_A M' \to B \otimes_A M \to B \otimes_A M''$;
- the map Spec$B \to$ Spec$A$ is surjective.

We will state the following proposition that will be useful to prove some presheaves on X_{et} are sheaves.

Proposition 3.1.4 *For any faithfully flat homomorphism $A \to B$, the sequence*

$$0 \to A \to B \xrightarrow{b \mapsto 1 \otimes b - b \otimes 1} B \otimes_A B$$

is exact.

Proof Step 1: The statement is true if $f : A \to B$ admits a section, i.e., a homomorphism $s : B \to A$ such that $s \circ f = \text{id}$.

To prove this, let $k : B \otimes_A B \to B$ send $b \otimes b' \mapsto b.fs(b')$. Then

$$k(1 \otimes b - b \otimes 1) = fs(b) - b.$$

Thus, if $1 \otimes b - b \otimes 1 = 0$, then $b = fs(b) \in f(A)$.

Step 2: If the statement is true for $a' \mapsto a' \otimes 1 : A' \to A' \otimes_A B$, where $A \to A'$ faithfully flat homomorphism, then it is true for $A \to B$.

The sequence for $A' \to A' \otimes B$ is obtained from that for $A \to B$ by tensoring with A'.

Step 3: The homomorphism $b \mapsto b \otimes 1 : B \to B \otimes_A B$ has a section, namely, the map $b \otimes b' \mapsto bb'$.

Since, by assumption, $A \to B$ is faithfully flat, this completes the proof.

Unramified and étale morphisms. A local homomorphism $f : A \to B$ of local rings is unramified if $B/f(m_A)B$ is a finite separable field extension of A/m_A and is essentially of finite type. (i.e. $B = S^{-1}A[t_1, ..., t_n]$ for some variables $t_1, ..., t_n$) This agrees with the definition in algebraic number theory where one only considers discrete valuation rings.

A morphism $\varphi : Y \to X$ of (locally Noetherian) schemes is unramified if it is of finite type and if the maps $O_{X,\varphi(y)} \to O_{Y,y}$ are unramified for all $y \in Y$. It suffices to check the condition for the closed points y of Y.

Example 3.1.5 *Let L/K be a finite field extension. Then Spec$L \to$ Spec$K$ is unramified if and only if the extension L/K is separable.*

Example 3.1.6 *Let L/K be an extension of number fields, and let O_L, O_K be their respective rings of integers. For any prime ideal $\mathfrak{q}$ of O_L, setting $\mathfrak{p} = \mathfrak{q} \cap O_K$, the extension $k(\mathfrak{q})$ of $k(\mathfrak{p})$ is separable. The morphism SpecO_L $\to$ SpecO_K is unramified at a prime ideal $\mathfrak{q}$ of O_L if and only if $\mathfrak{q}(O_L)_\mathfrak{q}$ is generated by $\mathfrak{p} = \mathfrak{q} \cap O_K$. It is therefore the usual definition of unramifiedness from algebraic number theory.*

Proposition 3.1.7 *Let $f : Y \to X$ be a morphism of finite type. Then f is unramified if and only if for every $y \in X$, the fiber Y_y is finite and if $k(x)$ is separable over $k(y)$ for every $x \in Y_y$.*

Proof See [5] section 4.3, proposition 3.20. for the proof.

A morphism of finite type $\varphi : Y \to X$ of schemes is *étale* if it is flat and unramified.

Let $X =$ Spec$A$ where A is an integral domain. For any proper ideal $\mathfrak{a} \subset A$, the map $Z \hookrightarrow X$ corresponding to the homomorphism $A \to A/\mathfrak{a}$ is unramified, but not flat, and hence not étale. This agrees with intuition of "étale" meaning "local isomorphism": the inclusion of a proper closed submanifold into a connected manifold is not a local isomorphism.

Example 3.1.8 *Let k be a field, let $P(T) \in k[T]$ a monic polynomial, and $X =$ Spec $k[T]/(P)$. Then a point $x \in X$ corresponds to an irreducible factor $Q(T)$ of $P(T)$. The canonical morphism $X \to$ Spec k is étale at x if and only if $Q(T)$ is a separable polynomial (i.e., without multiple root in the algebraic closure of k) and if $Q(T)$ is a simple factor of $P(T)$.*

Proposition 3.1.9 *The following proposition are true.*

- *Any closed immersion is an unramified morphism.*
- *Any open immersion is an étale morphism.*
- *Unramified morphims and étale morphims are stable under base change, composition, and fibered products.*

Proof See [5] section 4.3, proposition 3.22. for the proof.

Roughly speaking, étale morphisms have all the properties suggested by the analogy with local isomorphisms. Here is another list of important properties.

Proposition 3.1.10 *Let $\varphi : Y \to X$, $\psi : Z \to Y$ be étale morphisms.*

- *For all $y \in Y, O_{Y,y}$ and $O_{X,x}$ have the same Krull dimension.*
- *If $\varphi \circ \psi$ and φ are étale, then so also is ψ.*
- *The morphism φ is quasi finite.*
- *The morphism φ is open.*

When X and Y are connected varieties, the first properties says that they have the same dimension. The second one says that the fibres of φ are all finite. And the last statement follows from the more general fact that flat morphisms of finite type are open.

3.2 Grothendieck (pre)topologies

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.

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 to 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.

Definition 3.2.1 *Let $\mathfrak{C}$ be a category. We consider all familes of morphisms $\{U_i \to U\}_{i\in I}$ in $\mathfrak{C}$ having a common target. A* Grothendieck (pre)topology *on $\mathfrak{C}$ is a set τ whose elements are some of these families (the families that do belong to τ are called open coverings), satisfying the following axioms:*

- *Isomorphisms are open coverings: If $U' \to U$ is an isomorphism, then one-element family $\{U' \to U\}$ belongs to τ.*
- *An open covering of an open covering is an open covering: If $\{U_i \to U\}$ belongs to τ, and $\{V_{ij} \to U_i\}$ belongs to τ for each i, then the $\{V_{ij} \to U\}$ belongs to τ.*
- *A base extension of an open covering is an open covering: If $\{U_i \to U\}$ belongs to τ, and $V \to U$ is a morphism, then the fiber products $\{V \times_U U_i \to V\}$ belong to τ.*

Note that Grothendieck (pre)topology gives rise to a Grothendieck topology, and all the Grothendieck topologies we will use arise this way. So from now on, we will abuse terminology and call a pretopology a topology.

Definition 3.2.2 *A pair $(\mathfrak{C}, \tau)$ where τ is a Grothendieck topology on a category $\mathfrak{C}$ is called a* site.

The Zariski site. Let X be a topological space. Let $\mathfrak{C}$ be the category whose objects are the open sets in X, and such that for any $U, V \in \mathfrak{C}$,

$$\mathrm{Hom}(U,V) = \begin{cases} \{i\} & \text{if } U \subset V, \text{ and } i : U \to V \text{ is the inclusion} \\ \emptyset & \text{otherwise.} \end{cases}$$

Let τ be the collection of families $U_i \to U$ such that $\bigcup_i U_i = U$. Then τ is a Grothendieck topology on $\mathfrak{C}$, called the classical Grothendieck topology.

Let X be a scheme. The (small) Zariski site X_{Zar} is the site associated to the underlying topological space $\mathrm{sp}(X)$.

The (small) étale site. Fix a scheme X. Take $\mathfrak{C}$ to be the category Ét_X whose objects are the étale morphism $U \to X$, and in which morphisms are X-morphisms $U \to V$. (These will automatically étale by proposition 3.1.10.) Call a family $\{\phi_i : U_i \to U\}$ of morphisms in $\mathfrak{C}$ an open covering if $\bigcup_i \phi_i(U_i)=U$ as topological spaces. This defines (small) étale site X_{et}.

Remark that for the big étale site, one would take $\mathfrak{C}$=Schemes$_X$. Open coverings are defined as families of étale morphisms $\{\phi_i : U_i \to U\}$ such that $\bigcup_i \phi_i(U_i)=U$.

Morphisms of sites.

Definition 3.2.3 *A morphism of sites (or continuous map) $(\mathfrak{C}', \tau') \to (\mathfrak{C}, \tau)$ is a functor in the opposite direction $\mathfrak{C} \to \mathfrak{C}'$ taking open coverings to open coverings.*

The reversal of direction makes the definition compatible with maps of topological spaces:

Example 3.2.4 *Let $f : X' \to X$ is a continuous map of topological spaces. Equip the categories of open subsets of X and X' with the Grothendieck topologies to obtain sites $(\mathfrak{C}, \tau)$ and $(\mathfrak{C}', \tau')$. Then f induces a morphism of sites $(\mathfrak{C}', \tau') \to (\mathfrak{C}, \tau)$: namely, the functor $\mathfrak{C} \to \mathfrak{C}'$ takes an open subset U of X to the open subset $f^{-1}(U)$ of X'.*

If a set X is equipped with topologies τ' and τ (in the usual sense), and τ' is finer (has more open sets) than τ, then the identity map $(X, \tau') \to (X, \tau)$ is a continuous map of topological spaces. Similarly:

Example 3.2.5 *For any scheme X we have morphisms of sites*

$$X_{et} \to X_{Zar}.$$

Sometimes we just omit the notion τ, if the Grothendieck topology is clear.

3.3 Presheaves and sheaves

A *presheaf of sets* on a site $\mathfrak{T}$ is a contravariant functor $F : \text{Cat}(\mathfrak{T}) \to \text{Sets}$. Thus, to each object U in $\text{Cat}(\mathfrak{T})$, F attaches a set $F(U)$, and to each morphism $\varphi : U \to V$ in $\text{Cat}(\mathfrak{T})$, a map $F(\varphi) : F(V) \to F(U)$ in such a

way that $F(\psi \circ \varphi) = F(\varphi) \circ F(\psi)$ and $F(\mathrm{id}_U)$=$\mathrm{id}_{F(U)}$. Note that the notion of a presheaf on $\mathfrak{T}$ does not depend on the coverings. We sometimes denote $F(\varphi) : F(V) \to F(U)$ by $a \to a|_U$, although this can be confusing because there may be more than one morphism $U \to V$.

Similarly, a presheaf of (abelian) groups or rings on $\mathfrak{T}$ is a contravariant functor from $\mathrm{Cat}(\mathfrak{T})$ to the category of (abelian) groups or rings.

A *sheaf* on $\mathfrak{T}$ is a presheaf F that satisfies the sheaf condition:

$$(S): \qquad F(U) \to \prod_{i \in I} F(U_i) \rightrightarrows \prod_{(i,j) \in I \times I} F(U_i \times_U U_j)$$

is exact for every covering $(U_i \to U)$. Thus F is a sheaf if the map

$$f \mapsto (f|U_i) : F(U) \to \prod F(U_i)$$

identifies $F(U)$ with the subset of the product consisting of families (f_i) such that

$$f_i|U_i \times_U U_j = f_j|U_i \times_U U_j$$

for all $i, j \in I \times I$. Note that when $\mathfrak{T}$ is the site arising from a topological space, these definitions coincide with the usual definitions.

A morphism of presheaves is simply a morphism of functors (alias, natural transformation) and a morphism of sheaves is a morphism of presheaves between sheaves. Let X be a scheme and its étale topology. According to the general definition, a sheaf F on X_{et} is a contravariant functor $\mathrm{Et}/X \to$ Sets (or Ab, or ...) satisfying condition (S) for every $U \to X$ étale and every étale covering $(U_i \to U)$.

Note that a sheaf F on X_{et} defines by restriction a sheaf on U_{Zar} for every $U \to X$ étale. In particular, if $U = \coprod U_i$, then $F(U) \xrightarrow{\sim} \prod F(U_i)$. Before giving some examples of sheaves, we have following proposition that makes it easier to check that a presheaf is a sheaf.

Proposition 3.3.1 *In order to verify that a presheaf F on X_{et} is a sheaf, it suffices to check that F satisfies the sheaf condition (S) for Zariski open coverings and for étale coverings $V \to U$ (consisting of a single map) with V and U both affine.*

Proof See [10] chapter II, section 1, proposition 1.5. for the proof.

3.4 Examples of sheaves on $X_{\mathbf{et}}$

Let $A \to B$ be the homomorphism of rings corresponding to a surjective étale morphism $V \to U$ of affine schemes. In checking the second condition of previous proposition, we shall usually make use only of the fact that $A \to B$ is faithfully flat (i.e., we shall not need to use that it is unramified).

The structure sheaf on X_{et}. For any $U \to X$ étale, define

$$O_{X_{\mathrm{et}}}(U) = \Gamma(U, O_U).$$

Certainly, its restriction to U_{Zar} is a sheaf for any étale over X. That it is a sheaf on X_{et} follows from Proposition 3.3.1 and 3.1.4.

The sheaf defined by an affine scheme Z. An affine X-scheme Z defines a contravariant functor:

$$F : \mathrm{Et}/X \to \mathrm{Sets}, \qquad F(U) = \mathrm{Hom}_X(U, Z).$$

This is a sheaf of sets. First F satisfies the sheaf criterion for open Zariski coverings, we use the glueing morphisms of schemes here. Thus it suffice to show that

$$Z(A) \to Z(B) \rightrightarrows Z(B \otimes_A B)$$

is exact for any faithfully flat map $A \to B$. For Z affine, defined by ring C, then the sequence becomes

$$\mathrm{Hom}_{A-\mathrm{alg}}(C, A) \to \mathrm{Hom}_{A-\mathrm{alg}}(C, B) \rightrightarrows \mathrm{Hom}_{A-\mathrm{alg}}(C, B \otimes_A B).$$

The exactness of this follows immediately from 3.1.4 and left exactness of functor $\mathrm{Hom}_{A-\mathrm{alg}}(C, -)$. If Z has a group structure, then F_Z is a sheaf of groups.

The sheaf defined by a coherent O_X-module. Let $\mathcal{M}$ be a sheaf of coherent O_X-modules on X_{Zar} in the usual sense of algebraic geometry (see next subsection for more information). For any étale map $\varphi : U \to X$, we obtain a coherent O_U-module $\varphi^*\mathcal{M}$ on U_{Zar}. For example, if U and X are affine, corresponding to rings B and A respectively, then $\mathcal{M}$ is defined by a finitely generated A-module M and $\varphi^*\mathcal{M}$ corresponds to the B-module $B \otimes_A M$. There is a presheaf $U \mapsto \Gamma(U, \varphi^*\mathcal{M})$ on X_{et}, which we denote $\mathcal{M}^{\mathrm{et}}$. For

example, $(O_{X_{\mathrm{Zar}}})^{\mathrm{et}} = O_{X_{\mathrm{et}}}$. To verify that $\mathcal{M}^{\mathrm{et}}$ is a sheaf it suffices, again thanks to Propoosition 3.1.4, to show that the sequence

$$0 \to M \to B \otimes_A M \rightrightarrows B \otimes_A B \otimes_A M$$

is exact whenever $A \to B$ is faithfully flat. This can be proved exactly as in the case $M = A$, i.e. Proposition 3.1.4.

3.5 Descent for morphisms of affine schemes and coherent modules

Sheaves of modules. Since modules are linear representations of rings, hence they are important as a tool for studying rings. We will recall some definitions of sheaves of modules for Zariski topology.

Definition 3.5.1 *Let (X, O_X) be a ringed space. A* sheaf of O_X-modules *(or simply an O_X-module) is a sheaf F on X, such that for each open set $U \subset X$, the group $F(U)$ is an O_X-module, and for each inclusion of open sets $V \subset U$, the restriction of homomorphism $F(U) \to F(V)$ is compatible with the module structures via the ring homomorphism $O_X(U) \to O_X(V)$. A morphism $F \to G$ of sheaves of O_X-modules is a morphism of sheaves, such that for each open set $U \subset X$, the map $F(U) \to G(U)$ is a homomorphism of $O_X(U)$-modules.*

Note that the kernel, cokernel, and image of a morphism of O_X-modules is again an O_X-module. If F' is a subsheaf of O_X-modules of an O_X-module F, then the quotient sheaf F/F' is an O_X-module. Any direct sum, direct product, direct limit, or inverse limit of O_X-modules is an O_X-module. If F and G are two O_X-modules, we denote the group of morphisms from F to G by $Hom_{O_X}(F, G)$, or sometimes $Hom_X(F, G)$ or $Hom(F, G)$ if no confusion can arise. A sequence of O_X-modules and morphisms is exact if it is exact as a sequence of sheaves of abelian groups.

If U is an open subset of X, and if F is an O_X-module, then $F|_U$ is an $O_X|_U$-module. If F and G are two O_X-modules, the presheaf

$$U \mapsto Hom_{O_X|_U}(F|_U, G|_U)$$

is a sheaf, which we call the sheaf Hom, and denote by $Hom_{O_X}(F, G)$, It is also an O_X-module.

We define the tensor product $F \otimes_{O_X} G$ of two O_X-modules to be the sheaf associated to the presheaf $U \mapsto F(U) \otimes_{O_X(U)} G(U)$. We will often write simply $F \otimes G$, with O_X understood.

As O_X-module, F is free if it is isomorphic to a direct sum of copies of O_X. It is locally free is X can be covered by open sets of U for which $F|_U$ is a free $O_X|_U$-module. In that case the rank of F on such an open set is the number of copies of the structure sheaf needed (finite or infinite). If X is connected, the rank of a locally free sheaf is the same everywhere. A locally free sheaf of rank 1 is also called an invertible sheaf.

A sheaf of ideals on X is a sheaf of modules I which is a subsheaf of O_X. In other words, for every open set U, $I(U)$ is an ideal in $O_X(U)$.

Let $f : (X, O_X) \to (Y, O_Y)$ be a morphism of ringed spaces. If F is an O_X-module, then f_*F is an f_*O_X-module. Since we have the morphism $f^\# : O_Y \to f_*O_X$ of sheaves of rings on Y, this gives f_*F a natural structure of O_Y-module. We call it the direct image of F by the morphism f.

Now let G be a sheaf of O_Y-modules. Then $f^{-1}G$ is an $f^{-1}O_Y$-module. Because of the adjoint property of f^{-1}, i.e. for any sheaves F on X and G on Y we have

$$Hom_X(f^{-1}G, F) = Hom_Y(G, f_*F),$$

we have a morphism $f^{-1}O_Y \to O_X$ of sheaves of rings on X. We define f^*G to be the tensor product

$$f^{-1}G \otimes_{f^{-1}O_Y} O_X.$$

Thus f^*G is an O_X-module. We call it the pull-back of G by the morphism f.

Now that we have the general notion of a sheaf of modules on a ringed space, we specialize to the case of schemes with Zariski topology. We start by defining the sheaf of modules $\tilde{M}$ on Spec$A$ associated to a module M over a ring A.

Definition 3.5.2 *Let A be a ring and let M be an A-module. We define the sheaf associated to M on SpecA, denoted by $\tilde{M}$ as follows. For each prime ideal $\mathfrak{p} \subset A$, let $M_\mathfrak{p}$ be the localisation of M at $\mathfrak{p}$. For any open set $U \subset$ SpecA we define the group $\tilde{M}(U)$ to be the set of functions $s : U \to \coprod_{\mathfrak{p} \in U} M_\mathfrak{p}$ such that for each $\mathfrak{p} \in U, s(\mathfrak{p}) \in M_\mathfrak{p}$ and such that s is locally a fraction m/f with $m \in M$ and $f \in A$. To be precise, we require that for each $\mathfrak{p} \in U$, there is a neighborhood V of $\mathfrak{p}$ in U, and there are elements $m \in M$ and $f \in A$,*

such that for each $\mathfrak{q} \in V, f \notin \mathfrak{q}$, *and* $s(\mathfrak{q}) = m/f$ *in* $M_{\mathfrak{q}}$. *We make* $\tilde{M}$ *into a sheaf by using the obvious restriction maps.*

Proposition 3.5.3 *Let* A *be a ring, and let* M *be an* A*-module, and let* $\tilde{M}$ *be the sheaf on* $X =$*SpecA associated to* M. *Then:*

- $\tilde{M}$ *is an* O_X*-module;*
- *for each* $\mathfrak{p} \in X$, *the stalk* $(\tilde{M})_{\mathfrak{p}}$ *of the sheaf* $\tilde{M}$ *at* $\mathfrak{p}$ *is isomorphic to the localized module* $M_{\mathfrak{p}}$*;*
- *for any* $f \in A$, *the* A_f*-module* $\tilde{M}(D(f))$ *is isomorphic to the localized module* M_f*;*
- *in particular,* $\Gamma(X, \tilde{M}) = M$.

Proof See [6], chapter II, section 5, proposition 5.1. for the proof.

Proposition 3.5.4 *Let* A *be a ring and let* $X =$ *SpecA. Also let* $A \to B$ *be a ring homomorphism, and let* $f :$ *SpecB* $\to$ *Spec* A *be the corresponding morphism of spectra. Then:*

- *the map* $M \to \tilde{M}$ *gives an exact, fully faithful functor from the category of* A*-modules to the category of* O_X*-modules;*
- *if* M *and* N *are two* A*-modules, then* $\widetilde{(M \otimes_A N)} \simeq \tilde{M} \otimes_{O_X} \tilde{N}$*;*
- *If* $\{M_i\}$ *is any family of* A*-modules, then* $\widetilde{\oplus M_i} \simeq \tilde{M}_i$*;*
- *for any* B*-module* N *we have* $f_*(\tilde{N}) \simeq \widetilde{({}_A N)}$, *where* ${}_A N$ *means* N *considered as an* A*-module;*
- *for any* A*-module* M *we have* $f^*(\tilde{M}) \simeq \widetilde{(M \otimes_A B)}$.

Proof See [6], chapter II, section 5, proposition 5.2. for the proof.

These sheaves of the form $\tilde{M}$ on affine schemes are our models for quasi coherent sheaves. A quasi-coherent sheaf on a scheme X will be an O_X-module which is locally of the form $\tilde{M}$.

Definition 3.5.5 *Let (X, O_X) be a scheme. A sheaf of O_X-modules F is* quasi-coherent *if X can be covered by open affine subsets $U_i = SpecA_i$, such that for each i there is an A_i-module M_i with $F|_{U_i} \simeq \tilde{M}_i$. We say that F is* coherent *if furthermore each M_i can be taken to be a finitely generated A_i-module.*

fpqc-Descent theorems. Assume all schemes are locally Noetherian. Now suppose that one wants to carry out a construction of a variety over a base field k. Sometimes all one can do directly is to construct its analogue X' over some field extension k'. Then one is faced with the task of deciding whether X' is the base extension of some k-variety X, if so, to construct X. This is a special case of the problem known as descent.

Proposition 3.5.6 *Let $f : Y \to X$ be faithfully flat and quasi-compact. To give a quasi-coherent O_X-module M is the same as to give a quasi-coherent module M' on Y plus an isomorphism $\phi : p_1^* M' \to p_2^* M'$, where $p_1, p_2 : Y \times_X Y \to Y$ are the first and second projections, satisfying*

$$p_{31}^*(\phi) = p_{32}^*(\phi) \circ p_{21}^*(\phi).$$

(Here the p_{ij} are the various projections $Y \times_X Y \times_X Y \to Y \times_X Y$, that is $p_{ji}(y_1, y_2, y_3) = (y_j, y_i), j > i$.)

Proof See [10], chapter I, section 2, proposition 2.22. for the proof.

We can consider the problem of descending schemes instead of quasi-coherent sheaves. One can deduce following proposition from the previous one.

Proposition 3.5.7 *Let $f : Y \to X$ be faithfully flat and quasi-compact. To give a scheme Z affine over X is the same as to give a scheme Z' affine over Y plus an isomorphism $\phi : p_1^* Z' \to p_2^* Z'$ satisfying*

$$p_{31}^*(\phi) = p_{32}^*(\phi) \circ p_{21}^*(\phi).$$

Proof See [10], chapter I, section 2, theorem 2.23 for the proof.

(For $p : S' \to S$, X is a S-scheme, we use the notation $p^*X = X \times_S S'$.) Moreover we have several properties of morphisms descend. Consider a Cartesian square

$$\begin{array}{ccc} Y & \longleftarrow & Y' \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f'} \\ X & \longleftarrow & X' \end{array}$$

in which the map $X' \to X$ is faithfully flat and quasi-compact. If f' is a quasi-compact (respectively separated, of finite type, proper, an open immersion, affine, finite, quasi-finite, flat, smooth, étale), then f is also.

3.6 Cohomology

The derived functor definition. We recall some definitions and techniques from Homological algebra.

Definition 3.6.1 *An* abelian category *is a category $\mathfrak{A}$, such that: for each $A, B \in Ob(\mathfrak{A})$, $Hom(A, B)$ has a structure of an abelian group, and the composition law is linear; finite direct sums exist; every morphism has a kernel and cokernel; every monomorphism is the kernel of its cokernel, every epimorphism is the cokernel of its kernel; and finally, every morphism can be factored into an epimorphism followed by a monomorphism.*

The following are all abelian categories:

Example 3.6.2 *The category of abelian groups, the category of modules over a ring A (commutative with identity as always), the category of sheaves of abelian groups on a topological space X, the category of sheaves of O_X-modules on a ringed space (X, O_X), the category of quasi-coherent sheaves of O_X-modules on a scheme X, the category of coherent sheaves of O_X-modules on a noetherian scheme X.*

Now we begin our review of homological algebra. A complex $A^\bullet$ in an abelian category $\mathfrak{A}$ is a collection of objects $A^i, i \in \mathbb{Z}$, and morphisms $d^i : A^i \to A^{i+1}$, such that $d^{i+1} \circ d^i = 0$ for all i. If the objects A^i are specified only in certain range, e.g., $i \geq 0$, then we set $A^i = 0$ for all other i. A morphism of complexes, $f : A^\bullet \to B^\bullet$ is a set of morphisms $f^i : A^i \to B^i$ for each i, which commute with the coboundary maps d^i.

The *ith cohomology object* $h^i(A^\bullet)$ of the complex $A^\bullet$ is defined to be $\ker(d^i)/\mathrm{im}(d^{i-1})$. If $f : A^\bullet \to B^\bullet$ is a morphism of complexes, then f induces a natural map $h^i(f) : h^i(A^\bullet) \to h^i(B^\bullet)$. If $0 \to A^\bullet \to B^\bullet \to C^\bullet \to 0$ is a short exact sequence of complexes, then there are natural maps $\delta^i : h^i(C^\bullet) \to h^{i+1}(A^\bullet)$ giving rise to a long exact sequence

$$\cdots \to h^i(A^\bullet) \to h^i(B^\bullet) \to h^i(C^\bullet) \xrightarrow{\delta^i} h^{i+1}(A^\bullet) \to \ldots$$

Two morphisms of complexes $f, g : A^\bullet \to B^\bullet$ are *homotopic* (written $f \sim g$) if there is a collection of morphisms $k^i : A^i \to B^{i-1}$ for each i (which need not commute with the d^i) such that $f - g = dk + kd$. The collection of morphisms, $k = (k^i)$ is called a homotopy operator. If $f \sim g$, then f and g induce the same morphism $h^i(A^\bullet) \to h^i(B^\bullet)$ on the cohomology objects, for each i.

A covariant functor $F : \mathfrak{A} \to \mathfrak{B}$ from one abellian category to another is *additive* if for any two objects A, A' in $\mathfrak{A}$, the induced map $\mathrm{Hom}(A, A') \to \mathrm{Hom}(FA, FA')$ is a homomorphism of abelian groups. F is left exact if it is additive and for every short exact sequence

$$0 \to A' \to A \to A'' \to 0$$

in $\mathfrak{A}$, the sequence

$$0 \to FA' \to FA \to FA''$$

is exact in $\mathfrak{B}$. If we can write a 0 on the right instead of left, we say F is right exact. If it is both left and right exact, we say it is exact. If only the middle part $FA' \to FA \to FA''$ is exact, we say F is exact in the middle.

For a contravariant functor we make analogous definitions. For example, $F : \mathfrak{A} \to \mathfrak{B}$ is left exact if it is additive, and for every short exact sequence as above, the sequence

$$0 \to FA'' \to FA \to FA'$$

is exact in $\mathfrak{B}$.

Example 3.6.3 *If $\mathfrak{A}$ is an abelian category, and A is a fixed object, then functor $B \to Hom\ (A, B)$, usually denoted $Hom(A, \bullet)$, is a covariant left exact functor from $\mathfrak{A}$ to category of abelian group **Ab**. The functor $Hom(\bullet, A)$ is a contravariant left exact functor from $\mathfrak{A}$ to **Ab**.*

Now we come to resolutions and derived functors. An object I of $\mathfrak{A}$ is *injective* if the functor $\mathrm{Hom}(\bullet, I)$ is exact. An injective resolution of an object A of $\mathfrak{A}$ is a complex $I^\bullet$, defined in degrees $i \geq 0$, together with a morphism $\epsilon : A \to I^0$, such that I^i is an injective object $\mathfrak{A}$ for each $i \geq 0$, and such that the sequence

$$0 \to A \xrightarrow{\epsilon} I^0 \to I^1 \to \dots$$

is exact.

If every object of $\mathfrak{A}$ is isomorphic to a subobject of an injective object of $\mathfrak{A}$, then we say $\mathfrak{A}$ has enough injectives. If $\mathfrak{A}$ has enough injectives, then every object has an injective resolution. Furthermore, a well-known lemma states that any two injective resolutions are homotopy equivalent.

Now let $\mathfrak{A}$ be an abelian category with enough injectives, and let $F : \mathfrak{A} \to \mathfrak{B}$ be a covariant left exact functor. Then we construct the *right derived functors* $R^iF, i \geq 0$, of F as follows. For each object A of $\mathfrak{A}$, choose once and for all an injective resolution $I^\bullet$ of A. Then we define $R^iF(A) = h^i(F(I^\bullet))$.

Now we fix a scheme X, and an element $\bullet$ of $\{\mathrm{Zar}, \mathrm{et}\}$. It turns out that the category of abelian sheaves on $X_\bullet$ has enough injectives.

Definition 3.6.4 *For $i \in \mathbb{Z}_{\geq 0}$, define the functor*

$$\{\textit{abelian sheaves on } X_\bullet\} \to \boldsymbol{Ab} : \quad F \mapsto H^i_\bullet(X, F)$$

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

$$\{\textit{abelian sheaves on } X_\bullet\} \to \boldsymbol{Ab} : \quad F \mapsto F(X).$$

If F is an abelian sheaf on $X_\bullet$, then the abelian group $H^i_\bullet(X, F)$ is called the i^{th} Zariski/étale cohomology group *of F.*

In particular, for any exact sequence of abelian sheaves on $X_\bullet$

$$0 \to F \to G \to H \to 0$$

we get a long exact sequence

$$0 \to H^0_\bullet(X, F) \to H^0_\bullet(X, G) \to H^0_\bullet(X, H) \to H^1_\bullet(X, F) \to \dots$$

Remark for each abelian sheaf F on $X_\bullet = (\mathfrak{C}, \tau)$ and for each "open subset" $U \in \mathfrak{C}$, one can define $H^i_\bullet(U, F)$ by taking the derived functors of $\Gamma(U, -)$.

There is a canonical "pullback" homomorphism $H^i_\bullet(X,F) \to H^i_\bullet(U,F)$. In fact,

$$\mathfrak{C}^{\mathrm{op}} \to \mathbf{Ab}: \quad U \mapsto H^i_\bullet(U,F)$$

defines a presheaf called $H^i(F)$.

Alternatively, one can restrict F to the site $U_\bullet$ and take $H^i_\bullet(U, F|_U)$. There is a canonical isomorphism

$$H^i_\bullet(U,F) \simeq H^i_\bullet(U, F|_U),$$

because one can show that the functor $F \mapsto F|_U$ takes injective sheaves on $X_\bullet$ to injective sheaves on $U_\bullet$.

Čech cohomology. It is not practical to use the definition of the cohomology groups in terms of derived functors to compute them directly. Under mild hypotheses on X, the derived functor groups agree with the Čech groups, which are sometimes more manageable. Assume all rings are Noetherian and all schemes are locally Noetherian.

Let $U = (U_i \to X)_{i \in X}$ be an étale/Zariski covering of X, and let P be a presheaf of abelian groups on $X_\bullet$. Define

$$C^i(U,P) = \prod_{(i_0,\ldots,i_r) \in I^{r+1}} P(U_{i_0 \ldots i_r}), \quad \text{where } U_{i_0\ldots i_r} = U_{i_0} \times_X \cdots \times_X U_{i_r}.$$

For $s = (s_{i_0\ldots i_r}) \in C^i(U,P)$, define $d^i s \in C^{i+1}(U,P)$ by the rule

$$(d^i s)_{i_0 \ldots i_{r+1}} = \sum_{j=0}^{r+1} \mathrm{res}_j(s_{i_0 \ldots i_{j-1} i_{j+1} \ldots i_{r+1}})$$

where res_j is the restriction map corresponding to the projection map

$$U_{i_0\ldots i_{r+1}} \to U_{i_0 \ldots i_{j-1} i_{j+1} \ldots i_{r+1}}.$$

One verifies by a straight forward calculation that

$$C^\bullet(U,P) = C^0(U,P) \to \cdots \to C^i(U,P) \xrightarrow{d^i} C^{i+1}(U,P) \to \ldots$$

is a complex. Define

$$\check{H}^i(U,P) = h^i(C^\bullet(U,P)).$$

It is called the *ith Čech cohomology group* of P relative to the covering U. Note that

$$\check{H}^i(U,P) = \mathrm{Ker}(\prod P(U_i) \rightrightarrows \prod P(U_{ij})).$$

Therefore, for a sheaf F,

$$\check{H}^0(U,F) = \Gamma(X,F).$$

Definition 3.6.5 *Let $U = \{U_i \to X\}_{i\in I}$ and $V = \{V_j \to X\}_{j\in J}$ be open coverings. Then V is called a* refinement *of U if there is a map $\tau : J \to I$ such that $V_j \to X$ factors through $U_{\tau j} \to X$ for all $j \in J$.*

If V is refinement of U, then there is an induced morphism $\check{H}^i(U,F) \to \check{H}^i(V,F)$ for each $i \geq 0$ which is independent of τ and the X-morphism $V_j \to U_{\tau j}$. We may passing to the limit over all coverings, and so obtain Čech cohomology groups

$$\check{H}^i(X,F) = \lim_{\to U} \check{H}^i(U,F).$$

Proposition 3.6.6 *If F is a sheaf of abelian groups on Zariski/étale site $X_\bullet = (\mathfrak{C}, \tau)$, then we have*

- $\check{H}^0(X,F) \xrightarrow{\sim} H^0(X,F) = F(X)$
- $\check{H}^1(X,F) \xrightarrow{\sim} H^1(X,F)$
- $\check{H}^2(X,F) \hookrightarrow H^2(X,F)$

Proof See [9], chapter 6, section 4, proposition 6.4.11. for the proof.

The Mayer-Vietoris sequence. When $U = (U_i \to X)$ is a open covering of X (in the Zariski sense), then the Čech cohomology group can be computed using alternating cochains. For example, if $X = U_0 \cup U_1$, then the Čech cohomology group of a presheaf P are the cohomology groups of the complex

$$\Gamma(U_0,P) \times \Gamma(U_1,P) \to \Gamma(U_0 \cap U_1, P);$$

in particular, $\check{H}^i(X,F) = 0$ for $i \geq 2$.

Theorem 3.6.7 *Let $X = U_0 \cap U_1$ (union of two open subsets in Zariski sense). For any sheaf F on $X_\bullet$, there is an infinite exact sequence*

$$\cdots \to H^i(X,F) \to H^i(U_0,F) \oplus H^i(U_1,F) \to H^i(U_0 \cap U_1, F) \to H^{i+1}(X,F) \to \ldots$$

Proof See [11], chapter I, section 10, proposition 10.8. for the proof.

For Zariski topology and X is a noetherian topology space, there is a Vanishing theorem of Grothendieck as follows:

Theorem 3.6.8 *Let X be a Noetherian topological space of dimension n. Then for all $i > n$ and all sheaves of abelian groups F on X, we have $H^i(X, F) = 0$.*

Proof See [6], chapter III, section 2, theorem 2.7 for the proof.

3.7 Principal Homogeneous Spaces and H^1

For sheaves of abelian groups, from proposition 3.6.6, we have that $H^1(X_\bullet, F)$ coincides with $\check{H}^1(X_\bullet, F)$, where $\bullet \in \{\text{et, Zar}\}$. Now we try to interpret $\check{H}^1(X_\bullet, F)$ as the group of principal homogeneous spaces for F, sheaves of noncommutative groups. As usual assume all rings are Noetherian and all schemes are locally Noetherian.

Definition of the first Čech group. Let $U = (U_i \to X)_{i\in I}$ be an étale/Zariski covering of X, and let $\mathcal{G}$ be a sheaf of groups on $X_\bullet$ (not necessarily commutative), where $\bullet \in \{\text{et, Zar}\}$. We write $U_{ij\ldots}$ for $U_i \times_X U_j \times_X \cdots$. A 1-cocycle for U with values in $\mathcal{G}$ is a family $(g_{ij})_{(i,j)\in I\times I}$ with $g_{ij} \in \mathcal{G}(U_{ij})$ such that

$$(g_{ij}|_{U_{ijk}}) \cdot (g_{jk}|_{U_{ijk}}) = (g_{ik}|_{U_{ijk}}), \text{all } i, j, k.$$

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

$$g'_{ij} = (h_i|_{U_{ij}}) \cdot g_{ij} \cdot (h_j|_{U_{ij}})^{-1}, \text{all } i, j.$$

The set of 1-cocycles modulo $\sim$ is denoted $\check{H}^1(U, \mathcal{G})$. It is not in general a group, but it does have a distinguished element represented by the 1-cocycle (g_{ij}) with $g_{ij} = 1$ for all i, j.

A sequence

$$1 \to \mathcal{G}' \to \mathcal{G} \to \mathcal{G}'' \to 1$$

of sheaves of groups is said to be exact if

$$1 \to \mathcal{G}'(U) \to \mathcal{G}(U) \to \mathcal{G}''(U)$$

is exact for all $U \to X$ étale (or open subset for Zariski topology) and $\mathcal{G} \to \mathcal{G}'$ is locally surjective. Such a sequence gives rise to a sequence of sets

$$1 \to \mathcal{G}'(X) \to \mathcal{G}(X) \to \mathcal{G}''(X) \to \check{H}^1(X, \mathcal{G}') \to \check{H}^1(X, \mathcal{G}) \to \check{H}^1(X, \mathcal{G}'')$$

that is exact is the following sense: the image of each arrow is exactly the set mapped to the distinguished element by the following arrow.

Principal Homogeneous spaces or torsors. Let $\mathfrak{C}$ be a (small/big) étale/Zariski site. Let $\mathfrak{X}$ and $\mathfrak{Y}$ be sheaves of sets on $\mathfrak{C}$. Then we have presheaves on $\mathfrak{C}$:

$$Hom(\mathfrak{X}, \mathfrak{Y}): \quad X \mapsto \mathrm{Hom}_{\mathfrak{C}/X}(\mathfrak{X}_{|X}, \mathfrak{Y}_{|X})$$

$$Isom(\mathfrak{X}, \mathfrak{Y}): \quad X \mapsto \mathrm{Isom}_{\mathfrak{C}/X}(\mathfrak{X}_{|X}, \mathfrak{Y}_{|X})$$

These presheaves are sheaves. Argument for that: Let $X \in \mathfrak{C}$, $U = (U_i \to X)_{i \in I}$ is an open covering of X, and $(f_i : \mathfrak{X}|_{U_i} \to \mathfrak{Y}|_{U_i})_{i \in I}$ compatible, descent for sheaves (almost a tautology) says that

$$\mathrm{Sh}(\mathfrak{C}/X) \to (\mathrm{Sh}(U) + \text{descent data}) \text{ is an equivalence;}$$

so $\exists!\ f : \mathfrak{X}_{|X} \to \mathfrak{Y}_{|X}$ inducing the f_i.

Definition 3.7.1 *$\mathfrak{X}$ and $\mathfrak{Y}$ are* locally isomorphic *if for any $X \in \mathfrak{C}$ there exists an open covering $U = (U_i \to X)_{i \in I}$ such that for every $i \in I$ we have $\mathfrak{X}_{|U_i}$ is isomorphic to $\mathfrak{Y}_{|U_i}$.*

Example 3.7.2 *We have a notion locally free O_X-modules of rank n on a ringed space (X, O_X).*

Now assume that $\mathfrak{X}$ and $\mathfrak{Y}$ are locally isomorphic. Then commuting actions

$$\mathrm{Aut}(\mathfrak{X}) \circlearrowleft Isom(\mathfrak{X}, \mathfrak{Y}) \circlearrowright \mathrm{Aut}(\mathfrak{Y}),$$

is a typical example of a bi-torsor.

Definition 3.7.3 *Let $\mathcal{G}$ be a sheaf of groups on $\mathfrak{C}$ and $\mathfrak{X}$ a sheaf of sets with a $\mathcal{G}$-action: $\mathcal{G} \times \mathfrak{X} \to \mathfrak{X}$, i.e, for every $X \in \mathfrak{C}$: $\mathcal{G}(X) \times \mathfrak{X}(X) \to \mathfrak{X}(X)$ is a $\mathcal{G}(X)$-action, functorial in X. The $\mathfrak{X}$ is a $\mathcal{G}$-*torsor *if $(\mathcal{G}, \mathfrak{X}$, action) is locally isomorphic to $(\mathcal{G}, \mathcal{G}$, left translation). Equivalently: for every $X \in \mathfrak{C}$, $\mathcal{G}(X)$ acts freely and transitively on $\mathfrak{X}(X)$, and there exists an open covering $U = (U_i \to X)_{i \in I}$ such that $\mathfrak{X}(U_i) \neq \emptyset$.*

Back to the previous situation: $\mathfrak{X}$ and $\mathfrak{Y}$ are locally isomorphic on $\mathfrak{C}$. Let $I = Isom(\mathfrak{X}, \mathfrak{Y})$ and $\mathcal{G} = Aut(\mathfrak{X})$. Then for every $X \in \mathfrak{C}$ we have $I \times \mathfrak{X} \to \mathfrak{Y}$, $I(X) \times \mathfrak{X}(X) \to \mathfrak{Y}(X)$, $(i, x) \mapsto i(x)$ is the quotient for the right $\mathcal{G}$-action $(i, x) \circ g = (i \circ g, g^{-1}(x))$. Notation :

$$\mathfrak{Y} = I \otimes_{\mathcal{G}} \mathfrak{X} = (X \mapsto (I(X) \times \mathfrak{X}(X))/\mathcal{G}(X))^{\#}.$$

Now we consider for site $X_\bullet$ where $\bullet \in \{et, Zar\}$. A torsor $\mathfrak{X}$ is trivial if it is isomorphic (as a sheaf with a left action of $\mathcal{G}$) to $\mathcal{G}$ acting on itself by left multiplication, or, equivalently, if $\mathfrak{X}(X) \neq \emptyset$. We say that the covering $U = (U_i \to X)_{i \in I}$ splits $\mathfrak{X}$ if $\mathfrak{X}(U_i) \neq \emptyset$.

Let $\mathfrak{X}$ be a torsor for $\mathcal{G}$. Let $U = (U_i \to X)_{i \in I}$ be an open covering of X that splits $\mathfrak{X}$, and choose an $s_i \in \mathfrak{X}(U_i)$ for each i. Because of definition of torsor, there exists a unique $g_{ij} \in \mathcal{G}(U_{ij})$, such that

$$(s_i|_{U_{ij}}) \cdot g_{ij} = s_j|_{U_{ij}}.$$

Then $(g_{ij})_{I \times I}$ is a cocycle, because (omitting the restriction signs)

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

Moreover, replacing s_i with $s'_i = s_i \cdot h_i, h_i \in \mathcal{G}(U_i)$ leads to a cohomologous cocycle. Thus, $\mathfrak{X}$ defines a class $c(\mathfrak{X})$ in $\check{H}^1(U, \mathcal{G})$.

Proposition 3.7.4 *The map $\mathfrak{X} \mapsto c(\mathfrak{X})$ defines a bijection from the set of isomorphism classes of principal homogenous spaces for $\mathcal{G}$ split by U to $\check{H}^1(U, \mathcal{G})$.*

Proof See [11], chapter I, section 11, proposition 11.1. for the proof.

Picard groups. For a scheme X, $\mathrm{Pic}(X)$ is defined as the group of isomorphism classes of invertible sheaves (or line bundles) on X for the Zariski topology, with the group operation being tensor product. Hilbert's theorem 90 says that there is a canonical isomorphism $H^1(X_{et}, \mathbb{G}_m) \simeq H^1(X_{Zar}, \mathbb{G}_m) \simeq \mathrm{Pic}(X)$. Note that since $\mathbb{G}_m$ is commutative, the first Čech cohomology group is isomorphic with the derived functor definition, i.e. $\check{H}^1(X_\bullet, \mathbb{G}_m) \simeq H^1(X_\bullet, \mathbb{G}_m)$ for $\bullet \in \{\mathrm{et,Zar}\}$.

Example 3.7.5 • *The Picard group of the spectrum of a Dedekind domain is its ideal class group.*

- *The invertible sheaves on projective space $\mathbb{P}^n(k)$ for k a field, are isomorphic to the twisting sheaves $\mathcal{O}(m)$ and $\mathcal{O}(m) \neq \mathcal{O}(n)$ if $m \neq n$, so the Picard group of $\mathbb{P}^n(k)$ is isomorphic to $\mathbb{Z}$.*

Twisted-forms. Let Y be a scheme (sheaf of modules, algebras or group scheme) over X. Another object Y' of the same type over X is a twisted-form of Y for the Zariski/étale topology on X if there exists a covering $U = (U_i \to X)$ for the Zariski/étale topology such that $Y \times_X U_i \simeq Y' \times_X U_i$ for all i. Any such twisted-form Y' defines an element $c(Y') \in \check{H}^1(U, \underline{\mathrm{Aut}}(Y))$, where $\underline{\mathrm{Aut}}(Y)$ is the sheaf associated with the presheaf $V \mapsto \mathrm{Aut}_V(Y \times_X V)$, as follows: let ϕ_i be an isomorphism $Y \times_X U_i \to Y' \times_X U_i$; then (α_{ij}), where $\alpha_{ij} = \phi_i^{-1} \circ \phi_j$, is a 1-cocycle representing $c(Y')$. The class $c(Y')$ is well-defined, and two twisted-form Y' and Y'' are isomorphic over X if and only if $c(Y') = c(Y'')$. Any element of $\check{H}^1(U, \underline{\mathrm{Aut}}(Y))$ defines a descent datum on $Y \times_X V$ where $V = \coprod U_i$, that is, an isomorphism ϕ satisfying the conditions of proposition 3.5.7. The map $Y' \mapsto c(Y')$ thus defines an injection from the set of isomorphism classes of twisted-forms of Y that become trivial when restricted to U into $\check{H}^1(U, \underline{\mathrm{Aut}}(Y))$, and this injection is surjective whenever every descent datum on $Y \times_X V$ arises from twisted-form.

4 On Gauss's 3 squares theorem by Bas Edixhoven

4.1 Gauss's 3 squares theorem

The theorem is the following, where, for d a non-zero integer that is 0 or 1 mod 4, O_d denotes the quadratic order of discriminant d, that is, $O_d = \mathbb{Z}[(\sqrt{d}+d)/2]$.

Theorem 4.1.1 *Let $n \in \mathbb{Z}_{\ ge1}$ be a square free. Then the number of solutions in $\mathbb{Z}^3$ of the equation $x^2+y^2+z^2=n$ is equal to:*

$$\#\{x \in \mathbb{Z}^3 : x_1^2+x_2^2+x_3^2=n\} = \begin{cases} 0 & \text{if } n \equiv 7(8), \\ 48.\frac{\#Pic(O_{-n})}{\#(O_{-n}^\times)} & \text{if } n \equiv 3(8), \\ 24.\frac{\#Pic(O_{-4n})}{\#(O_{-4n}^\times)} & \text{if } n \equiv 1,2(4). \end{cases}$$

Gauss proved and formulated it in terms of equivalence classes of quadratic forms, not of ideals. The proof is difficult, it is an amount of about 240 pages of these that one has to read in his book Disquisitiones. Gauss took a path, solving the difficult problem of deciding which quadratic forms can be embedded into $\mathbb{Z}^3$ with the standard inner product, and in how many ways.

Bas Edixhoven had the idea to think in terms of SO_3 as group scheme over $\mathbb{Z}$ and transporters between solutions. These transporters are, for solutions in the same orbit, bi-torsors for the stabilisers. And these torsors are Zariski locally trivial. The idea of the proof is to relate the H^1 of the stabiliser H to the relevant class group uses exact sequence of cohomology. This gives a short proof but not an elementary one, giving all the understanding that one could want.

One of the difficulty to relate to the relevant class group is that the $\mathbb{Z}$-structure of H is not that of the restriction of scalars of the multiplicative group from O_d to $\mathbb{Z}$, but its open subscheme with connected fibres. So now let us start our proof.

4.2 Proof of Gauss's 3 squares theorem by Algebraic geometry

Let n be in $\mathbb{Z}_{\geq 1}$. Let X_n be the closed subscheme of $\mathbb{A}^3$ over $S := \mathrm{Spec}(\mathbb{Z})$ defined by $x^2+y^2+z^2=n$. Let G be the group scheme SO_3 over S, i.e.,

equations in GL_3 are : $g^t.g = 1$, $\det(g) = 1$. Then G acts tautologically on $\mathbb{A}^3$, inducing an action on X_n. Let $\mathcal{G}$ be the sheaf of groups on S for the Zariski topology given by G: for every open U in S we have $\mathcal{G}(U) = G(U)$. Recall that an open subset of S is in the form $U = \text{Spec } \mathbb{Z}[1/m]$ for some m non-zero integer. Let $X_n(\mathbb{Z})^{\text{prim}}$ be the subset of $X_n(\mathbb{Z})$ consisting of primitive elements, that is, triples (a, b, c) with $a\mathbb{Z} + b\mathbb{Z} + c\mathbb{Z} = \mathbb{Z}$. Also $X_n(\mathbb{Z})^{\text{prim}}$ is stable under $G(S)$.

Assume that $X_n(\mathbb{Z})^{\text{prim}} \neq \emptyset$. Let P be in $X_n(\mathbb{Z})^{\text{prim}} \neq \emptyset$ and let $H := G_P$, the stabilizer of P in G, i.e., for every $\mathbb{Z}$-algebra A :

$$H(A) = \{g \in G(A) : gP = P \text{ in } A^3\}.$$

Thus H is subgroup scheme with additional equation in G is given by $gP = P$. Denote $\mathcal{H}$ the sheaf of group on S given by H. Note that $H(\mathbb{R})$ is rotation with axis $\mathbb{R}.P$, therefore H is commutative group scheme.

Now for any $Q \in X_n(\mathbb{Z})^{\text{prim}}$, let $G_{P,Q} \rightarrowtail G$, the *transporteur* from P to Q in G, is defined as for any $\mathbb{Z}$-algebra A :

$$G_{P,Q}(A) = \{g \in G(A) : gP = Q \text{ in } A^3\}.$$

Also denote $\mathcal{T}_{P,Q}$ the sheaf of group on S given by $G_{P,Q}$. We have $\mathcal{H}$ acts on it on the right, by composition.

Proposition 4.2.1 *With the above notation and assumptions, for every Q in $X_n(\mathbb{Z})^{prim}$ the transporter is an $\mathcal{H}$-torsor.*

Proof Let Q be in $X_n(\mathbb{Z})^{\text{prim}}$. For every open U of S the action of $\mathcal{H}(U)$ on $\tau_{P,Q}(U)$ is free and transitive:

$$\text{for } g \in \mathcal{T}_{P,Q}(U) \text{ and } h_1, h_2 \in \mathcal{H}(U) \text{ if } g.h_1 = g.h_2 \text{ implies } h_1 = h_2,$$

$$\text{for any } g_1, g_2 \in \mathcal{T}_{P,Q}(U) \text{ take } h = g_1^{-1}.g_2 \in \mathcal{H}(U) \text{ such that } g_1.h = g_2.$$

What we must show next is that for every $s = (p) \in S$, where p is prime number, there is an open $U = \text{Spec } \mathbb{Z}[1/m]$ containing s (i.e. $p \nmid m$) such that $\mathcal{T}_{P,Q}(U)$ is not empty.

For each nonzero v in $\mathbb{Q}^3$ we define s_v to be the symmetry with respect to v, that is, the $\mathbb{Q}$-linear map

$$s_v : \mathbb{Q}^3 \to \mathbb{Q}^3, \quad x \mapsto x - 2\frac{\langle x, v\rangle}{\langle v, v\rangle}v.$$

Observe that $s_v = s_{v'}$ if v' is a nonzero multiple of v. For w and v nonzero in $\mathbb{Q}^3$, $s_w s_v$ is in $G(\mathbb{Q})$, and if m in $\mathbb{Z}$ is nonzero and w and v are in $\mathbb{Z}[1/m]^3$, then $s_w s_v$ is in $G(\mathbb{Z}[1/m])$. For v in $\mathbb{Z}^3$ not a multiple 2, $\langle v, v\rangle$ is not divisible by 4, hence the symmetry s_v preserves $\mathbb{Z}[1/m]^3$ for a suitable odd number m. In particular for primitive v, it says $s_v : \mathbb{Z}^3_{(2)} \to \mathbb{Z}^3_{(2)}$.

If $Q = P$ then the unit element of $G(S)$ is in $\mathcal{T}_{P,Q}(S)$ and therefore it is trivial $\mathcal{H}$-torsor. Assume now $Q \neq P$.

We first deal with the point $s = (2)$. Let v be any primitive element of $\mathbb{Z}^3$ that is orthogonal to P. Let w be a primitive element of $\mathbb{Z}^3$ of which $Q - P$ is a multiple of w (Want to say that $s_w = s_{Q-P}$). Then $s_w s_v$ is in $G(\mathbb{Z}[1/m])$ for some odd integer m, and $s_w s_v P = s_w P = Q$ because $\langle P, P\rangle = \langle Q, Q\rangle$.

Let now $s = (p)$ in S for some odd prime number p. Note that the reductions $\bar{P}$ and $\bar{Q}$ of P and Q mod p are both nonzero in $\mathbb{F}_p^3$ because they are primitive. However, when p divides n we have $\langle \bar{P}, \bar{P}\rangle$=0 and $\langle \bar{Q}, \bar{Q}\rangle$=0 in $\mathbb{F}_p$. If we have $\bar{v}$ in $\mathbb{F}_p^3$ such that $\langle \bar{v}, \bar{v}\rangle \neq 0$ in $\mathbb{F}_p$ and $\langle s_{\bar{v}}\bar{P} - \bar{Q}, s_{\bar{v}}\bar{P} - \bar{Q}\rangle \neq 0$ in $\mathbb{F}_p$, then, taking v any lift in $\mathbb{Z}^3$ of $\bar{v}$, and taking $w := s_v P - Q$, we have $s_w s_v$ in $\mathcal{T}_{P,Q}(\mathbb{Z}[1/m]$ for a suitable m prime to p.

So, it remains to show that for k a finite field whose characteristic is not 2, and nonzero elements x and y in k^3 with $\langle x, x\rangle = \langle y, y\rangle$, there exists z in k^3 such that $\langle z, z\rangle = \langle x, x\rangle$, $\langle x - z, x - z\rangle \neq 0$ and $\langle z - y, z - y\rangle \neq 0$.

Let $a := \langle x, x\rangle$. Let V be the set of z in k^3 with $\langle z, z\rangle = a$. Let C be the set of v in k^3 with $\langle v, v\rangle = 0$, the nilcone or so. Then what we must show is that V is not contained in the union of $x + C$ and $y + C$. For v in C we have $x+v$ in V if and only if $\langle v, x\rangle = 0$. In other words, $V \cap (x+C) = x+(x^\perp \cap C)$. Similarly, $V \cap (y + C) = y + (y^\perp \cap C)$. Let q denote the number of elements if k. Then $V \cap (x + C)$ has $2q - 1$ if it is a union of two distinct k-rational lines, q elements if it is a line with multiplicity 2, and just 1 element if it is a union of conjugates lines. If $a = 0$ then $V = C$ and $x + C$ are cones with apex 0 and x respectively, on the same conic in the hyperplane at infinity and as x is in C both contain the line through 0 and x and both have the same tangent plane along that line. Therefore, if $a = 0$, both $V \cap (x + C)$ and $V \cap (y + C)$ consist of q elements, and as V has q^2 elements, V is not contained in the union of $x + C$ and $y + C$. Now assume $a \neq 0$. Then either V is split and has $(q + 1)^2 - (q + 1)$ elements, or it is not split and has no k-rational lines at all. In the first case V minus its intersections with $x + C$ and $y + C$ has at least $(q+1)^2 - (q+1) - 2(2q-1)$ elements, that is, at least $q^2 - 3q + 2$ elements, a number > 0. In the second case , we have at least

$q^2 + 1 - 2$ elements, also > 0.

Let $H^1(S, \mathcal{H})$ denote the set of isomorphism classes of right-$\mathcal{H}$-torsors on S (for the Zariski topology). Then the previous proposition shows that we have the map:

$$c : X_n(\mathbb{Z})^{\text{prim}} \to \mathrm{H}^1(S, \mathcal{H}), \quad Q \mapsto [\mathcal{T}_{P,Q}],$$

sending Q to the isomorphism class of $\mathcal{T}_{P,Q}$ (as a sheaf with a right action of $\mathcal{H}$). The following statements are then very standards.

Lemma 4.2.2 *Let Q_1 and Q_2 be in $X_n(\mathbb{Z})^{prim}$. Then Q_1 and Q_2 are in the same $G(\mathbb{Z})$-orbit if and only if they have the same image under c.*

Proof Assume first that Q_1 and Q_2 are in the same $G(\mathbb{Z})$-orbit. Let g be an element of $G(\mathbb{Z}) = \mathcal{G}(S)$ such that $gQ_1 = Q_2$. Then left-multiplication in $\mathcal{G}$ by g is an isomorphism from $\mathcal{T}_{P,Q_1}$ to $\mathcal{T}_{P,Q_2}$.

Now assume that $c(Q_1) = c(Q_2)$. Let ϕ be an isomorphism from $\mathcal{T}_{P,Q_1}$ to $\mathcal{T}_{P,Q_2}$. Let U be an open subset of S on which $\mathcal{T}_{P,Q_1}$ has a section, t, say. Then $\phi(t)$ is in $\mathcal{T}_{P,Q_2}(U)$, and $\phi(t)t^{-1}$ is in $\mathcal{T}_{Q_1,Q_2}$. We claim that this element $\phi(t)t^{-1}$ does not depend on the choice of t. Any choice t_1 is of the form $t.h$ for a unique h in $\mathcal{H}(U)$, and

$$\phi(t_1)t_1^{-1} = \phi(t.h)(t.h)^{-1} = \phi(t)h.h^{-1}.t^{-1} = \phi(t)t^{-1},$$

showing indeed what we claimed. But then all the local U are compatible, and there is a unique g in $\mathcal{T}_{Q_1,Q_2}(S) \subset \mathcal{G}(S)$ that induces ϕ.

Lemma 4.2.3 *An element of $H^1(S, \mathcal{H})$ is in the image of c if and only if it is mapped to the trivial element in $H^1(S, \mathcal{G})$ by the map induced by the inclusion $\mathcal{H} \to \mathcal{G}$.*

Proof For $\mathcal{T}$ a right-$\mathcal{H}$-torsor, the associated right-$\mathcal{G}$-torsor is the quotient of $\mathcal{T} \times \mathcal{G}$ by the action of $\mathcal{H}$ given (locally) by $(t, g) \mapsto (th, h^{-1}g)$. We denote this right-$\mathcal{G}$-torsor by $\mathcal{T} \otimes_{\mathcal{H}} \mathcal{G}$.

Let Q be in $X_n(\mathbb{Z})^{\text{prim}}$. Let $U \subset S$ be open, such that $\mathcal{T}_{P.Q}(U)$ is not empty. To t in $\mathcal{T}_{P.Q}(U)$ we associate the element (t, t^{-1}) of $(\mathcal{T} \times \mathcal{G})(U)$, and its image $\bar{t}$ in $(\mathcal{T} \otimes_{\mathcal{H}} \mathcal{G})(U)$. As t is unique up to $t_1 = t.h$ with h is unique in $\mathcal{H}(U)$, $\bar{t}$ does not depend on the choice of t and therefore defines an element of $(\mathcal{T} \otimes_{\mathcal{H}} \mathcal{G})(S)$, showing that $\mathcal{T} \otimes_{\mathcal{H}} \mathcal{G}$ is trivialisable.

Now assume that $\mathcal{T}$ is a right-$\mathcal{H}$-torsor such that $\mathcal{T} \otimes_{\mathcal{H}} \mathcal{G}$ is trivialisable. Let s be in $(\mathcal{T} \otimes_{\mathcal{H}} \mathcal{G})(S)$. Locally on S, s comes from a (t, g) in $(\mathcal{T} \times \mathcal{G})(U)$, unique up to $(t_1, g_1) = (t.h, h^{-1}.g)$ with h in $\mathcal{H}(U)$. Such a (t, g) gives us $Q_U := g^{-1}P$ in $X_n(U)$. This Q_U does not depend on the choice of (t, g) and therefore gives us a Q in $X_n(S) = X_n(\mathbb{Z})$ (note that X_n gives a sheaf for the Zariski topology). Sending t to g^{-1} is an isomorphism from $\mathcal{T}$ to $\mathcal{T}_{P,Q}$ on U that does not depend on the choice of t, hence is an isomorphism from $\mathcal{T}$ to $\mathcal{T}_{P,Q}$.

Lemma 4.2.4 *Every right-$\mathcal{G}$-torsor on S is trivialisable.*

Proof Let $\mathcal{O}$ denote the structure sheaf $\mathcal{O}_{\mathrm{Spec}(\mathbb{Z})}$. As $\mathcal{G}$ is the sheaf of automorphisms of $(\mathcal{O}^3, b, d)$, with b the standard symmetric bilinear form and $d : \mathcal{O} \to \det(\mathcal{O}^3)$ the standard trivialisation of the determinant (sending 1 to say $e_1 \wedge e_2 \wedge e_3$), $H^1(S, \mathcal{G})$ is the set of isomorphism classes of twists of $(\mathcal{O}^3, b, d)$ (for the Zariski topology). So, what we must show is that every such twist is isomorphic to $(\mathcal{O}^3, b, d)$.

Let $(\mathcal{M}, b_M, d_M)$ be a twist: $\mathcal{M}$ is a locally free $\mathcal{O}$-module of rank 3, b_M a symmetric $\mathcal{O}$-billinear form on $\mathcal{M}$ with values in $\mathcal{O}$, and d_M a trivialisation of $\det(\mathcal{M})$, such that $(\mathcal{M}, b_M, d_M)$ is locally isomorphic to $(\mathcal{O}^3, b, d)$. Then $M := \mathcal{M}(S)$ is a free $\mathbb{Z}$-module of rank 3, with a positive definite perfect symmetric $\mathbb{Z}$-valued bilinear form. This is because locally free module will be flat and a flat module over integral domain, i.e. $\mathbb{Z}$, is torsion-free. Since M is finitely generated and torsion-free then it's free module. Let m be a shortest non-zero element of M. If $\langle m, m\rangle \geq 2$, then the open ball with radius 1 in $M_{\mathbb{R}}$ maps injectively into $M_{\mathbb{R}}/M$, hence the volume of $M_{\mathbb{R}}/M$ is at least $4\pi/3$. But that volume is 1 because its square, i.e. discriminant of (M, B_M), is a positive integer not divisible by any prime number. Hence there is an element m in M with $\langle m, m\rangle = 1$. Then $M = \mathbb{Z}m \oplus m^{\perp}$, and continuing our argument with $m^{\perp}$ shows that M has an orthonormal basis.

Putting things together, we have proved the following

Proposition 4.2.5 *Assume $X_n(\mathbb{Z})^{prim} \neq \emptyset$. Then the map c above induces a bijection*

$$SO_3(\mathbb{Z}) \setminus X_n(\mathbb{Z})^{prim} \to H^1(S, \mathcal{H}).$$

Let us now study the sheaf $\mathcal{H}$ and its first cohomology group, in order to relate it to a class number of an imaginary quadratic order. Because of difficulties at the prime number 2 we introduce the following two lemmas.

Lemma 4.2.6 *The natural morphism $SO_3(\mathbb{Z}_{(2)}) \to SO_3(\mathbb{Q})$ is an isomorphism.*

Proof We claim that $O_3(\mathbb{Z}_{(2)}) \to O_3(\mathbb{Q})$ is an isomorphism. The claim implies the statement that we must prove. To prove our claim, first observe that the morphism is injective because $\mathbb{Z}_{(2)} \to \mathbb{Q}$ is. Hence it suffices to prove that $O_3(\mathbb{Z}_{(2)}) \to O_3(\mathbb{Q})$ is surjective. It is standard fact that $O_3(\mathbb{Q})$ is generated by symmetries (true for all $O_n(\mathbb{Q})$; by showing that the standard basis can be mapped to any orthonormal basis by composition of symmetries in suitable hyperplanes). Hence it suffices to show that any symmetry s in $O_3(\mathbb{Q})$ is in $O_3(\mathbb{Z}_{(2)})$. But such symmetry is of the form s_v above with v is a primitive element of $\mathbb{Z}^3$. For such a v, the integer $\langle v, v\rangle$ is not divisible by 4 (here we really use that v is in $\mathbb{Z}^3$ and not in $\mathbb{Z}^d$ with $d > 3$), and hence s_v is in $O_3(\mathbb{Z}_{(2)})$.

Note that our definition of $H^1(S, \mathcal{H})$ will coincide with definition by Čech cohomology, also since H is commutative it is the same with the derive functor definition of cohomology. It's allowed us to use various tools.

Lemma 4.2.7 *The natural morphism $H^1(Spec(\mathbb{Z}), \mathcal{H}) \to H^1(Spec(\mathbb{Z}[1/2]), \mathcal{H})$ is an isomorphism.*

Proof For every odd integer m we have the exact sequence (The Mayer-Vietoris sequence theorem 3.6.7) coming from the covering of Spec($\mathbb{Z}$) by the disjoint union of the spectra of $\mathbb{Z}[1/m]$ and $\mathbb{Z}[1/2]$:

$$0 \to \mathcal{H}(\mathbb{Z}) \to \mathcal{H}(\mathbb{Z}[1/m]) \oplus \mathcal{H}(\mathbb{Z}[1/2]) \to \mathcal{H}(\mathbb{Z}[1/2m]) \to$$
$$\to H^1(\mathbb{Z}, \mathcal{H}) \to H^1(\mathbb{Z}[1/m], \mathcal{H}) \oplus H^1(\mathbb{Z}[1/2], \mathcal{H}) \to H^1(\mathbb{Z}[1/2m], \mathcal{H}) \to 0.$$

Note that H^2 becomes 0 by Grothendieck's theorem (theorem 3.6.8) because of the dimension equal to 1. For varying m we have a direct system of exact sequence of abelian groups, and as this system is filtered its colimit exact, giving exact sequence:

$$0 \to \mathcal{H}(\mathbb{Z}) \to \mathcal{H}_2 \oplus \mathcal{H}(\mathbb{Z}[1/2]) \to \mathcal{H}_\eta \to H^1(\mathbb{Z}, \mathcal{H}) \to H^1(\mathbb{Z}[1/2], \mathcal{H}) \to 0,$$

where $\mathcal{H}_2$ and $\mathcal{H}_\eta$ are the stalk of $\mathcal{H}$ at 2 and at the generic point η of Spec($\mathbb{Z}$), respectively, and where we have used that the limits of the $H^1(\mathbb{Z}[1/m], \mathcal{H})$ and the $H^1(\mathbb{Z}[1/2m], \mathcal{H})$ are zero (every Zariski torsor will be trivial on some neighborhood of 2 and η by definition of torsor itself).

Now $\mathcal{H}_2$ is the stabilizer of P in $SO_3(\mathbb{Z}_{(2)})$, and $\mathcal{H}_\eta$ is the stabilizer of P in $SO_3(\mathbb{Q})$. Then the previous lemma implies that $\mathcal{H}_2 \to \mathcal{H}_\eta$ is an isomorphism, and that proves the statement of the lemma.

Combining the result of the last lemma with the last proposition gives that

$$SO_3(\mathbb{Z})\backslash X_n(\mathbb{Z})^{\text{prim}} \to H^1(\text{Spec}(\mathbb{Z}[1/2]), \mathcal{H})$$

is a bijection.

Next we must determine H. We just know it over $\mathbb{Z}[1/2]$.

Lemma 4.2.8 *H does not depend on P: for every $Q \in X(\mathbb{Z})^{prim}, G_Q = H$.*

Proof Locally for some open $U \subset S$, $Q = gP$ where $g \in G(U)$. Then we have isomorphism

$$H = G_P \xrightarrow{\sim} G_Q, \quad h \mapsto ghg^{-1}.$$

The isomorphism is independent of the choice of g. Indeed, if $Q = gP = g'P$ for other $g' \in G(U)$ then $g' = gh'$ for some $h \in H(U)$. Since H is commutative, it gives the same map $h \mapsto ghg^{-1}$.

Now we start relating $\mathcal{H}$ to an imaginary quadratic order, by considering $P^\perp$ as free $\mathbb{Z}$-module of rank 2 with the positive definite symmetric bilinear form obtained by restricting that of $\mathbb{Z}^3$. We have the exact sequence of $\mathbb{Z}$-modules:

$$0 \to P^\perp \to \mathbb{Z}^3 \to \mathbb{Z} \to 0, \quad \text{with } \mathbb{Z}^3 \to \mathbb{Z}, Q \mapsto \langle Q, P \rangle.$$

Let N be the group scheme $SO(P^\perp)$ over $\mathbb{Z}$, and let $\mathcal{N}$ be the sheaf of groups on Spec($\mathbb{Z}$) (with the Zariski topology) given by N. The action of H on $P^\perp$ gives a morphism $H \to N$, and by that an injective morphism $\mathcal{H} \to \mathcal{N}$.

Lemma 4.2.9 *The morphism $H \to N$ is an isomorphism over $\mathbb{Z}[1/n]$.*

Proof The element $(1/n)P$ of $\mathbb{Z}[1/n]^3$ is mapped to 1 in $\mathbb{Z}[1/n]$ in the exact sequence above with kernel $P^\perp$. Therefore, $\mathbb{Z}[1/n]^3$ is the orthogonal direct sum of $P^\perp_{\mathbb{Z}[1/n]}$ and $\mathbb{Z}[1/n].P$. As H is the stabilizer in SO_3 of P it is the same as N.

It turns out that at prime $p \neq 2$ dividing n the morphism $H \to N$ is not an isomorphism. For such a prime p, $\langle P, P\rangle$ is zero in $\mathbb{F}_p$, and therefore $P^{\perp}_{\mathbb{F}_p}$ is the sub-$\mathbb{F}_p$-vector space of $\mathbb{F}_p^3$ orthogonal to the non-zero element $P_{\mathbb{F}_p}$ which satisfies $\langle P_{\mathbb{F}_p}, P_{\mathbb{F}_p}\rangle = 0$. With respect to a suitable basis e_i of $\mathbb{F}_p^3$ with $e_1 = P_{\mathbb{F}_p}$, the symmetric bilinear form b is the standard one: $b(e_1, e_3) = b(e_2, e_2) = 1$, and $b(e_i, e_j) = 0$ otherwise. Then (e_1, e_2) is a basis of $P^{\perp}$. Direct computation shows that with respect to this basis $N_{\mathbb{F}_p}$ and $H_{\mathbb{F}_p}$ are the following matrix groups

$$N_{\mathbb{F}_p} = \left\{ \begin{bmatrix} a & b \\ 0 & 1/a \end{bmatrix} : a^2 = 1 \right\} \quad \text{and} \quad H_{\mathbb{F}_p} = \left\{ \begin{bmatrix} 1 & b & -b^2/2 \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{bmatrix} \right\}$$

over $\mathbb{F}_p$.

Lemma 4.2.10 *Let $p \neq 2$ be a prime dividing n. Then $H(\mathbb{Z}_{(p)})$ is the set of g in $N(\mathbb{Z}_{(p)})$ that fix $P_{\mathbb{F}_p}$ in $P^{\perp}_{\mathbb{F}_p}$.*

Proof Let g be in $N(\mathbb{Z}_{(p)})$ 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 $P^{\perp}_{\mathbb{F}_p} - \mathbb{F}_p P_{\mathbb{F}_p}$ (elements in $P^{\perp}_{\mathbb{F}_p}$ which is not in $\mathbb{F}_p P_{\mathbb{F}_p}$). Then $\langle v, v\rangle \neq 0$ in $\mathbb{F}_p$, and, with s_v the symmetry in $P^{\perp}_{\mathbb{Z}_{(p)}}$ with respect to v, $s_v g$ is an automorphism of $P^{\perp}$ of determinant -1. Then $s_v g$ has eigenvalues 1 and -1 (note that $(s_v g)^T . s_v g = id$). 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. Then $\mathbb{F}_p P_{\mathbb{F}_p} = L^+_{\mathbb{F}_p}$, hence $\mathbb{F}_p P_{\mathbb{F}_p} \neq L^-_{\mathbb{F}_p}$ because $\mathbb{F}_p P_{\mathbb{F}_p}$ is the set x in $P^{\perp}_{\mathbb{F}_p}$ such that $\langle x, x\rangle = 0$. (Recall that a symmetry s_v fixes vectors that perpendicular to v). 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 $H(\mathbb{Z}_{(p)})$.

We define Φ to be the sheaf on Spec($\mathbb{Z}$), 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 Spec($\mathbb{F}_p$) via the embedding i_p of Spec($\mathbb{F}_p$) into Spec($\mathbb{Z}$). Then for each such p the map $N(\mathbb{Z}_{(p)}) \to \mathbb{F}_2$ that sends g to 0 if

$gP_{\mathbb{F}_p} = P_{\mathbb{F}_p}$ in $P^{\perp}_{\mathbb{F}_p}$ and to 1 otherwise is a morphism from $\mathcal{N}_p$ to $\mathbb{F}_2$, giving together a surjective morphism $\mathcal{N} \to \Phi$. We have proved the following proposition

Proposition 4.2.11 *The sequence* $0 \to \mathcal{H} \to \mathcal{N} \to \Phi \to 0$ *of sheaves of* $\mathbb{Z}$*-modules is exact on Spec*$(\mathbb{Z}[1/2])$.

Lemma 4.2.12 *The symmetric bilinear from* b *on* $P^{\perp}$ *obtained by restricting* $\langle \cdot, \cdot \rangle$ *from* $\mathbb{Z}^3$ *is positive definite, and its discriminant is* n.

Proof Let us first prove the primitivity (the positive definiteness is obvious). Let (f_1, f_2) a $\mathbb{Z}$-basis of $P^{\perp}$. As $\mathbb{Z}^3/P^{\perp}$ is free (of rank one), we can (and do) take an f_3 in $\mathbb{Z}^3$ such that (f_1, f_2, f_3) is a $\mathbb{Z}$-basis of $\mathbb{Z}^3$. Let g be the Gramm matrix of b with respect to the basis f : $g_{i,j} = b(f_i, f_j)$. As the discriminant of $(\mathbb{Z}^3, \langle \cdot, \cdot \rangle)$ equals 1, we have $\det(g)$=1. In particular, at every prime number p, the rank of g in $M_3(\mathbb{F}_p)$ equals 3. It follows that not all $g_{i,j}$ with $i \leq 2$ and $j \leq 2$ can be zero in $\mathbb{F}_p$. This concludes the proof of primitivity.

Then we consider $\mathrm{discr}(P^{\perp}, b)$. 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

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

We conclude that $\mathrm{discr}(P^{\perp}, b) = n$.

Now it is time to say more about N and $\mathcal{N}$, at least over $\mathbb{Z}[1/2]$. We define a ring O by (see also example in section 2.4.3):

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

We let T denote the group scheme over $\mathbb{Z}$ obtained by restriction of scalars from O to $\mathbb{Z}[1/2]$ applied to $\mathbb{G}_{m,O}$:

$$T := \mathrm{Res}_{\mathbb{Z}[1/2,\sqrt{-n}]/\mathbb{Z}[1/2]} \mathbb{G}_m = \mathrm{Spec}\ (\mathbb{Z}[1/2][a, b]/(a^2 + nb^2)).$$

So for any $\mathbb{Z}[1/2]$-algebra A we obtain:

$$T(A) = (A[u]/(u^2 + n))^{\times} = \{a_1 + a_2.u : a_1^2 + na_2^2 \in A^{\times}\}.$$

The norm map from O to $\mathbb{Z}[1/2]$ induces a morphism:

$$\mathrm{Norm} : T \to \mathbb{G}_{m,\mathbb{Z}[1/2]} : \quad a_1 + a_2.u \mapsto a_1^2 + na_2^2.$$

We let T_1 denote the kernel of this norm morphism, i.e., T_1 is the spectrum of $\mathbb{Z}[1/2, a, b]/(a^2 + nb^2 - 1)$. We also have injective morphism $\mathbb{G}_m \rightarrowtail T : a \mapsto a + 0.u$. We have following proposition:

Proposition 4.2.13 *We have an exact sequence of group schemes over* $\mathbb{Z}[1/2]$ *for the Zariski topology (big site),*

$$\mathbb{G}_m \rightarrowtail T \twoheadrightarrow H_{\mathbb{Z}[1/2]}$$

To prove this, we need several lemmas. First we prove that the group scheme N is equal to T_1 over $\mathbb{Z}[1/2]$.

Lemma 4.2.14 *The group scheme* $N_{\mathbb{Z}[1/2]}$ *over* $\mathbb{Z}[1/2]$ *is isomorphic to* T_1.

Proof We claim that any (M, b, d) with M 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, is, locally for the étale topology on $\mathrm{Spec}(\mathbb{Z}[1/2])$ is isomorphic to $\mathbb{Z}[1/2]^2$ with diagonal form $(1, n)$ and with $d : 1 \mapsto e_1 \wedge e_2$.

We prove the claim. Let g be in $M_2(\mathbb{Z})$ be the Gramm matrix b with respect to some $\mathbb{Z}[1/2]$-basis of $M_{\mathbb{Z}[1/2]}$, 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 $\mathbb{Z}[1/2, \sqrt{k}]$ 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 Gramm 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 $\mathbb{Z}[1/2k]$, and $\mathrm{Spec}(\mathbb{Z}[1/2k])$ is an open neighborhood in $\mathrm{Spec}(\mathbb{Z}[1/2])$ of $\mathrm{Spec}(\mathbb{F}_p)$.

Now we derive the conclusions of the lemma from the claim by étale descent. Recall that $N = SO(P^\perp)$, hence N is the automorphism group scheme of $(P^\perp, b, d)$ for any choice of orientation d. Similarly, T_1 is the automorphism group scheme of $(\mathbb{Z}^2[1/2]^2, (1, n), e_1 \wedge e_2)$. (We can work this by equation in section 2.3 and do some computation to get equation for T_1). Étale locally on $\mathrm{Spec}([\mathbb{Z}[1/2])$ our $(P^\perp, b, d)$ is isomorphic to $(\mathbb{Z}^2[1/2]^2, (1, n), e_1 \wedge e_2)$.

Let $U = \{(U_i \to \mathrm{Spec}(\mathbb{Z}[1/2])_{i\in I}\}$ be a cover and ϕ_i an isomorphism from $(P^\perp, b, d)$ to $(\mathbb{Z}^2[1/2]^2, (1,n), e_1 \wedge e_2)$ over U_i. Then each ϕ_i induces an isomorphism Φ_i over U_i from N to T_1. The fact that $T_1(\bar{\mathbb{Q}})$ is commutative implies that these Φ_i do not depend on the choice of ϕ_i. Therefore, the $(\Phi_i)_{i\in I}$ are compatible. By étale descent for morphisms of affine schemes, we get an isomorphism ϕ from N to T_1.

We observe that the fibres of T_1 at the primes $p \neq 2$ dividing n are reducible, as they are the spectrum of $\mathbb{F}_p[a,b]/(a^2-1)$. We let T_1^0 be the open subscheme of T_1 obtained by removing the irreducible components of these fibres given by $a = -1$. So T_1 and T_1^0 is equal over $\mathbb{Z}[1/2n]$. Let Φ be the étale group scheme over $\mathbb{Z}[1/2]$ obtained by gluing the two sections of the constant group scheme $(\mathbb{F}_2)_{\mathbb{Z}[1/2]}$ outside the primes $p \neq 2$ dividing n. And as a sheaf over $\mathbb{Z}[1/2]$, we have

$$\Phi = \oplus_{2\neq p|n} i_{p,*}\mathbb{F}_2 : (\text{given by equation } a_1^2 + 0.a_2^2 = 1 \text{ over } \mathbb{F}_p).$$

Then we get a short exact sequence of group schemes over $\mathbb{Z}[1/2]$:

$$0 \to T_1^0 \to T_1 \to \Phi \to 0,$$

in which $T_1 \to \Phi$, as a morphism of schemes (not group schemes), has two sections given by $0 \mapsto 1$ and $1 \mapsto -1$. So here we have a quotient that is surjective even in the Zariski topology.

The previous lemma shows that under our isomorphism between N and T_1, we have following lemma:

Lemma 4.2.15 *$H \xrightarrow{\sim} T_1^0$ is isomorphism over $\mathbb{Z}[1/2]$.*

To complete our proof for our proposition, we need to prove $T \twoheadrightarrow T_1^0$ has a kernel $\mathbb{G}_m$. To see this, consider the automorphism

$$T \to T : a_1 + u.a_2 \mapsto a_1 - u.a_2.$$

Then the map $T \to T$ given by $a_1 + u.a_2 \mapsto \frac{a_1+u.a_2}{a_1-u.2_2}$ has kernel $\mathbb{G}_m$ and image T_1^0.

Now from the proposition, we have long exact sequence as follows:

$$0 \to \mathbb{G}_m(\mathrm{Spec}\mathbb{Z}[1/2]) \to T(\mathrm{Spec}\mathbb{Z}[1/2]) \to H(\mathrm{Spec}\mathbb{Z}[1/2]) \to H^1(\mathrm{Spec}\mathbb{Z}[1/2], \mathbb{G}_m) \to$$

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

Now $H^1(\mathrm{Spec}\mathbb{Z}[1/2], \mathbb{G}_m) = \mathrm{Pic}(\mathbb{Z}[1/2])$ which is 0 because $\mathbb{Z}[1/2]$ is Principal Ideal domain. Also from Grothendieck's vanishing theorem (theorem 3.6.8), we have $H^2(\mathrm{Spec}\mathbb{Z}[1/2], \mathbb{G}_m) = 0$ since dimension of $\mathrm{Spec}\mathbb{Z}[1/2]$ is equal to 1. Thus we obtain:

$$H^1(\mathrm{Spec}\mathbb{Z}[1/2], T) \xrightarrow{\sim} H^1(\mathrm{Spec}\mathbb{Z}[1/2], H).$$

Proposition 4.2.16 *The first cohomology group $H^1(Spec\mathbb{Z}[1/2], T)$ is equal to $Pic(O)$=$Pic(\mathbb{Z}[1/2, \sqrt{-n}])$.*

Proof First we can consider $H^1(\mathrm{Spec}\mathbb{Z}[1/2], T)$ as a group of $\mathbb{G}_m$-torsor on $\mathrm{Spec}(\mathbb{Z}[1/2, \sqrt{-n}])$ that can be trivialized on covers that come from $\mathrm{Spec}(\mathbb{Z}[1/2])$. In other words, $H^1(\mathrm{Spec}\mathbb{Z}[1/2], T)$ is the group of invertible $\mathbb{Z}[1/2, \sqrt{-n}]$-modules M with the property that for each prime number p there is an integer a not divisible by p such that M becomes free over $\mathbb{Z}[1/2, \sqrt{-n}, 1/a]$.

We will prove more general statement as follows: Let $f : T = \mathrm{Spec}B \to S = \mathrm{Spec}A$ be a finite morphism, where T is Noetherian. Suppose $L = \tilde{M} \in \mathrm{Pic}(T)$ is an invertible sheaf on T. Then for any t in T and $s = f(t)$, we can find an open subset V of T that contains t such that $L_{|V} \simeq \mathcal{O}_{T|V}$ and $V \supseteq f^{-1}(S_i)$ where S_i is an open subset that contains s. We use following lemma:

Lemma 4.2.17 *Let B be a Noetherian ring and $m_1, ..., m_n$ are maximal ideals. Suppose $L = \tilde{M}$ is an invertible sheaf on $SpecB$, then there exists an open subset V contains $\{m_1, ..., m_n\}$ such that $L_{|V} \simeq \mathcal{O}_{T|V}$.*

Proof For each m_i, let V_i be an open subset contains it such that $L_{|V_i} \simeq \mathcal{O}_{T|V_i}$. We can take $V_i = D(f_i)$ a principal open subset. Now consider the stalk at m_i

$$L_{m_i}/m_iL_{m_i} = M/m_iM = M \otimes_B B/m_i = (M \otimes_B B_{m_i}) \otimes_{B_{m_i}} (B_{m_i}/m_iB_{m_i})$$

$$= L_{m_i} \otimes_{B_{m_i}} k(m_i),$$

which means that M/m_iM is 1-dimensional vector space over $B/m_i = k(m_i)$. So we can find a basis e_i such that $M/m_iM = e_i.B/m_i$. By Chinese reminder theorem we have

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

after tensoring by M over B, we will get

$$M \to \oplus_{i=1}^{n} M/m_i M \to 0.$$

So there exists e in M that maps to $(e_i)_{1\leq i\leq n}$. Now $M \supset e.B$, because the image of e in M/m_iM is a basis over B/m_i, by Nakayama's lemma we obtain $e.B_{m_i} = M_{m_i}$. This implies $L_{m_i} = e.\mathcal{O}_{T,m_i}$, so there exists $D(f_i)$ contains m_i such that $L_{|D(f_i)} = e.\mathcal{O}_{T|D(f_i)}$. If we take $V = \cup D(f_i)$ then $L_{|V} = e.\mathcal{O}_{T|V}$ as desired.

In fact we can change the maximal ideal m_i with prime ideal p_i in the argument by considering that if V is an open subset that contains m_i then for any prime ideal $p_i \subset m_i$ is also contained in V. This lemma can prove our statement by considering $f^{-1}(s)$ is a finite set in T. Thus we can find $V \supset f^{-1}(s)$ such that $L_{|V} \simeq \mathcal{O}_{T|V}$. Because finite implies proper, in particular f is closed map, so $f : T \setminus V \to Z$ a closed subset of S. And $s \notin Z$ which means $f^{-1}(S_i := S \setminus Z) \subset V$ as the statement.

By taking $B =$Spec$(\mathbb{Z}[1/2, \sqrt{-n}])$ and $A =$Spec$(\mathbb{Z}[1/2])$ we have proven the proposition.

We almost finish our proof of Gauss's theorem, now let $X_n(\mathbb{Z}[1/2])^{\text{prim}}$ denote the subset of $X_n(\mathbb{Z}[1/2])$ consiting of the (x, y, z) with $\mathbb{Z}[1/2].x + \mathbb{Z}[1/2].y + \mathbb{Z}[1/2].z = \mathbb{Z}[1/2]$.

Lemma 4.2.18 *We have*

$$X_n(\mathbb{Z})^{prim} = X_n(\mathbb{Z}[1/2])^{prim}$$

$$SO_3(\mathbb{Z}) = SO_3(\mathbb{Z}[1/2])$$

$$SO_3(\mathbb{Z}) \setminus X_n(\mathbb{Z})^{prim} = SO_3(\mathbb{Z}[1/2]) \setminus X_n(\mathbb{Z}[1/2])^{prim}.$$

Proof Let (x, y, z) be in $X_n(\mathbb{Z}[1/2])^{\text{prim}}$. Write (x, y, z) as $2^m(x_1, y_1, z_1)$ with m in $\mathbb{Z}$ and x_1, y_1 and z_1 in $\mathbb{Z}$ and not all multiple of 2. Then $x_1^2 + y_1^2 + z_1^2$ is 1 or 2 or 3 in $\mathbb{Z}/4\mathbb{Z}$. We conclude that $m = 0$ and that (x, y, z) is in $X_n(\mathbb{Z})^{\text{prim}}$. We have already shown $SO_3(\mathbb{Z}_{(2)}) = SO_3(\mathbb{Q})$. This implies the other two equalities.

So we get following

$$G(\mathbb{Z}) \setminus X_n(\mathbb{Z})^{\text{prim}} = G(\mathbb{Z}[1/2]) \setminus X_n(\mathbb{Z}[1/2])^{\text{prim}} \xrightarrow{\sim} \text{Pic}(\mathbb{Z}[1/2, \sqrt{-n}]).$$

Indeed, we have proved: if $X_n(\mathbb{Z})^{\text{prim}} \neq \emptyset$, then

$$\begin{aligned} \#X_n(\mathbb{Z})^{\text{prim}} &= \frac{\#G(\mathbb{Z}[1/2])}{\#H(\mathbb{Z}[1/2])}.\#\text{Pic}(\mathbb{Z}[1/2, \sqrt{-n}]) \\ &= \frac{24}{\mathbb{Z}[1/2, \sqrt{-n}]^{\times,\circ}_{tors}}.\text{Pic}(\mathbb{Z}[1/2, \sqrt{-n}]), \end{aligned}$$

where $\mathbb{Z}[1/2, \sqrt{-n}]^{\times,\circ}_{tors} = \{t = a_1 + a_2.\sqrt{-n} \in \mathbb{Z}[1/2.\sqrt{-n}]^{\times} : \text{torsion}, \forall p \neq 2, p|n : a_1 \equiv 1(p)\}$. If n are 1, 2, 5 or 6 mod 8 then $O = O_{-4n}[1/2]$, while if n is 3 mod 8 then $O = O_{-n}[1/2]$. The fact that 2 is inert or ramified in O_d for $d = -n$ or $d = -4n$ implies that Pic(O)=Pic(O_d). And we have the proof of Gauss's theorem.

References

[1] B.Edixhoven: *On Gauss's 3 square theorem*, preprint (2011).

[2] P.Gille and L. Moret-Bally: *Actions algébriques de groupes arithmétiques*, to appear in "Torsors, theory and applications", Edinburg (2011), Proceedings of the London Mathematical Society, edited by V. Batyrev et A. Skorobogatov.

[3] G. Shimura: *Quadratic diophantine equations, the class number, and the mass formula*, Bulletin of the AMS, Volume 43, Number 3, July (2006).

[4] M.Bhargava and B.H. Gross: *Arithmetic invariant theory*, arXiv (2012).

[5] Q.Liu: *Algebraic Geometry and Arithmetic Curves*, Oxford university press (2002).

[6] R. Hartshorne: *Algebraic Geometry*, Springer GTM 52 (1977).

[7] W.C. Waterhouse: *Introduction to Affine Group Schemes*, Springer-Verlag GTM 66 (1979).

[8] J.S.Milne: *Basic Theory of Affine Group Schemes*, course notes version 1.00 (2012).

[9] B.Poonen: *Rational points on varieties*, course notes (2008).

[10] J.S.Milne: *Étale cohomology*, Princeton university press (1980).

[11] J.S.Milne: *Lectures on Étale Cohomology*, course notes version 2.20 (2012).

[12] S.Bosch, W. Lütkebohmert, M. Raynaud: *Néron Models*, Springer-Verlag (1990).