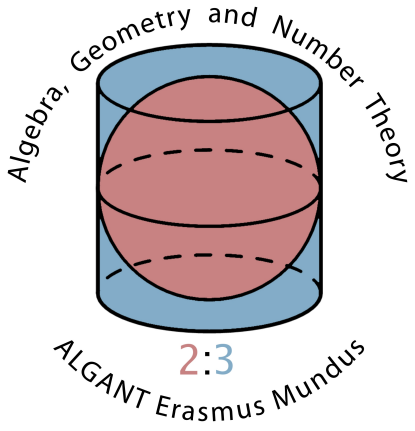

Integral points on 2-dimensional quadrics over curves

Luca Giovenzana
gemegiove92@hotmail.it

Advised by Prof. Dr. S.J. Edixhoven

Universiteit Leiden

Università degli Studi di Milano

ALGANT Master's Thesis - 20 July 2016

Contents

1 Introduction

The subject of this thesis is inspired by some side results obtained in Albert Gunawan's PhD thesis [2]. While Gunawan works with the ring of integers, we start considering a similar problem but over a different base scheme, namely $\mathrm{Spec}(k[t])$ for a field k. Assuming that the field is algebraically closed and of characteristic different from 2, we obtain a similar result.

More precisely, we consider the solutions to the equation:

$$xy + z^2 = f$$

where $f \in k[t]$ is a squarefree polynomial of odd degree. Let $X_f(k[t])$ denote the set of primitive solutions in $k[t]$ and let $SO(q)(k[t])$ denote the special orthogonal group of matrices with entries in $k[t]$ which preserve the quadratic form $k[t]^3 \to k[t]$, $(x, y, z) \mapsto xy + z^2$; the group $SO(q)(k[t])$ acts on the set $X_f(k[t])$ in a natural way. In Chapter 3 we prove that there is a bijection:

$$SO(q)(k[t]) \setminus X_f(k[t]) \xrightarrow{\sim} \mathrm{Pic}^\circ(C)$$

where C denotes the completion of the affine curve $\mathrm{Spec}(\frac{k[t,v]}{(v^2-f)})$.

Inspired by this result, we translate the problem to a different setting; in the last chapter we consider the analogous problem for schemes over $\mathbb{P}^1_k$. We fix f a global section of the invertible sheaf $\mathcal{O}(2d)$ on $(Sch_{|\mathbb{P}^1_k})_{Zar}$ and we study the solutions to the equation:

$$xy + z^2 = f$$

for x, y, z local sections of $\mathcal{O}(d)$.
Assume that f restricted to $\mathbb{P}^1_k$ is represented by a polynomial of degree $2d$; let X_f be the scheme parametrizing the solutions of that equations over $(Sch_{|\mathbb{P}^1_k})_{Zar}$ and let $SO(q)$ be the group scheme defined by the quadric $q : \mathcal{O}(d)^3 \to \mathcal{O}(2d)$ described $\forall Y \in Sch_{|\mathbb{P}^1_k}$, $\forall (a, b, c) \in \mathcal{O}(d)^3(Y)$ by $q(a, b, c) = ab + c^2$. The group scheme $SO(q)$ acts on X_f and in Chapter 4 we exhibit a map:

$$SO(q)(\mathbb{P}^1_k) \setminus X_f(\mathbb{P}^1_k) \to \mathrm{Pic}(C)$$

where C is the curve defined as the zero locus of $s^2 - f$ for s a local section of $\mathcal{O}(d)$.

Many questions arise from this result, maybe some of them can be addressed in a future work.

2 A first variation

2.1 The setting

In Gunawan's thesis ([2]), a theorem from Gauss is studied with the language of modern sheaf theory, namely counting primitive solutions of the equation:

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

with n a natural number and with x, y, z varying in the ring of integers.

As a first variation on the theme, we will consider as base ring $R := k[t]$ where k is an algebraically closed field with characteristic different from 2. We start considering the set of solutions in R^3 to the equation:

$$q(x, y, z) = f$$

where f is in R and q is the quadratic form $q(x, y, x) = xy + z^2$; since we are assuming that 2 is invertible as section of the base scheme $\mathrm{Spec}(R)$, there is a perfect correspondence between quadratic forms and symmetric bilinear ones, so we will denote, throughout the whole thesis, with b the bilinear form associated to q. In the following, we will see how to modify Gunawan's method in order to make it work in these hypotheses and which assumptions are needed to do some geometry.

The set of solutions is clearly described as R-points of a scheme. To see this we proceed as follows, for every ideal I in a ring A, let $Z(I) \subseteq \mathrm{Spec}(A)$ denote the associated Zariski closed; moreover let $A^3_R = \mathrm{Spec}(R[x, y, z])$. Define $\tilde{X_f} := Z((q(x, y, z) - f)) \subseteq \mathbb{A}^3_R$, then for every R-algebra A, the A-points consist of the solutions to the equation we are considering:

$$\tilde{X}_f(A) = \{(a, b, c) \in A^3 |\ q(a, b, c) - f = 0\}.$$

We restrict our attention to the set of primitive solutions, thus we shall consider another scheme: for our purpose it is enough to intersect the closed subscheme $\tilde{X_f}$ with the open subscheme $\mathbb{A}^3_R \setminus Z((x, y, z)) \hookrightarrow \mathbb{A}^3_R$. Therefore the R-points of the intersection, say X_f, are the primitive solutions:

$$X_f(R) = \{(a, b, c) \in R^3 |\ q(a, b, c) - f = 0 \text{ and } gcd(a, b, c) = 1\}$$

and for an arbitrary R-algebra A, the primitive condition can be restated saying that

$$X_f(A) = \{(a, b, c) \in A^3 |\ q(a, b, c) - f = 0 \text{ and } Z(a) \cap Z(b) \cap Z(c) = \emptyset\}$$

i.e. a, b, c are global sections of $\mathbb{A}_A$ with no common zeroes. There is a natural sheaf of groups acting on it, indeed the sheaf of groups $\mathcal{G}$ consisting of the linear automorphisms of $\mathbb{A}^3_R$ for which the quadratic form q is invariant, i.e. for every R-algebra A we have:

$$\mathcal{G}(A) = \mathrm{SO}(b)(A) = \{m \in \mathrm{GL}_3(A) | mQm^t = Q \text{ and } det(m) = 1\}$$

where Q is the matrix associated to q. Thus $\mathcal{G}$ is represented over the big Zariski site of schemes over R by the group scheme $SO_R(b)$. We take now a little break: the next section is a digression on the theory of torsors that we will use later.

2.2 Sheaves of groups acting on sheaves of sets:

The category of abelian sheaves over a topological space (or over a site) is known to be abelian and the cohomology groups can be defined thanks to the theory of derived functors. In case one considers sheaves of non necessarily abelian groups (which arise naturally in geometry) something can be recovered. In this chapter we outline the basic things we need about that. We will mainly follow [3], which is a complete treatment of the theory

Instead of working on a topological space we will make use of the more general notion of a site; for this, we start recalling the basic definitions:

Definition 1. Let $\mathcal{C}$ be a category. For a Grothendieck topology on it we mean the assignment to every object X in $\mathcal{C}$ of a collection of *coverings* $\{U_i \to X\}_{i\in I}$ such that the following axioms are satisfied:

- for every isomorphism $\gamma : U \to X$, $\{\gamma : U \to X\}$ is a covering of X
- for every covering $\{U_i \to X\}_{i\in I}$ of X and any arrow $f : V \to X$, the pull-backs $U_i \times V$ exist and the collection $\{U_i \times V \to V\}_{i\in I}$ is a covering of V.
- for every $\{U_i \to X\}_{i\in I}$ covering of X and $\{V_{i,j} \to U_i\}_{j\in J_i}$ covering of U_i, the collection of composites $\{V_{ij} \to V_i \to X\}_{i\in I, j\in J_i}$ is a covering of X.

A category with a Grothendieck topology is called a site.

We give some examples to introduce notation that will be used later.

Example 2.

1. To see how this is a generalization of giving a topology on a set, consider a topological space X and let $open(X)$ the category whose objects are the open subset of X and the arrows are the inclusions. The category $open(X)$ has a natural structure of a site with the coverings given by jointly surjective families $\{U_i \to U\}$.
2. In more generality one can consider the Grothendieck topology on the category of topological spaces, where for every topological space X a covering is a jointly surjective collection of open embeddings $\{U_i \to X\}_{i\in I}$.
3. In analogy with the first two examples one can consider schemes instead of simple topological spaces; for schemes S and X, we can therefore consider the following sites:
   - the small Zariski site X_{Zar} is given by the full subcategory of $Sch_{/X}$ consisting of open immersions $U \to X$; for every object $U \to X$, the coverings are jointly surjective collections $\{U_i \to U\}_{i\in I}$;
   - the big Zariski site $(Sch_{/S})_{Zar}$ consists of all the schemes over S and for every object $X \to S$ a covering is given by a jointly surjective collection of open immersions $\{U_i \to X\}_{i\in I}$;
   - the small étale site $X_{ét}$ is given by the full subcategory of $Sch_{/X}$ consisting of objects $U \to X$ étale; for every object $U \to X$, a covering is given by a jointly surjective collection $\{U_i \to U\}_{i\in I}$ of (necessarily étale) morphisms;

- the big étale site $(Sch_{/S})_{\acute{e}t}$ consists of the category of all schemes over S, where for every object $X \to S$ the coverings are given by jointly surjective collections $\{U_i \to X\}_{i\in I}$ of étale morphisms.

Clearly, having defined a topology, we want to speak about sheaves:

Definition 3. Let $\mathcal{C}$ be a site, a (contravariant) functor $F : \mathcal{C}^{op} \to Set$ is said to be a sheaf if: for every object X in $\mathcal{C}$ and every covering $\{U_i \to X\}_{i\in I}$ the following diagram:

$$F(X) \to \prod_{i\in I} F(U_i) \rightrightarrows \prod_{i,j\in I} F(U_i \times U_j)$$

where the two arrows between the products are induced by the different projections, is an equalizer.

A contravariant functor to the category of rings, groups or vector spaces is said to be a sheaf if the composition with the forgetful to Set is.

A pair $(\mathcal{C}, \mathcal{O})$, with $\mathcal{C}$ a site and $\mathcal{O}$ a sheaf of sets on it, is often called a ringed site; for instance, the sites of Example 3 are naturally ringed sites extending the sheaf of structure of the base scheme (for the étale site is not a trivial statement).

Definition 4. Let $\mathcal{C}$ be a site and let $\mathcal{X}, \mathcal{Y}$ be two sheaves of sets (or groups, rings, $\mathcal{O}$-modules) on it, then we define the presheaf $\mathcal{I}som(\mathcal{X}, \mathcal{Y})$ by the association:

$$\begin{aligned} \mathcal{I}som : \mathcal{C}^{op} &\to Set \\ X &\mapsto \mathrm{Isom}_{Sh(\mathcal{C}/X)}(\mathcal{X}_{|X}, \mathcal{Y}_{|X}) \end{aligned}$$

Notice that it is actually a sheaf.

Definition 5. Two sheaves $\mathcal{X}, \mathcal{Y}$ of sets (or groups, rings, $\mathcal{O}$-modules for a sheaf $\mathcal{O}$) over a site $\mathcal{C}$ are said to be locally isomorphic if for every object X in $\mathcal{C}$ there exists a covering $\{U_i \to X\}_{i\in I}$ such that $\forall i\ \mathcal{X}|_{U_i} \simeq \mathcal{Y}|_{U_i}$

Example 6. Let $(S, \mathcal{O})$ be a scheme and consider any of the sites of example 3, then locally free sheaves of rank n are locally isomorphic, indeed by definition they are defined as $\mathcal{O}$-modules locally isomorphic to $\mathcal{O}^n$.

Definition 7. Let $\mathcal{G}$ be a sheaf of groups and $\mathcal{X}$ a sheaf of sets on a site $\mathcal{C}$, we will be interested in the following notions:

action A left-action of $\mathcal{G}$ on $\mathcal{X}$ is a morphism of sheaves, say $\alpha : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$, such that for every object X in $\mathcal{C}$, $\alpha(X)$ defines an action of $\mathcal{G}(X)$ on $\mathcal{X}(X)$ in the usual sense.

freeness We say that $\mathcal{G}$ acts freely on $\mathcal{X}$ if for every object X in $\mathcal{C}$, the action of $\mathcal{G}(X)$ on $\mathcal{X}(X)$ is free.

transitivity We say that $\mathcal{G}$ acts transitively on $\mathcal{X}$ if for every object X in $\mathcal{C}$, $\forall x, y \in \mathcal{X}(X)$, there exists a covering $\{U_i \to X\}_{i\in I}$ and $\forall i \in I$ sections $g_i \in \mathcal{X}(U_i)$ such that $g_i \cdot x|_{U_i} = y|_{U_i}$.

We will denote by $\mathcal{G}$-sheaves the category whose data are given by: the objects are pairs $(\mathcal{X}, \alpha)$ with $\mathcal{X}$ a sheaf of sets and α as above; a morphism between two objects, which we will denote by $\mathcal{G}$-morphism, $(\mathcal{X}, \alpha)$ and $(\mathcal{Y}, \beta)$ is given by a morphism of sheaves $f : \mathcal{X} \to \mathcal{Y}$ compatible with the $\mathcal{G}$-action; in other words for every object X in $\mathcal{C}$ the diagram:

$$\begin{array}{ccc} \mathcal{G}(X) \times \mathcal{X}(X) & \xrightarrow{\alpha_X} & \mathcal{X}(X) \\ \downarrow{\scriptstyle id(X)\times f(X)} & & \downarrow{\scriptstyle f(X)} \\ \mathcal{G}(X) \times \mathcal{Y}(X) & \xrightarrow{\beta_X} & \mathcal{Y}(X) \end{array}$$

is commutative.

In the following, if there is no risk of confusion, we will talk about $\mathcal{G}$-sheaves $\mathcal{X}$ and $\mathcal{Y}$ instead of pairs $(\mathcal{X}, \alpha)$ and $(\mathcal{Y}, \beta)$.

Similarly, one can define sheaves of sets with a right-action by a sheaf of groups.

Definition 8. Let $\mathcal{G}$ be a sheaf of groups acting on a sheaf of sets $\mathcal{X}$ on a site $\mathcal{C}$ and let x be a global section of $\mathcal{X}$, the stabilizer $\mathcal{G}_x$ is defined to be the presheaf given, $\forall X$ object in $\mathcal{C}$, by $\mathcal{G}_x(X) = \mathcal{G}(X)|_{x|_X}$. It is actually a sheaf.

Even if all the sites which appear in this thesis have a final object, it can be that a site does not have one; if this is the case, the set of global sections of the sheaf $\mathcal{X}$ is defined to be the set $\mathrm{Hom}_{PSh}(e, \mathcal{X})$, where e is a final object in the category of presheaves on $\mathcal{C}$, see for example [4], TAG 01FT.

Remark 9. In case of transitive action, if the stabilizer $\mathcal{G}_x$ is commutative, then $\forall y \in \Gamma(\mathcal{C}, \mathcal{X})$, the stabilizer $\mathcal{G}_y$ is canonically isomorphic to $\mathcal{G}_x$. In order to see this, notice that, by transitivity of the action, for every object X in $\mathcal{C}$, there exist a covering $\{U_i \to X\}_{i\in I}$ and sections $g_i \in \mathcal{G}(U_i)$ such that $\forall i \in I$ $g_i x_{|U_i} = y_{|U_i}$; thus define $\forall i \in I$ a morphism of sheaves $(\mathcal{G}_x)_{|U_i} \to (\mathcal{G}_y)_{|U_i}$ for every $Y \to U_i$ by:

$$\begin{aligned} \mathcal{G}_y(Y) &\to \mathcal{G}_x(Y) \\ h &\mapsto g_i^{-1} h g_i \end{aligned}$$

One can check that these isomorphisms are compatible and glue to an isomorphism $\mathcal{G}_x \to \mathcal{G}_y$, that they are independent the choice of the g_i and of the covering.

We turn now our attention to a particular kind of sheaves with an action of sheaf of groups, they play an important role in cohomology.

Definition 10. Let $\mathcal{G}$ be a sheaf of groups on a site $\mathcal{C}$, the $\mathcal{G}$-sheaf $(\mathcal{X}, \alpha)$ is said to be a $\mathcal{G}$-torsor if for every object X in $\mathcal{C}$, there exists an open covering $\{U_i \to X\}_{i\in I}$ such that $\forall i$ the pair $(\mathcal{X}|_{U_i}, \alpha|_{U_i})$ is a trivial torsor, i.e. it is isomorphic, as $\mathcal{G}|_{U_i}$-sheaves over U_i, to the pair $(\mathcal{G}|_{U_i}, m|_{U_i})$ where m denotes the action given by the (left-)multiplication.

Equivalently, a $\mathcal{G}$-sheaf $\mathcal{X}$ on a site $\mathcal{C}$ is a $\mathcal{G}$-torsor if the action of $\mathcal{G}$ on $\mathcal{X}$ is free and transitive and for every object X in $\mathcal{C}$, there exists an open covering $\{U_i \to X\}_{i\in I}$ such that $\forall i$ $\mathcal{X}(U_i) \neq \emptyset$.

Remark 11.
- Since $\mathcal{I}som$ is a sheaf, notice that a $\mathcal{G}$-torsor $\mathcal{X}$ is trivial if and only if it has global sections.
- The category of $\mathcal{G}$-torsors is a groupoid: every morphism between $\mathcal{G}$-torsors is an isomorphism.

Example 12. If $\mathcal{X}$ and $\mathcal{Y}$ are locally isomorphic sheaves over a site $\mathcal{C}$, then the sheaf $\mathcal{I}som(\mathcal{X}, \mathcal{Y})$ is naturally a bi-torsor with the sheaves of groups $\mathrm{Aut}(\mathcal{X})$, $\mathrm{Aut}(\mathcal{Y})$ acting on the right and left respectively.

A particular instance, which we will be interested in, is when $\mathcal{C} = (Sch/S)_{Zar}$ is the big Zariski site and $\mathcal{X} := \mathcal{O}^n$; then every locally free sheaf of rank n $\mathcal{Y}$ is locally isomorphic to $\mathcal{X}$ and vice versa; moreover $\mathrm{Aut}(\mathcal{X}) = \mathrm{GL}_{n,S}$.

Definition 13. Given two sheaves of sets on a site $\mathcal{C}$, $\mathcal{X}$ with a right $\mathcal{G}$-action and $\mathcal{Y}$ with a left $\mathcal{G}-$action, we can consider the (left-)action of $\mathcal{G}$ on their product given for every object X by:

$$\begin{aligned}(\mathcal{G} \times \mathcal{X} \times \mathcal{Y})(X) &\to (\mathcal{X} \times \mathcal{Y})(X)\\ (g, x, y) &\mapsto (xg^{-1}, gy)\end{aligned}$$

We define the sheaf *contracted product* of $\mathcal{X}$ and $\mathcal{Y}$, denoted $\mathcal{X} \otimes_{\mathcal{G}} \mathcal{Y}$ (or in the literature $\mathcal{X} \wedge^{\mathcal{G}} \mathcal{Y}$), to be the sheafification of the presheaf defined as the quotient by the action of $\mathcal{G}$:

$$\begin{aligned}&\mathcal{C}^{op} \to Sets\\ &X \mapsto \mathcal{X}(X) \times \mathcal{Y}(X)/\sim\end{aligned}$$

i.e. for every X in $\mathcal{C}$ we consider the quotient of $\mathcal{X}(X) \times \mathcal{Y}(X)$ by the equivalence relation defined by $(xg, y) \sim (x, gy)$ $\forall g \in \mathcal{G}(X)$.

Remark 14.
- The contracted product is, in general, just a sheaf, it doesn't come with an action of $\mathcal{G}$.
- The contracted product is functorial, if we fix the sheaf $\mathcal{X}$, then $\mathcal{X} \otimes_{\mathcal{G}} \_$ defines a functor from sheaves with a $\mathcal{G}$-action to sheaves of sets.
- Nevertheless, if $f : \mathcal{H} \to \mathcal{G}$ is a morphism of sheaves of groups, then $\mathcal{G}$ is endowed with an $\mathcal{H}$-action and for every $\mathcal{H}$-sheaf $\mathcal{X}$, the contracted product $\mathcal{X} \otimes_{\mathcal{H}} \mathcal{G}$ has a natural structure of $\mathcal{G}$-set (induced by the multiplication of $\mathcal{G}$ on itself). Moreover, the contracted product defines a functor between the categories of torsors:

$$\begin{aligned}f_* : \{\mathcal{H}\text{-torsors}\} &\to \{\mathcal{G}\text{-torsors}\}\\ \mathcal{T} &\mapsto \mathcal{T} \otimes_{\mathcal{H}} \mathcal{G}.\end{aligned}$$

- The contracted product $\mathcal{X} \otimes_{\mathcal{G}} \mathcal{Y}$ can be characterized by meaning of a universal property; namely, for every sheaf of sets $\mathcal{Z}$ and $\forall f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ morphism of sheaves, such that for every object X in $\mathcal{C}$, $\forall g \in \mathcal{G}(X)$ $f(X)(xg, y) = f(X)(x, gy)$ there exists a unique morphism $\varphi : \mathcal{X} \otimes_{\mathcal{G}} \mathcal{Y} \to \mathcal{Z}$ such that $\varphi \circ p = f$, where $p : \mathcal{X} \times \mathcal{Y} \to \mathcal{X} \otimes_{\mathcal{G}} \mathcal{Y}$ is the quotient map.

Proposition 15. *Let $\mathcal{C}$ be a site and let $\mathcal{X}$ be a sheaf of sets; consider the sheaf of groups $Aut(\mathcal{X}) := \mathcal{I}som(\mathcal{X}, \mathcal{X})$, then the functor:*

$$\begin{aligned} Aut(\mathcal{X})\text{-torsors} &\to \text{ sheaves locally isomorphic to } \mathcal{X} \\ \mathcal{T} &\mapsto \mathcal{T} \otimes_{Aut(\mathcal{X})} \mathcal{X} \end{aligned}$$

defines an equivalence of categories with a quasi-inverse defined, for every sheaf $\mathcal{E}$ locally isomorphic to $\mathcal{X}$, by:

$$\mathcal{E} \mapsto \mathcal{I}som(\mathcal{X}, \mathcal{E}).$$

Proof. Let $\mathcal{E}$ be locally isomorphic to $\mathcal{X}$, then the morphism defined, for every object X in $\mathcal{C}$, by:

$$\begin{aligned} (\mathcal{I}som(\mathcal{X}, \mathcal{E}) \times \mathcal{X})(X) &\to \mathcal{E}(X) \\ (\varphi, a) &\mapsto \varphi(a) \end{aligned}$$

factorizes through the contracted product and gives an isomorphism.
On the other hand, let $\mathcal{T}$ be an $Aut(\mathcal{X})$-torsor, for every object X in $\mathcal{C}$ and every $a \in \mathcal{T}(X)$, let $\varphi_a : \mathcal{X}_{|X} \to \mathcal{T}_{|X} \otimes \mathcal{X}_{|X}$ be the morphism induced by:

$$\begin{aligned} \mathcal{T}_{|X} &\to \mathcal{T}_{|X} \times \mathcal{X}_{|X} \\ x &\mapsto (a, x) \end{aligned}$$

then

$$\begin{aligned} \mathcal{T}(X) &\to \mathcal{I}som(\mathcal{X}, \mathcal{T} \otimes \mathcal{X})(X) \\ a &\mapsto \varphi_a \end{aligned}$$

defines a morphism of $\mathcal{G}$-torsors, hence an isomorphism. □

The sheaf $\mathcal{T} \otimes_{Aut(\mathcal{X})} \mathcal{X}$ is generally called the twist of $\mathcal{X}$ by $\mathcal{T}$.

Clearly, the proposition holds not only for sheaves of sets, but also for sheaves of rings, groups or $\mathcal{O}$-modules for a sheaf of rings $\mathcal{O}$; for instance, we have the following:

Example 16. Consider the case where $\mathcal{C}$ is the big-Zariski site of schemes over a base scheme $(S, \mathcal{O})$; denote by $\mathcal{X} := \mathcal{O}^n$ so $\mathrm{Aut}(\mathcal{X})$=$\mathrm{GL}_{n,S}$ then, according to the proposition, the functor:

$$\begin{aligned} GL_{n,X}\text{-torsors} &\to \text{locally free } \mathcal{O}_X\text{-modules of rank } n \\ \mathcal{T} &\mapsto \mathcal{T} \otimes_{GL_{n,X}} \mathcal{O}_X^n \end{aligned}$$

defines an equivalence of categories with quasi-inverse given by:

$$\mathcal{E} \mapsto \mathcal{I}som(\mathcal{O}_X^n, \mathcal{E})$$

(where the associations on the arrows are understood.)

Definition 17. Let $\mathcal{C}$ be a site and $\mathcal{G}$ a sheaf of groups on it, the first cohomology set $H^1(\mathcal{C}, \mathcal{G})$ is defined to be the set of $\mathcal{G}$-torsors modulo isomorphism.

Remark 18. 1. In case $\mathcal{G}$ =Aut($\mathcal{X}$) for $\mathcal{X}$ a sheaf of sets on a site $\mathcal{C}$, then, thanks to proposition 15, the first cohomology set can be equivalently defined to be the set of isomorphism classes of twists of $\mathcal{X}$.

2. Notice that in general the first cohomology set is just a pointed set: the basepoint is given by the isomorphism class of the trivial torsor, but in case $\mathcal{G}$ is commutative we have the following:

Proposition 19. *Let $\mathcal{G}$ be a sheaf of groups on a site $\mathcal{C}$. Assume that $\mathcal{G}$ is a sheaf of commutative groups, then the first cohomology set, as defined in Definition 17 has a natural structure of group (given by the contracted product) and it is isomorphic to the usual first cohomology group (defined to be the right derived functor of taking global section)*

Example 20. Applying the considerations of the latter proposition and remark to $\mathcal{G} = \mathbb{G}_{m,S}$ for the small Zariski site S_{Zar}, we get the well-known fact that $H^1(S_{Zar}, \mathbb{G}_m)$ =$\{$locally invertible sheaves$\}/\sim$.

One last observation and we will be ready to state the theorem we need:

Definition 21. Let $\mathcal{G}$ be a sheaf of groups on a site $\mathcal{C}$ acting transitively on a sheaf of sets $\mathcal{X}$, let $x, y \in \Gamma(\mathcal{C}, \mathcal{X})$; then, the *transporter* ${}_y\mathcal{G}_x$ from x to y is defined to be the presheaf given by, for every object X in $\mathcal{C}$, ${}_y\mathcal{G}_x(X) = \{g \in \mathcal{G}(X)$ such that $y|_X = g \cdot x|_X\}$. It is actually a sheaf, a subsheaf of $\mathcal{G}$.

Remark 22. The transporter ${}_y\mathcal{G}_x$ is canonically a right $\mathcal{G}_x$-torsor and a left $\mathcal{G}_y$ torsor; thus, thanks to remark 9, if $\mathcal{G}_x$ is commutative, ${}_y\mathcal{G}_x$ is canonically a left and right $\mathcal{G}_y$-torsor for every $y \in \Gamma(\mathcal{C}, \mathcal{X})$.

Theorem 23. *Let $\mathcal{C}$ be a site, $\mathcal{X}$ a sheaf of sets with an action of a sheaf of groups $\mathcal{G}$. Assume that $\mathcal{G}$ acts on $\mathcal{X}$ transitively. Fix a global section $x \in \Gamma(\mathcal{C}, \mathcal{X})$ and define the sheaf of groups $\mathcal{H}$ to be the stabilizer $\mathcal{H} := \mathcal{G}_x$. Then there is an exact sequence:*

$$\Gamma(\mathcal{C}, \mathcal{H}) \xhookrightarrow{\iota} \Gamma(\mathcal{C}, \mathcal{G}) \xrightarrow{\alpha} \Gamma(\mathcal{C}, \mathcal{X}) \xrightarrow{\rho} H^1(\mathcal{C}, \mathcal{H}) \xrightarrow{i^*} H^1(\mathcal{C}, \mathcal{G})$$

where:

- *the morphism ι is the inclusion of the stabilizer $\mathcal{H}$*
- *the map α is given by the action of $\Gamma(\mathcal{C}, \mathcal{G})$ on x, i.e. $\gamma(g) := g \cdot x$*
- *the map ρ is given $\forall y \in \Gamma(\mathcal{C}, \mathcal{X})$ by $\rho(y) := [{}_y\mathcal{G}_x]$, where $[{}_y\mathcal{G}_x]$ is the isomorphism class of the transporter.*
- *the map ι^* is induced by the contracted product as observed in the remark 14*

The sequence is exact in the sense that the image of ι is the fibre of x under α, the image of α is the fibre of the basepoint $[\mathcal{H}]$ under ρ and in turn the image of ρ is the fibre of $[\mathcal{G}]$ under ι_*. Moreover, for $a, b \in \Gamma(\mathcal{C}, \mathcal{X})$, $\rho(a) = \rho(b)$ if and only if $\exists\ g \in \Gamma(\mathcal{C}, \mathcal{G})$ such that $ga = b$.

Proof. This follows from [3], Chapitre III, Proposition 3.2.2 and Corollaire 3.2.3. □

3 The affine case

We check now that we can apply Theorem 23 to the case we are dealing with.

Let $\mathcal{X}_f$ denote the sheaf of sets represented by X_f over the big Zariski site $(Sch_{|\mathrm{Spec}(R)})_{Zar}$, we want to show that $\mathcal{G}$ acts transitively on X_f and that $\mathcal{X}_f$ has a global section on the small Zariski site $\mathrm{Spec}(R)_{Zar}$.

We begin with the transitivity of the action of $\mathcal{G}$ on $\mathcal{X}_f$ restricted to the small Zariski site $\mathrm{Spec}(R)_{Zar}$. In order to show the transitivity of the action we will make use of symmetries, for this recall that:

Definition 24. Let M be a free module of rank n over a domain R endowed with a symmetric bilinear form $b : M \times M \to R$; let $v \in M$ be such that $b(v, v) \in R^*$, then the symmetry with respect the hyperplane perpendicular to v is given by:

$$\begin{aligned} s_v : M &\to M \\ x &\mapsto x - 2\frac{b(x,v)}{b(v,v)}v. \end{aligned}$$

It is known that any symmetry is an isometry in the sense that, in the notation of the definition, $\forall x \in M\ b(x, x) = b(s_v(x), s_v(x))$, but it doesn't lie in $SO(b)$; indeed, it doesn't preserve the orientation.

Theorem 25. *Let $\mathcal{X}_f$ and $\mathcal{G}$ be the sheaves defined above, then the action of $\mathcal{G}$ on $\mathcal{X}_f$ is transitive on the small-Zariski site $Spec(R)_{Zar}$.*

Proof. For the Zariski topology it is enough to show the transitivity stalk by stalk; therefore we are left to prove that, if $\mathfrak{m} \subset R$ is a maximal ideal, $\forall\ P, Q \in R^3_{\mathfrak{m}}$ such that $b(P, P) = b(Q, Q) = f$ with P and Q primitive, there exists $g \in \mathcal{G}(R_{\mathfrak{m}})$ such that $g \cdot P = Q$.
Our strategy is to find $v, w \in R^3_{\mathfrak{m}}$ such that $g := s_v \circ s_w$ makes the claim true. If $y \in R^3_{\mathfrak{m}}$, the condition for s_y to be defined is:

$$\overline{b(y, y)} \neq 0 \text{ in the residue field } k(m)$$

Notice that, for a given v, the w we are looking for, is already determined, it is of the form $\lambda(s_v(P) - Q)$ for a $\lambda \in \mathrm{Frac}(R)$; thus we reduced ourselves to exhibit the existence of $v \in R^3_{\mathfrak{m}}$ such that $b(v, v)$ and $b(s_v(P) - Q, s_v(P) - Q)$ are not trivial in the residue field $k(\mathfrak{m})$. The latter is equivalent to:

$$\frac{b(P,v)b(v,Q)}{b(v,v)} \neq \frac{b(P,Q) - f}{2}$$

the left hand side, interpreted as a function in the variable v is homogeneous and therefore defines a map $h : \mathbb{P}^2_k(k) \setminus C(k) \to k$, where by $\mathbb{P}^2(k)$ we denote the subset of closed points of $\mathbb{P}^2_k$ endowed with the subspace topology and by $C := Z(b)$ we mean the conic defined by the zeroes of the quadratic form associated to b. In order to conclude it is enough to show that h is not the constant zero function; for this, notice that if $x \in \mathbb{P}^2(k)$:

$$h(x) = 0 \Leftrightarrow x \in P^\perp \cup Q^\perp$$

where $P^\perp$ is the line $Z(xP_x + yP_y + zP_z) \cap \mathbb{P}^2(k)$ if $P = (P_x, P_y, P_z)$ and it is actually a line since P is assumed to be primitive. Since C is non singular and $\mathbb{P}^2(k)$ is irreducible (k is assumed algebraically closed) it follows that $P^\perp \cup Q^\perp \subsetneq C \cup P^\perp \cup Q^\perp \subsetneq \mathbb{P}^2(k)$ i.e. there are at least two points $x, y \in \mathbb{P}^2(k)$ where h is defined and $h(x) = 0 \neq h(y)$. □

A point in $X_f(R)$ is given by $(f, 1, 0)$, from now on we denote it by $P := (f, 1, 0)$, moreover we define $\mathcal{H}$ to be its stabilizer, i.e. $\mathcal{H} := \mathcal{G}_P$. We have shown that the hypotheses of Theorem 23 are fulfilled for the action of $\mathcal{G}$ on$\mathcal{X}_f$, hence we have the following exact sequence:

$$\mathcal{H}(R) \hookrightarrow \mathcal{G}(R) \longrightarrow X_f(R) \longrightarrow H^1(\mathrm{Spec}(R)_{Zar}, \mathcal{H}) \longrightarrow H^1(\mathrm{Spec}(R)_{Zar}, \mathcal{G})$$

In the following we will study the objects appearing in this sequence, the first result is that $H^1(Spec(R)_{Zar}, \mathcal{G})$ is trivial.

Lemma 26. *Let k be an algebraically closed field and let $q : k^3 \to k$ be a non-degenerate quadratic form, then the group schemes $PGL_{2,k}$ and $SO(q)$ are isomorphic.*

Proof. Let C denote the conic $Z(q) \subseteq \mathbb{P}^2_k$, then, since k is algebraically closed, it has at least a point and therefore it is isomorphic to $\mathbb{P}^1_k$. The group $SO(q)$ acts on $\mathbb{P}^2_k$ in a natural way fixing the quadric C, this defines an action of $SO(q)$ on $\mathbb{P}^1_k$; in other words, there is a morphism of group schemes $\rho : SO(q) \to PGL_{2,k}$. I claim that this is an isomorphism. In order to see the injectivity, consider an $m \in SO(q)$ such that $\rho(m)$ is trivial in $PGL_{2,k}$, i.e. $\forall Q \in C,\ m \cdot Q = Q$, I want to show that m acts as the identity on the whole $\mathbb{P}^2_k$; for this, let $P \in \mathbb{P}^2_k$ be any point, write $\{P\} = l \cap r$ for two different lines. Thanks to Bezout's theorem, the intersection between any line and C consist of two points counted with multiplicity; without loss of generality we might assume that both l and r cut C in two distinct points, say $l \cap C = \{L_1, L_2\}$, then $m(l)$ is completely determined by $m(L_1)$ and $m(L_2)$, so $m(l) = l$ and the same holds for r. We conclude that $\forall P \in \mathbb{P}^2_k, m(P) = m(l \cap r) = l \cap r = P$. Thus ρ is injective.

In order to complete the proof we exhibit the inverse morphism; since we are assuming that k is algebraically closed all the quadratic forms are classified by the rank, so to make the inverse morphism explicit, without loss of generality we may assume that $q(a, b, c) = ab - c^2$.

Consider the morphism $\mathrm{Spec}(\varphi) : \mathbb{P}^1_k \to \mathbb{P}^1_k$, which for every $(x : y) \in \mathbb{P}^1_k(A)$ is given by $(x : y) \mapsto (px + qy : rx + sy)$ for $p, q, r, s \in k$, i.e. it is induced by the morphism of rings $\varphi : k[x, y] \to k[x, y]$ represented on the first degree by the matrix: $\left(\begin{smallmatrix} p & r \\ q & s \end{smallmatrix}\right)$ with respect to the basis $\{x, y\}$. The morphism φ induces an automorphism of the k-module $k[x, y]_2$ and it is easy to compute that it is represented by the matrix:

$$\Phi := \begin{pmatrix} p^2 & pr & r^2 \\ 2pq & ps + qr & 2rs \\ q^2 & qs & s^2 \end{pmatrix}$$

with respect to the basis $\{x^2, xy, y^2\}$.

Consider now the Segre embedding $\mathrm{Spec}(s) : \mathbb{P}^1_k \to \mathbb{P}^2_k$ defined on the A-points for every k-algebra A by $(x : y) \mapsto (x^2 : xy : y^2)$; in other words it is induced by $s : k[a, b, c] \to k[x, y],\ a \mapsto x^2,\ b \mapsto xy,\ c \mapsto y^2$. The morphism s induces an isomorphism of k-modules: $k[a, b, c]_1 \to k[x, y]_2$ which sends the

basis $\{a, b, c\}$ onto the basis $\{x^2, xy, y^2\}$, therefore $s^{-1}\varphi s$ extends uniquely to an automorphism of $k[a, b, c]$; this defines a morphism Ψ :$\mathrm{PGL}_{2,k} \to \mathrm{PGL}_{3,k}$, by $\mathrm{Spec}(\varphi) \mapsto \mathrm{Spec}(s^{-1}\varphi s)$ which actually factorizes through $\mathrm{SO}(q) \hookrightarrow \mathrm{PGL}_{3,k}$. In order to conclude, notice that any automorphism of $\mathbb{P}^1_k$ is determined by the image of the three k-points $(1:0), (1:1), (0:1)$; moreover we have that $\mathrm{Spec}(s^{-1}\varphi s)$ is represented by the matrix Φ^t and so the points $(1:0:0), (0:0:1), (1:1:1)$ map to $(p^2 : pr : r^2), (q^2 : qs : s^2), ((p+q)^2 : (p+q)(r+s) : (r+s)^2)$, but the former are the images of $(1:0), (1:1), (0:1)$ and the latter of $\varphi^{-1}(1:0), \varphi^{-1}(1:1), \varphi^{-1}(0:1)$ under the Segre embedding.

This show that the composite $\rho\Psi$ is the identity and concludes the proof. □

Proposition 27. *Let R and $\mathcal{G}$ be as above, then the first cohomology set $H^1(\mathrm{Spec}(R)_{Zar}, \mathcal{G})$ is trivial.*

Proof. Since $\mathcal{G}$ is represented by the group scheme $\mathrm{SO}(q)$ which is isomorphic to $\mathrm{PGL}_{2,k}$ we are left to show that the first cohomology group of the latter is zero.
For this, notice that $\mathrm{PGL}_{2,k}$ fits into a short sequence of sheaves of (nonabelian) groups exact for the Zariski topology over $\mathrm{Spec}(R)$:

$$0 \to \mathbb{G}_m \to \mathrm{GL}_2 \to \mathrm{PGL}_2 \to 0.$$

Looking at the long exact sequence we have:

$$H^1(\mathrm{Spec}(R), \mathrm{GL}_2) \to H^1(\mathrm{Spec}(R), \mathrm{PGL}_2) \to H^2(\mathrm{Spec}(R), \mathbb{G}_m).$$

Now notice that $H^1(\mathrm{Spec}(R),\mathrm{GL}_{2,k})$ is trivial, indeed it is in bijection with the isomorphism classes of $\mathrm{GL}_{2,k}$-torsors; or equivalently, thanks to Proposition 15,with the isomorphism classes of twists of $\mathcal{O}^2$. Since we are considering the affine scheme $\mathrm{Spec}(R)$, the latter are given by projective modules which locally are free of rank 2. But R is a PID, thus finitely generated projective R-modules are free, hence the isomorphism classes of $\mathcal{O}^2$-torsors consist only of the trivial ones.

The group $H^2(\mathrm{Spec(R)},\mathbb{G}_{m,k})$ is trivial too by the vanishing theorem of Grothendieck ([1], Chapter III, Theorem 2.7).

This proves the thesis. □

Notice that one could prove the transitivity of the action of $\mathcal{G}$ on X_f for the étale topology, which is implied by the transitivity on the Zariski one, showing that the map $\mathcal{G} \times X_f \to X_f \times X_f,\ (g, x) \mapsto (gx, x)$ is surjective; nevertheless, showing that $H^1(\mathrm{Spec}(R)_{\acute{e}t}, \mathcal{G})$ is trivial would require a study of the Brauer group of R.

In any case, since we have proven the transitivity of the action and the triviality of the first cohomology group of $\mathcal{G}$ on the small Zariski site over $\mathrm{Spec}(R)$, from the sequence of Theorem 23 we deduce the bijection:

$$\mathcal{G}(R) \setminus \mathcal{X}_f(R) \to H^1(\mathrm{Spec}(R)_{Zar}, \mathcal{H})$$

In the next section we turn our attention to the study of the stabilizer $\mathcal{H}$; our main strategy is to study its relation with the orthogonal complement of a fixed section lying in $\Gamma(\mathrm{Spec}(R)_{Zar}, \mathcal{X}_f)$.

3.1 The stabilizer $\mathcal{H}$

In this section we deal with the study of the stabilizer sheaf of groups $\mathcal{H}$, but first, we take a look to the orthogonal complement $P^\perp$. The existence of the primitive solution $P = (f, 1, 0))$ guarantees that there is an exact sequence of R-modules:

$$0 \to P^\perp \to R^3 \xrightarrow{\tilde{b}} R \to 0 \tag{1}$$

where for every $Q \in R^3$, $\tilde{b}(Q) := b(Q, P)$ and we denote by $P^\perp$ its kernel. The fact that P is primitive implies that $\tilde{b}$ is surjective and, since R is free, we conclude that the sequence splits. In general deducing something on $P^\perp$ could be tough, but assuming to work with the quadratic form $q(x, y, z) = xy + z^2$, we have the advantage of knowing a point in $X_f(R)$; even more, for every R-algebra A, the point $P_A := (f, 1, 0) \in A^3$ lies in $X_f(A)$. In addition to this, we can even exhibit an explicit base for $P^\perp$: one is given by the vectors $e_1 := (0, 0, 1)$ and $e_2 := (f, -1, 0)$; the Gram matrix of the bilinear form restricted to the orthogonal complement, $b|_{P^\perp}$, with respect to this basis is given by:

$$GM = \begin{pmatrix} 1 & 0 \\ 0 & -f \end{pmatrix}$$

therefore we deduce that $\mathrm{disc}(b_{|P^\perp}) = -f$.

We can finally focus on the study of $\mathcal{H} := \mathcal{G}_P$, the stabilizer of the point P. The leading strategy is to let it act on the orthogonal complement and study the induced map from $\mathcal{H}$ to the automorphism group or to the endomorphism ring of $P^\perp$.

First of all, notice that $\mathcal{H}$ acts on $(P^\perp, b_{|P^\perp}, d)$ in the sense that it respects both the restriction of the bilinear form to $P^\perp$ and the restriction of the canonical orientation, therefore there is a morphism of sheaves $\mathcal{H} \to \mathcal{T}_1$ where we denote with $\mathcal{T}_1$ the sheaf $SO(b_{|P^\perp})$ of the automorphism group of $(P^\perp, b_{|P^\perp}, d)$. Actually, the latter can be computed:

Proposition 28. *For every R-algebra A we have that*

$$\mathcal{T}_1(A) = \left\{ \begin{pmatrix} a & cf \\ c & a \end{pmatrix} \middle| \, a, c \in A \text{ and } a^2 - c^2 f = 1 \right\}$$

in other words the sheaf $\mathcal{T}_1$ is represented by the spectrum of the R-algebra $\frac{R[x,y]}{(x^2 - y^2 f - 1)}$ over the big Zariski site $(Sch_{/R})_{Zar}$.

Proof. By definition we have:

$$SO(b_{|P^\perp})(A) = \{m \in GL_2(A) \text{ such that } m^t GM m = GM \text{ and } \det(m) = 1\}$$

Let

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

then direct computations show that m is in $\mathrm{SO}_2(b_{|P^\perp})(A)$ if and only if the following conditions hold:

$$\begin{cases} a^2 - c^2 f = 1 \\ ab - cdf = 0 \\ b^2 - d^2 f = -f \\ ad - bc = 1. \end{cases}$$

From the last equation we deduce that $\mathrm{Spec}(A) = D(a) \cup D(b)$; on the open $D(a)$ we have that $b = cdf/a$ and substituting in the condition given by the determinant we get:

$$1 = ad - bc = ad - c^2 df/a = 1/a(a^2 - c^2 f)d = d/a$$

i.e. we get $d = a$ and $b = cf$. The same can be shown analogously on $D(b)$ proving the thesis. □

If we consider the sequence 1 restricted to $D(f) \subseteq \mathrm{Spec}(R)$, i.e. tensoring by $R[1/f]$, it is still exact and a section is given by $s : R[1/f] \to R[1/f]^3$, $1 \mapsto (1, 1/f, 0)$; therefore we have the split $R[1/f]^3 \simeq P^\perp \oplus R[1/f](1, 1/f, 0)$ and for every open $U \subseteq \mathrm{Spec}(R[1/f])$, the elements in $\mathcal{H}(U)$ are of the form:

$$m = \begin{pmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

with respect to the basis $\{e_1, e_2, (1, 1/f, 0)\}$. In particular, the association:

$$m \mapsto \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

defines an isomorphism $\mathcal{H} \xrightarrow{\sim} \mathcal{T}_1$ on $\mathrm{Spec}(R[1/f])$. On all the other points the morphism $\mathcal{H} \to \mathcal{T}_1$ is nevertheless injective: every stalk embeds in the stalk at the generic point, where the morphism is injective.

In particular we get that the stabilizer of P is commutative, therefore, thanks to Remark 9, the stabilizer of any point is canonically isomorphic to $\mathcal{H}$ and the set $H^1(\mathrm{Spec}(R), \mathcal{H})$ has actually a natural group structure.

We take now a closer look at the sheaf $\mathcal{T}_1$: it is clearly a subgroup of the multiplicative group of the endomorphism ring of $P^\perp$, but we gain a commutative ring if we restrict our attention to the endomorphisms which commute with the automorphisms lying in $\mathcal{T}_1$; formally, we have the following:

Proposition 29. *Let $\mathcal{T}_1$ denote, as above, the sheaf of groups given by the automorphisms of $(P^\perp, b_|, d)$, moreover let $End_{\mathcal{T}_1}(P^\perp) \subseteq End(P^\perp)$ denote the endomorphisms of $P^\perp$, which restricted to every open $U \subseteq Spec(R)$, commute with the automorphisms in $\mathcal{T}_1(U)$, then*

$$End_{\mathcal{T}_1}(P^\perp) \simeq \frac{R[v]}{(v^2 - f)}.$$

Proof. Recall that $P^\perp$ is a free R-module of rank 2, in particular $\mathrm{End}(P^\perp) \simeq \mathrm{Mat}(R,2)$. Notice that the ring $\frac{R[v]}{(v^2-f)}$ has a natural structure of free R-module of rank 2, it is isomorphic to the direct sum $R \oplus Rv$. Let $c+dv \in \frac{R[v]}{(v^2-f)}$ be any element with $c, d \in R$, then the multiplication by it can be seen as an endomorphism of the underlying module; in other words this defines, with the appropriate choice for an R-base of $\frac{R[v]}{(v^2-f)}$, the morphism of rings:

$$\begin{aligned} \psi : \frac{R[v]}{(v^2-f)} &\to \mathrm{End}(P^\perp) \\ c+dv &\mapsto \begin{pmatrix} c & df \\ d & c \end{pmatrix}. \end{aligned}$$

On the other hand, for every R-algebra A, the action of $\mathcal{T}_1(A)$ can be expressed via the embedding:

$$\begin{aligned} \varphi : \mathcal{T}_1(A) = \{a, b \in A |\ a^2 - b^2 f = 1\} &\to \mathrm{End}(P_A^\perp) \\ (a,b) &\mapsto a \cdot \mathrm{Id} + b \cdot \begin{pmatrix} 0 & f \\ 1 & 0 \end{pmatrix}. \end{aligned}$$

Clearly we have that $\mathrm{Im}(\varphi) \subseteq \mathrm{Im}(\psi) \subseteq \mathrm{End}_{\mathcal{T}_1}(P^\perp)$, so we are only left to show that $\mathrm{End}_{\mathcal{T}_1}(P^\perp) \subseteq \mathrm{Im}(\psi)$, but this follows from a straightforward computation. □

Denote by B the ring $B := \frac{R[v]}{(v^2-f)}$ and $U := \mathrm{Spec}(B)$ (we will reserve C to denote the completed curve), then the inclusion $R \hookrightarrow B$ represents the projection $\pi : U \to \mathbb{A}^1_k$. It defines a 2:1 covering of the affine line outside the branch points $B_f := \{(x-\alpha) \in \mathrm{Spec}(R) \text{ such that } f(\alpha) = 0\}$:

$$\pi_{|(U \setminus \pi^{-1}(B_f))} : U \setminus \pi^{-1}(B_f) \to \mathbb{A}^1_k \setminus B_f.$$

The curve U comes with a natural automorphism of order 2, say σ, namely the one associated to the ring morphism: $B \to B,\ a+bv \mapsto a-bv$.

We consider again the sheaf $\mathcal{T}_1$: we can say something more about it. Clearly we have that $\mathcal{T}_1(R) \hookrightarrow B^*$, but moreover for every R-algebra A we have that $T_1(A)$ injects naturally in $(B \otimes A)^*$; in other words, there is a morphism of sheaves $\mathcal{T}_1 \hookrightarrow \mathcal{T}$, where we denote by $\mathcal{T}$ the sheaf $\pi_*(\mathbb{G}_{m,U})$, also known as the Weil restriction of the multiplicative group with respect to π.

The involution σ induces an involution on the Weil restriction, given for every R-algebra A by:

$$\begin{aligned} \sigma_A^* : \mathcal{T}(A) &\to \mathcal{T}(A) \\ a+bv &\mapsto a-bv \end{aligned}$$

and we also consider the two endomorphisms of $\mathcal{T}$ $id \cdot \sigma^*$ and id/σ^*, defined on every algebra A by:

$$(id \cdot \sigma^*)_A(a+bv) = (a+bv)(a-bv) = a^2 - b^2 f \tag{2}$$

$$(id/\sigma^*)_A(a+bv) = \frac{a+bv}{a-bv} = \frac{a^2 + b^2 f + v(2ab)}{a^2 - b^2 f}. \tag{3}$$

It is clear, by proposition 29, that $\mathcal{T}_1$ is a kernel for the morphism $id \cdot \sigma^*$. Moreover, from the inclusion $\mathcal{T} \hookrightarrow \mathrm{Mat}(2, A)$ described above, it is easy to deduce that the element $a + bv \in A \otimes B$, with $a, b \in A$, is invertible if and only if $a^2 - b^2 f \in A^*$, i.e. the map $id \cdot \sigma^*$ factorizes through $\mathbb{G}_m$.

In addition to this, notice that, if G is a commutative group and σ an automorphism of order 2, we can always consider the endomorphisms $id \cdot \sigma$ and id/σ and their composition is trivial, indeed $\forall g \in G$ it holds the following:

$$(id \cdot \sigma)((id/\sigma)(g)) = (id \cdot \sigma)(g\sigma(g)^{-1}) = g\sigma(g)^{-1}\sigma(g)\sigma(\sigma(g^{-1})) = 1.$$

Applying this consideration to our case we conclude that the morphism id/σ^* factorizes through $\mathcal{T}_1$. The determination of its kernel is immediate: for every R-algebra A, an element $a + bv \in \mathcal{T}(A)$ with $a, b \in A$, lies in the kernel if and only if $a + bv = \sigma^*(a + bv) = a - bv$, and since 2 is invertible we conclude that $b = 0$; therefore we get that $\ker(id/\sigma^*)_A = A^*$, thus $\ker(id/\sigma^*) = \mathbb{G}_m$.

To complete the study of the stabilizer sheaf $\mathcal{H}$, we will show that it is isomorphic to the quotient sheaf $\mathcal{T}/\mathbb{G}_m$; for this, we are going to show that they represent a kernel of the same sheaf morphism; actually we have already shown that they inject in $\mathcal{T}_1$, so we are left to exhibit that they have isomorphic cokernels.

Let's begin with the cokernel of the injection $i : \mathcal{H} \hookrightarrow \mathcal{T}_1$, we have already seen that over $\mathrm{Spec}(R[1/f])$ it is an isomorphism, the following lemma allows us to conclude:

Lemma 30. *Let $\alpha \in k$ such that $f(\alpha) = 0$ and consider the maximal ideal $(t-\alpha) \in Spec(R)$, then the image of the injective morphism i, at the stalk $\mathcal{H}_{(t-\alpha)}$ is given by:*

$$i(\mathcal{H}(R_{(t-\alpha)})) = \{m \in \mathcal{T}_1(R_{(t-\alpha)}) | \overline{m} P_{k((t-\alpha))} = P_{k((t-\alpha))}\}$$

where $\overline{m}$ and $P_{k((t-\alpha))}$ are the projections to the residue fields $k((t-\alpha))$.

Proof. Since k is algebraically closed, it is clear that $k((t-\alpha)) \simeq k$, nevertheless we keep using the notation $k((t-\alpha))$ to stress the fact that we are considering just the points corresponding to roots of f.

First of all, notice that $P_{k(t-\alpha)} \in P^{\perp}_{k(t-\alpha)}$ since $b(P, P) = f$ which is trivial at the residue field (or even by direct computation as $P_{(t-\alpha)} = (0, 1, 0)$). By definition of $\mathcal{H}$ an inclusion holds, indeed every element in $\mathcal{H}(k(t-\alpha))$ fixes the point $P_{k(t-\alpha)}$. Thus, we are only left to show that every $m \in \mathcal{T}_1(R_{(t-\alpha)})$ such that $\overline{m} P_{k((t-\alpha))} = P_{k((t-\alpha))}$ actually lies in $i(\mathcal{H}(R_{k((t-\alpha))}))$. Consider $Q := (0, 0, 1) \in P^{\perp}$ then $b(Q, Q) = 1 \in k((t-\alpha))$ hence the symmetry s_Q is well defined on $P^{\perp}_{k(t-\alpha)}$; the composite $s_Q m$ is in the orthogonal group $O_2(b)$, but it doesn't respect the orientation, hence it is a symmetry, say s_T for a point T, which is a base for the eigenspace of $s_Q m$ relative to the eigenvalue -1. Therefore we conclude that $s_Q m = s_T$ and that $m = s_Q s_T$ is in $i(\mathcal{H}(R_{(t-\alpha)}))$. □

We have already seen an explicit description of $\mathcal{T}_1(A)$ for an R-algebra A, if we consider $A = k(\mathfrak{m})$ the residue field at a point $\mathfrak{m} \in \mathrm{Spec}(R) \setminus D(f)$, i.e. at a point where f vanishes, we have, with respect to a basis $\{e_1, e_2\}$ with

$e_1 = P_{k(\mathfrak{m})}$, that:

$$\mathcal{T}_1(k(\mathfrak{m})) = \left\{ m = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \text{ such that } a, b \in k(\mathfrak{m}) \text{ and } a^2 = 1 \right\}$$

in particular at every stalk the index of $\mathcal{H}(R_{k(\mathfrak{m})})$ in $\mathcal{T}_1(R_{k(\mathfrak{m})})$ is 2, i.e. the stalk of the cokernel is isomorphic to $\mathbb{F}_2$; from the previous lemma it is clear that an element $m \in \mathcal{T}_1(R_{k(\mathfrak{m})})$, with the above notation is in the image of $i_{k(\mathfrak{m})}$ if and only if $a = 1$.

We are now ready to determine the cokernel of $\mathcal{H} \hookrightarrow \mathcal{T}_1$: for every $\mathfrak{m} \in \mathrm{Spec}(R) \setminus D(f)$ we consider the morphism of sheaves of groups $q_{\mathfrak{m}} : \mathcal{T}_1 \to i_{\mathrm{Spec}(k(\mathfrak{m})),*}\mathbb{F}_2$ such that:

$$\forall U \ni \mathfrak{m} \text{ open in } \mathrm{Spec}(R),\ q_{\mathfrak{m}}(U): \quad \mathcal{T}_1(U) \to i_{\mathrm{Spec}(k\mathfrak{m}),*}\mathbb{F}_2(U)$$
$$m \mapsto \begin{cases} 0 \text{ if } m_{k(\mathfrak{m})} P_{k(\mathfrak{m})} = P_{k(\mathfrak{m})} \\ 1 \text{ otherwise} \end{cases} .$$

Finally we conclude that the cokernel is given by:

$$q : \mathcal{T}_1 \xrightarrow{\sqcap q_{\mathfrak{m}}} \prod_{\substack{\mathfrak{m}=(x-\alpha)| \\ f(\alpha)=0}} i_{Spec(k\mathfrak{m}),*}\mathbb{F}_2 =: \mathcal{Q}. \tag{4}$$

We study now the cokernel of the morphism $id/\sigma^* : \mathcal{T} \to \mathcal{T}_1$. First of all notice that, thanks to the formula 2, the composite $q \circ (id/\sigma^*)$ is trivial. With some computations (completely analogous to [2], Lemma 3.5.18), it can be shown that $\forall \mathfrak{m} \in \mathrm{Spec}(R) \setminus D(f)$, $\forall a + bv \in \mathcal{T}_1(R_{\mathfrak{m}})$ such that a is 1 in the residue field $k(\mathfrak{m})$, $\exists\ c + dv \in \mathcal{T}(R_{\mathfrak{m}})$ with $id/\sigma^*(c + dv) = a + bv$.

Thus, we can finally conclude that the sheaves $\mathcal{T}/\mathbb{G}_m$ and $\mathcal{H}$ are isomorphic or, in other words, that there is an exact sequence of abelian sheaves over $\mathrm{Spec}(R)_{Zar}$:

$$0 \to \mathbb{G}_m \to \mathcal{T} \to \mathcal{H} \to 0.$$

This allows us to prove the following:

Lemma 31. *There is an isomorphism between the first cohomology groups*

$$H^1(Spec(R), \mathcal{T}) \simeq H^1(Spec(R), \mathcal{H})$$

Proof. Consider the long exact sequence induced in cohomology by $0 \to \mathbb{G}_m \to \mathcal{T} \to \mathcal{H} \to 0$:

$$H^1(Spec(R), \mathbb{G}_m) \to H^1(Spec(R), \mathcal{T}) \to H^1(Spec(R), \mathcal{H}) \to H^2(Spec(R), \mathbb{G}_m).$$

The elements of the group $H^1(Spec(R), \mathbb{G}_m)$ are the isomorphism classes of $\mathbb{G}_m$-torsors, or equivalently, thanks to Proposition15, invertible sheaves, which amounts to saying projective R-modules of rank 1; since R is a PID every finite projective module is free and this shows that $H^1(Spec(R), \mathbb{G}_m)$ consists only of the class of the trivial bundle $\mathcal{O}$.

As already said before, thanks to the vanishing theorem by Grothendieck, the group $H^2(Spec(R), \mathbb{G}_m)$ is trivial because the dimension of $\mathbb{P}^1_k$ is 1. This concludes the proof. □

Corollary 32. *The cohomological groups $H^1(Spec(R), \mathcal{H})$ and $H^1(U, \mathbb{G}_m)$ are isomorphic.*

Proof. Thanks to the previous lemma it is enough to show the isomorphism $H^1(\mathrm{Spec}(R), \mathcal{T}) \simeq H^1(U, \mathbb{G}_m)$. For this, notice that the map $\pi : U \to \mathbb{P}^1_k$ is finite, therefore the invertible sheaves on U are trivialized by open covering of $\mathbb{P}^1_k$, from this the thesis follow; for details see [2], Lemma 3.6.1. □

Notice that if f is square-free, U is a smooth, affine, hyperelliptic curve and if f is of odd degree and we denote by C the completed curve, then U is the scheme given by the complement of a single point in C, say P_∞. In the latter case we have $Pic(U) \simeq Pic^\circ(C)$; in order to see this we can proceed as follows: the inclusion of the free group generated by the class $[P_\infty]$ gives an exact sequence of abelian groups, namely:

$$0 \to [P_\infty]\mathbb{Z} \to \mathrm{Pic}(C) \to \mathrm{Pic}(U) \to 0.$$

On the other hand, we have the exact sequence defining $\mathrm{Pic}^\circ(C)$ as kernel of the degree morphism:

$$0 \to \mathrm{Pic}^\circ(C) \to \mathrm{Pic}(C) \stackrel{deg}{\to} \mathbb{Z} \to 0.$$

Since $\mathbb{Z}$ is free the sequence splits, an interesting choice is given by $s : \mathbb{Z} \to \mathrm{Pic}(C)$, defined by $s(1) = [P_\infty]$, indeed this gives the commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{s} & \mathrm{Pic}(C) & \longrightarrow & \mathrm{Pic}^\circ(C) & \longrightarrow & 0 \\ & & \downarrow \sim & & \| & & & & \\ 0 & \longrightarrow & [P_\infty]\mathbb{Z} & \xrightarrow{s} & \mathrm{Pic}(C) & \longrightarrow & \mathrm{Pic}(U) & \longrightarrow & 0 \end{array}$$

and we get an isomorphism $\mathrm{Pic}^\circ(C) \to \mathrm{Pic}(U)$ by functoriality of cokernel.

In conclusion, from the study of the exact sequence given by Theorem 23, we can conclude that we have a bijection:

$$\mathcal{G}(k[t]) \setminus X_f(k[t]) \to \mathrm{Pic}^\circ(C).$$

This arrow is just a bijection, but the target has a natural group structure. It would be nice to have some geometrical interpretation of this map. Notice that the domain is given by a quotient by the action of a group scheme, nevertheless it does not seem so interesting since the group scheme is not finite over k and, in particular, the group $\mathcal{G}(k[t])$ consists of matrices (with some properties) with entries in a polynomial ring.

In the next chapter we translate this problem in a different setting, we consider schemes over the projective line.

4 Turn to the projective setting

In the previous chapters, we showed how the study of the solutions of an equation produces, under some conditions, a map onto the Jacobian of a hyperelliptic curve. The aim of this chapter is to study the same problem on another base scheme: we no longer consider the affine line but the projective one; in particular in the previous chapter, in order to deal with the Picard group of a curve, we assumed the polynomial f to be of odd degree, here we would like to recover something for a polynomial of even degree.

In the following we will always assume that the field k is algebraically closed and that its characteristic is different from 2: we have no reason to believe these hypotheses are necessary, but with them we can get what we are looking for; maybe working with fewer hypotheses can be the subject for a future work.

Now we see how we can modify the previous situation to have a nice interpretation in the projective setting. First of all, a natural thing is to consider, instead of a polynomial, a global section f of the invertible sheaf $\mathcal{O}(2d)$.

In order to keep a correspondence to the first chapter we write $\mathbb{P}^1_k = \mathbb{A}^1_k \cup \{\infty\} = \mathrm{Spec}(k[t]) \cup \{\infty\}$; on the other hand we will denote $\mathbb{P}^1_k \setminus \{0\} = \mathrm{Spec}(k[s])$, where the gluing isomorphism on the intersection is given identifying s with t^{-1}; moreover we fix as d-th Serre twist the sheaf $\mathcal{O}(d\infty)$ so that $\Gamma(\mathbb{P}^1_k, \mathcal{O}(d))$ can be seen as the set polynomials of degree less or equal than d.

Working along the lines of the previous chapter, we want a scheme parametrizing the solutions to the equation $ab + c^2 = f$. First of all, we want to make precise this last statement. For this, consider the following:

Definition 33. Let X be a scheme, $\mathcal{L}$ an invertible sheaf and $\mathcal{E}$ a locally free sheaf on X. For an $\mathcal{L}$-valued bilinear form we mean a morphism of sheaves $b : \mathcal{E} \times \mathcal{E} \to \mathcal{L}$ which is $\mathcal{O}_X$-bilinear, or equivalently, it induces a morphism $\tilde{b} : \mathcal{E} \otimes \mathcal{E} \to \mathcal{L}$.

Moreover, we say that $\tilde{b}$ is symmetric if it is invariant for the switch map $\mathcal{E} \otimes \mathcal{E} \to \mathcal{E} \otimes \mathcal{E}$.

Remark 34. The composite of an $\mathcal{L}$-valued bilinear form with the diagonal morphism $\Delta : \mathcal{E} \to \mathcal{E} \otimes \mathcal{E}$ defines an $\mathcal{L}$-valued quadratic form $q_b := b \circ \Delta$ in the sense that the following diagram:

$$\begin{array}{ccc} \mathcal{O}_X \otimes \mathcal{E} & \longrightarrow & \mathcal{E} \\ \downarrow{\scriptstyle (\_)^2 \otimes q_b} & & \downarrow{\scriptstyle q_b} \\ \mathcal{O}_X \otimes \mathcal{L} & \longrightarrow & \mathcal{L} \end{array}$$

commutes; where the horizontal arrows are induced by the maps defining the $\mathcal{O}$-module structure of $\mathcal{L}$ and $\mathcal{E}$.

Let $\mathcal{O}(n)$ denote, for every integer n, the n-th Serre twist on $\mathbb{P}^1_k$, the subject of our study will be the ($\mathcal{O}(d)$-valued) quadratic form defined, for every scheme $X \to \mathbb{P}^1_k$, by:

$$\begin{aligned} q : \mathcal{O}(d)^3(X) &\to \mathcal{O}(2d)(X) \\ (a, b, c) &\mapsto ab + c^2 \end{aligned}$$

Since we want a scheme parametrizing the solutions of $q((a, b, c)) = f$, we make use of the fact that if $\mathcal{E}$ is a locally free sheaf of finite rank over a scheme

X, then it is representable, over the big-Zariski site $(Sch_{/X})_{Zar}$, by the scheme $\underline{\mathcal{E}} := \underline{\mathrm{Spec}}\,(Symm(\mathcal{E}^\vee))$.

Thus, consider the morphism of schemes over $\mathbb{P}^1_k$, $\underline{\mathcal{O}(d)}^3 \to \underline{\mathcal{O}(2d)}$, induced by q (by abuse of notation we will denote it by q too). In analogy with the previous chapter, we want X_f to be the scheme such that for every $T \xrightarrow{p} \mathbb{P}^1_k$:

$$X_f(T) = \{(a,b,c) \in (\Gamma(T, p^*\mathcal{O}(d)^3))|\ ab + c^2 = f \text{ and } Z(a) \cap Z(b) \cap Z(c) = \emptyset\}.$$

To impose the condition about the zero loci we shall consider the open subscheme $W \hookrightarrow \underline{\mathcal{O}(d)}^3$ defined to be the complement of the zero section; hence we finally define $\overline{X_f}$ to be the pull-back of $q_{|W}$ along the section f:

$$\begin{array}{ccc} X_f & \longrightarrow & W \\ \downarrow & & \downarrow{\scriptstyle q_{|W}} \\ \mathbb{P}^1_k & \xrightarrow{f} & \underline{\mathcal{O}(2d)}. \end{array}$$

In analogy with the affine case, we have a group scheme acting on the sheaf defined by X_f, indeed the group scheme $SO(q)$ acts on $\underline{\mathcal{O}(d)}^3$; moreover the quadratic form $q : \underline{\mathcal{O}(d)}^3 \to \underline{\mathcal{O}(2d)}$ and the zero section $\mathbb{P}^1_k \to \underline{\mathcal{O}(2d)}$ are invariant for the action, thus the action restricts to W and to X_f. Let $\mathcal{G}$, as for the affine case, denote the sheaf of groups represented by $SO(q)$, then we have an action of $\mathcal{G}$ on the sheaf represented by X_f, say $\mathcal{X}_f$.

We have already seen the transitivity of the action on $\mathbb{P}^1 \setminus \{\infty\}$, thus we are left to show the transitivity just at the stalk ∞. Before going on, it is better to fix some notation; the sheaf $\mathcal{O}(2d)$ is locally free of rank 1, hence on $\mathbb{P}^1_k \setminus \{0\}$ is isomorphic to a $k[t]$-module of rank 1 and on $\mathbb{P}^1_k \setminus \{\infty\}$ is isomorphic to a $k[s]$-module of rank 1. From now on, in the following we will fix generators of these free modules, i.e. we describe the restriction maps as:

$$\begin{array}{cc} \mathcal{O}(2d) \to \mathcal{O}(2d)(\mathbb{P}^1_k \setminus \{\infty\}) & \mathcal{O}(2d) \to \mathcal{O}(2d)(\mathbb{P}^1_k \setminus \{0\}) \\ x \mapsto x & x \mapsto x/t^{2d} \end{array}$$

in other words we fix generators $\mathcal{O}(2d)(\mathbb{P}^1_k \setminus \{\infty\}) = 1 \cdot k[t]$ and $\mathcal{O}(2d)(\mathbb{P}^1_k \setminus \{0\}) = t^{2d} \cdot k[s] = s^{-2d}k[s]$.

It is now straightforward showing that the transitivity at ∞ can be reduced to the proof of the transitivity at 0, indeed, since transitivity on the Zariski topology is a local property, it is enough to look at the solutions on a neighbourhood of ∞, like $\mathbb{P}^1 \setminus \{0\}$, and there the situation is identical to the one on $\mathbb{P}^1_k \setminus \{\infty\}$, in the sense that we are looking at solutions of:

$$q_{|\mathbb{P}^1 \setminus \{0\}} : \mathcal{O}(d)^3(\mathbb{P}^1 \setminus \{0\}) = (1/t^d \cdot k[s])^3 \to \mathcal{O}(2d)(\mathbb{P}^1 \setminus \{0\}) = 1/t^{2d} \cdot k[s] = s^{2d}k[s]$$
$$1/t^d(a,b,c) \mapsto (1/t^{2d})(ab + c^2 - f)$$

where the action of $\mathcal{G}$ is the same one of the affine case. In particular, if we denote the section $f_{\mathbb{P}^1_k \setminus \{\infty\}} = \sum_{i=0}^{2d} f_i t^i$, then $f_{\mathbb{P}^1_k \setminus \{0\}} = s^{-2d} f = s^{-2d} \sum_{i=0}^{2d} f_i s^{2d-i}$. This shows how to deduce the transitivity at the point ∞ from Theorem 25.

From now on, we assume that the restriction of f to $\mathbb{P}^1_k \setminus \{\infty\}$ is a square-free polynomial of degree $2d$, therefore a point in $\mathcal{X}_f(\mathbb{P}^1_k)$ is given by $P := (f_1, f_2, 0)$, where $f = f_1 f_2$ for two global sections $f_1, f_2 \in \mathcal{O}(d)$ whose restrictions to $\mathbb{P}^1_k$ are two coprime polynomials of degree d.

As in the affine case, the hypotheses of Theorem 23 are fulfilled and so we have an exact sequence over the small Zariski site $(\mathbb{P}^1_k)_{Zar}$:

$$\mathcal{H}(\mathbb{P}^1_k) \hookrightarrow \mathcal{G}(\mathbb{P}^1_k) \longrightarrow X_f(\mathbb{P}^1_k) \longrightarrow H^1((\mathbb{P}^1_k)_{Zar}, \mathcal{H}) \longrightarrow H^1((\mathbb{P}^1_k)_{Zar}, \mathcal{G})$$

where with $\mathcal{H} := \mathcal{G}_P$ we denote the stabilizer sheaf of the point P.

As before we proceed with the study of the objects appearing in this exact sequence. We begin with the stabilizer $\mathcal{H}$, using the same strategy of the affine case: we let it act on the orthogonal complement. For this, consider the orthogonal complement $P^\perp$, defined to be the kernel of the morphism of sheaves:

$$\begin{aligned} \mathcal{O}(d)^3 &\to \mathcal{O}(2d) \\ (a,b,c) &\mapsto b((a,b,c),P) = (af_2 + bf_1)/2 \end{aligned}$$

thus we have that $P^\perp$ is a subsheaf of $\mathcal{O}(d)^3$, moreover it is locally free of rank 2. Indeed, two orthogonal and independent elements which lie in $P^\perp$ are given by $(0,0,1)$ and $(f_1,-f_2,0)$. This gives us the monomorphsim $\mathcal{O}(d\cdot\infty)(0,0,1)\oplus \mathcal{O}\cdot(f_1,f_2,0) \hookrightarrow P^\perp$ and by rank reasons we conclude that it actually is an isomorphism. We focus our attention on the sheaf $P^\perp$; once restricted to the opens $\mathbb{P}^1_k \setminus \{0\}$ and $\mathbb{P}^1_k \setminus \{\infty\}$, it is described by a free module of rank 1 over the ring $k[t]$ and $k[s]$ respectively. In order to see what the discriminant of the form b restricted to $P^\perp$ is, we can compute the Gram matrices relative to $(P^\perp, b_{|P^\perp})$, once restricted on the two affines. For this, first of all, notice that b, for the standard basis of $\mathcal{O}(d)^3$ is represented by the matrix with constant values, i.e. global sections of the structure sheaf:

$$\frac{1}{2}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Then, with the above notation, we have that on $\mathbb{P}^1_k \setminus \{\infty\}$ our basis is given by $(0,0,1)$ and $(f_1,-f_2,0)$ which gives the Gram matrix:

$$\begin{pmatrix} 1 & 0 \\ 0 & -f \end{pmatrix}$$

while on the open $\mathbb{P}^1_k \setminus \{0\}$ the basis has the form $(0,0,1), 1/t^d(f_1,-f_2,0)$ so the Gram matrix is:

$$\begin{pmatrix} 1 & 0 \\ 0 & -\frac{f}{t^{2d}} \end{pmatrix}$$

hence we conclude that the bilinear symmetric form b restricted to the subsheaf $P^\perp$ has discriminant $-f$ as section of $\mathcal{O}(2d)$.

Recall that in the previous chapter we came across an affine curve, now we consider a projective plane curve: consider the zero locus of the equation $s^2 = f$ for s a local section of $\mathcal{O}(d)$, in other words we define C to be the pull-back of $(-)^2$ along f:

$$\begin{array}{ccc} \tilde{C} & \longrightarrow & \underline{\mathcal{O}(d)} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle (-)^2} \\ \mathbb{P}^1_k & \xrightarrow{f} & \underline{\mathcal{O}(2d)} \end{array}$$

where by $(\_)^2$ we mean the map that on T-points, for every scheme $T \to \mathbb{P}^1$, is given by:

$$\begin{aligned} \underline{\mathcal{O}(d)}(T) &\to \underline{\mathcal{O}(2d)}(T) \\ s &\mapsto s^2. \end{aligned}$$

Notice that the curve $\pi \to C$ is a hyperelliptic curve.

Re-define $\mathcal{T} := \pi_* \mathbb{G}_{m,\tilde{C}}$, the pushforward of the multiplicative group of the completed curve, then, from the previous chapter, we recover the description of the stabilizer as cokernel in the short exact sequence of sheaves on the site $(Sch_{/\mathbb{P}^1_k})_{Zar}$:

$$0 \to \mathbb{G}_{m,\mathbb{P}^1_k} \to \mathcal{T} \to \mathcal{H} \to 0.$$

As before we can consider the long exact sequence in cohomology:

$$\mathrm{Pic}(\mathbb{P}^1_k) \xrightarrow{\pi^*} \mathrm{Pic}(C) \to H^1(\mathbb{P}^1_k, \mathcal{H}) \to H^2(\mathbb{P}^1_k, \mathbb{G}_m)$$

Again, always thanks to the vanishing theorem of Grothendieck ([1], Chapter III,Theorem 2.7), the group $H^2(\mathbb{P}^1_k, \mathbb{G}_m)$ is trivial because of the dimension of $\mathbb{P}^1_k$.

The group $\mathrm{Pic}(\mathbb{P}^1_k)$ is known to be isomorphic to $\mathbb{Z}$; we now have a closer look at the Picard group of the curve C: since there is a rational point on C, the degree map is surjective onto $\mathbb{Z}$, and this gives us a split $\mathrm{Pic}(\mathbb{Z}) \simeq \mathrm{Pic}^\circ(C) \oplus \mathbb{Z}$. To give an isomorphism is equivalent to choosing a section of the degree map; for instance we can choose a ramification point, say $y \in C$ such that $\pi(y) = x \in \mathbb{P}^1_k$, then we have the isomorphism:

$$\begin{aligned} Pic(C) &\to Pic^\circ(C) \oplus \mathbb{Z} \\ \mathcal{L} &\mapsto (\mathcal{L} \otimes \mathcal{O}(-deg(\mathcal{L}) \cdot y), deg(\mathcal{L})) \end{aligned}$$

Let fix even the isomorphism $\gamma : \mathbb{Z} \to Pic(\mathbb{P}^1_k)$ imposing $\gamma(1) = \mathcal{O}(x)$, then the morphism π^* between the Picard groups is given by:

$$\begin{aligned} \mathbb{Z} \to \mathrm{Pic}(\mathbb{P}^1_k) \to \mathrm{Pic}(C) &\to \mathrm{Pic}^\circ(C) \oplus \mathbb{Z} \\ 1 \mapsto \mathcal{O}(x) &\mapsto \mathcal{O}(2y) \mapsto (\mathcal{O}_C, 2) \end{aligned}$$

hence we conclude that $\mathrm{Pic}^\circ(C) \to \mathrm{Pic}(C)$ is injective and that $H^1(\mathbb{P}^1_k, \mathcal{H})$ is isomorphic to $\mathrm{Pic}^\circ(C) \oplus \mathbb{Z}/2\mathbb{Z}$.

We consider now the pointed set $H^1(\mathbb{P}^1_k, \mathcal{G})$; we showed that the corresponding pointed set in the affine case is trivial, but it does not hold the same over $\mathbb{P}^1_k$; indeed, consider the exact sequence of sheaves of groups defining PGL_2:

$$0 \to \mathbb{G}_m \to GL_2 \to PGL_2 \to 0$$

considering the exact sequence in cohomology (since we are dealing with non abelian groups we don't have groups), and recalling that $H^2(\mathbb{P}^1_k, \mathbb{G}_m)$ is trivial, we have:

$$\begin{aligned} 0 \to k^* \to GL_2(k) \to PGL_2(k) \to 0 \\ \mathrm{Pic}(\mathbb{P}^1_k) \hookrightarrow H^1(\mathbb{P}^1_k, PGL_2) \twoheadrightarrow H^1(\mathbb{P}^1_k, PGL_2) \end{aligned}$$

Recall that the set $H^1(\mathbb{P}^1_k, GL_2)$ consists of the GL_2-torsors over $\mathbb{P}^1_k$, i.e. it corresponds to the set $\{\mathcal{O}(a) \oplus \mathcal{O}(b) | (a,b) \in \mathbb{Z}\ b \geq a\}$; moreover the group $\mathbb{G}_m$ embeds diagonally in GL_2, therefore, the induced map on the first cohomology set is given by:

$$\begin{aligned} H^1(\mathbb{P}^1_k, \mathbb{G}_m) &\to H^1(\mathbb{P}^1_k, PGL_2) \\ [\mathcal{O}(a)] &\mapsto [\mathcal{O}(a) \oplus \mathcal{O}(a)] \end{aligned}$$

for $a \in \mathbb{Z}$. We deduce also that the pointed set $H^1(\mathbb{P}^1_k, PGL_2)$ is in bijection with the set of natural numbers $\mathbb{N}$ and we have the map:

$$\begin{aligned} H^1(\mathbb{P}^1_k, GL_2) \simeq \{(a,b) \in \mathbb{Z}^2 | b \geq a\} &\to H^1(\mathbb{P}^1_k, PGL_2) \\ (a,b) &\mapsto b - a \end{aligned}$$

In conclusion the exact sequence of Theorem 23 gives us the maps:

$$\mathcal{G}(\mathbb{P}^1_k) \setminus \mathcal{X}_f(\mathbb{P}^1_k) \hookrightarrow H^1(\mathbb{P}^1_k, \mathcal{H}) \to H^1(\mathbb{P}^1_k, PGL_2).$$

Unluckily we have no more a surjection onto the Picard group of a curve, but the LHS is farly more interesting than in the affine case. Notice that the set $X_f(\mathbb{P}^1_k)$ is in bijection with the k-points of a variety over k; indeed the set $X_f(\mathbb{P}^1_k)$ is the set of triples of polynomial (a,b,c) of degree less or equal than d with coefficients in k which satisfy the equation $ab + c^2 = f$.

We proceed now at the construction of this variety: let the polynomial f be written as $f = \sum_{i=0}^{2d} f_i t^i$ and let, analogously, a_i, b_i, c_i be the coefficients of a, b, c, then being a solution to $ab + c^2 = f$ can be stated in function of the coefficients, saying that a_i, b_i, c_i satisfy the $2d$ equations:

$$\begin{cases} h_0 := a_0 b_0 + c_0^2 - f_0 = 0 \\ \dots \\ h_{2d} := a_d b_d + c_d^2 - f_{2d} = 0 \end{cases}$$

It is clear now that, in order to see this set as the k-points of a variety, we consider the schemes $X :=$Spec$[\{t_i\}_{i=0}^{2d}]$ and $Y :=$Spec$(k[\{x_i\}_{i=0}^d, \{y_i\}_{i=0}^d, \{z_i\}_{i=0}^d])$ and the map defined on the rings by:

$$\begin{aligned} \psi : Spec\left[\{t_i\}_{i=0}^{2d}\right] &\to k\left[\{x_i\}_{i=0}^d, \{y_i\}_{i=0}^d, \{z_i\}_{i=0}^d\right] \\ t_i &\mapsto h_i(\{x_j\}, \{y_j\}, \{z_j\}) \end{aligned}$$

the variety V is given by the pullback of Spec(ψ) along the k-point representing f:

$$\begin{array}{ccc} V & \longrightarrow & X \\ \downarrow & & \downarrow{\scriptstyle \mathrm{Spec}(\psi)} \\ Spec(k) & \xrightarrow{f} & Y. \end{array}$$

We have the following:

Proposition 35. *The variety V defined above is smooth.*

Proof. In order to prove the claim it is enough to show that the map induced by Spec(ψ) at the tangent spaces of points of V is surjective. To see this, consider a triple of polynomials $\bar{a}, \bar{b}, \bar{c}$ such that $\bar{a}\bar{b} + \bar{c}^2 = f$ then we have:

$$(\bar{a} + \epsilon a)(\bar{b} + \epsilon b) + (\bar{c} + \epsilon c)^2 = f + \epsilon(\bar{a}b + \bar{b}a + 2\bar{c}c) + \epsilon^2 ...$$

therefore we are left to prove that the map:

$$\begin{aligned}(k[t]_{\leq d})^3 &\to k[t]_{\leq 2d}\\ (a,b,c) &\mapsto \bar{a}b + \bar{b}a + 2\bar{c}c\end{aligned}$$

is surjective. The conclusion is then given by the following lemma. □

Lemma 36. *Let k be a field, $n \in \mathbb{N}_{\geq 2}$, $f_1, ...f_n \in \Gamma(\mathbb{P}^1, \mathcal{O}(d\infty))$ without common zeroes, then the map:*

$$\begin{aligned}\tilde{\varphi} : (k[t]_{\leq d})^n &\to k[t]_{\leq 2d}\\ (g_1, ..., g_n) &\mapsto \sum g_i f_{i|\mathbb{P}^1\setminus\{\infty\}}\end{aligned}$$

is surjective.

Proof. Consider the morphism of sheaves $\varphi : \mathcal{O}(d)^n \to \mathcal{O}(2d)$ whose restriction to the affine $\mathbb{P}^1_k$ is $\tilde{\varphi}$; thanks to the hypothesis about the zero locus of the f_i it is surjective at every stalk, i.e. it is a surjective morphism of sheaves. Let K denote the kernel and Serre twist by $\mathcal{O}(-(d+1)\infty)$:

$$0 \to K(-(d+1)\infty) \to \mathcal{O}(-\infty)^n \to \mathcal{O}((d-1)\infty) \to 0$$

considering the long exact sequence in cohomology we have that $h^1(\mathcal{O}(-\infty)) = h^0(\mathcal{O}(-\infty)) = 0$, so $h^1(K) = h^0(\mathcal{O}((d-1)\infty)) = d$ Moreover, from $K \hookrightarrow \mathcal{O}(d)^n$ we deduce that $K \simeq \oplus_{i=1}^{n-1}\mathcal{O}(a_i)$ for some $a_i \leq d$. Thus we deduce:

$$d = h^1(K(-(d+1)\infty)) = h^1(\oplus_{i=1}^{n-1}(\mathcal{O}(a_i - (d+1))) = \sum_{i=1}^{n-1}(d - a_i)$$

From this we see that $\forall i\ a_i \geq 0$, thus $h^1(K) = 0$ and this concludes the proof. □

Now that we have a variety whose k-points correspond to the set $X_f(\mathbb{P}^1_k)$, it would be extremely interesting to extend the map

$$X_f(\mathbb{P}^1_k) \to \mathcal{G}(\mathbb{P}^1_k) \setminus \mathcal{X}_f(\mathbb{P}^1_k) \hookrightarrow H^1(\mathbb{P}^1_k, \mathcal{H}) \simeq \mathrm{Pic}^\circ(C) \oplus \mathbb{Z}/2\mathbb{Z}$$

to a morphism of schemes. In the same way, it seems to be very interesting the possibility of defining a lift $V \to$Pic(C) which induces the map $V \to H^1(\mathbb{P}^1_k, \mathcal{H})$ by composition with Pic(C)$\to H^1(\mathbb{P}^1_k, \mathcal{H}) \simeq$Pic$^\circ(C) \oplus \mathbb{Z}/2\mathbb{Z}$.

References

[1] Hartshorne, R. *Algebraic geometry*. Berlin, Heidelberg, New York: Springer-Verlag, 1977.

[2] Ph.D. thesis, Albert Gunawan, *Gauss's theorem on sums of 3 squares, sheaves, and Gauss Composition*, Universiteit Leiden, 2016,
available at `https://openaccess.leidenuniv.nl/handle/1887/38431`

[3] J.Giraud, *Cohomologie non abélienne, Die Grundlehren der mathematischen Wissenschaften, Band 179, Springer-Verlag, 1971*

[4] The Stacks Project author, *Stacks project*, `http://stacks.math.columbia.edu/`