Reconstruction of Cubic Surfaces

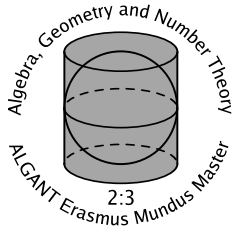
Calliari, D.

Davide Calliari

Reconstruction of Cubic Surfaces

Master's thesis, defended on July 7, 2011

Thesis advisor: Robin de Jong, Ronald van Luijk



Mathematisch Instituut
Universiteit Leiden

Contents

1 Introduction **3**

2 Symmetric quasigroups and singular cubic curves **4**
2.1 Symmetric quasigroups 4
2.2 Group law on cubic curves 9
2.2.1 Cubic curves with a K-rational singular point 11

3 Geometric Reconstruction of Cubic Surfaces **19**
3.1 Geometric reconstruction of a projective line 19
3.2 (C_m, C_a)-configurations 23
3.2.1 (C_m, C_a)-configurations from cubic surfaces 24
3.2.2 Reconstruction of the configuration 27
3.3 Geometric reconstruction of K from a (C_m, C_a)-configuration 28
3.4 Geometric reconstruction of the cubic surface V 29

4 Combinatorial Reconstruction of Cubic Surfaces **34**
4.1 Combinatorial Projective Line 34
4.2 Combinatorial Cubic Surfaces 35
4.2.1 Combinatorial cubic surfaces of geometric origin 36
4.3 Combinatorial (C_m, C_a)-configurations 36
4.4 Combinatorial Tetrahedral Configurations 37

5 Reconstruction Theorems **39**
5.1 Construction of a geometric cubic surface from combinatorial data 39
5.2 Reconstruction of the cubic surface 40

1 Introduction

In this paper, we want to reconstruct a cubic surface starting from some combinatorial data of it. But what "reconstruction" means precisely? For a general situation, it consists of the following problem.

Fix a generic geometric object. We do not know this object, but we know only partial information about it (expressible in an abstract, combinatorial way). Our purpose is to get back all the information about that geometric object, using only the combinatorial data that we have. The first (obvious) request is that we can actually get the partial information we need from the knowledge of the geometric object, of course. But mainly we want to construct a procedure that permit us to construct uniquely an object, of the same type as the original one, and we would like that this construction leads to an object that is isomorphic to the object we are started with. The problem of reconstruction investigates in how much information we need to do this, and in which cases we are able to do this. In other words, we would like to find the (combinatorial) constraints that characterize that object.

We are interested in cubic surfaces. The combinatorial data we are starting with consist more or less of the rational points, of the plane sections and of a ternary relation that states when three points are collinear. Our aim is to construct a way to get from these constraints a cubic surface that is isomorphic to the initial one. This construction does not work for any cubic surface, for example it will fails for ruled cubic surfaces. We refer to the section 5 in the end of this paper for a precise statement of these ideas, into some theorems.

In chapter 2, we will introduce some general facts on cubic curves. In particular, we will show that we can give to the set of the smooth rational points a structure of abelian group, and we will analyze this structure, especially for the singular cubics.

In chapter 3, we will do the following: first we will show how we can reconstruct a projective line; later on we will analyze how starting with a (C_m, C_a)-configuration we are able to find the ground field of the cubic surface; finally we will reconstruct the whole surface from a tetrahedral configuration.

In chapter 4, we translate all the geometric constructions of the previous chapter in a combinatorial way, and we raffine our construction using pencils of plane sections.

In chapter 5, we finally state the main theorem, divided into some statements, that sums up all what we have done in chapter 3 and in chapter 4.

2 Symmetric quasigroups and singular cubic curves

If we have any irreducible (plane) cubic curve, it is possible to give a structure of abelian group to it. In this chapter, we intend to analyze this structure, especially for cubics that are singular and whose singularity is defined over K, the definition field.

More generally, we will show that the smooth part of an (irreducible) cubic curve forms algebraically an abelian symmetric quasigroup. We will see then that choosing one smooth (K-rational) point makes it into an abelian group.

2.1 Symmetric quasigroups

We start saying what a symmetric quasigroup is. We can define it equivalently in the following two ways:

Definition 2.1 (Symmetric quasigroup - geometric definition)**.** *Let S be a nonempty set and consider $\mathfrak{Q}$ a subset of the cartesian product $S \times S \times S$. We will call the pair $(S, \mathfrak{Q})$ a* symmetric quasigroup *if the two following properties hold:*

(i) $\mathfrak{Q}$ is invariant under permutations of factors S.

(ii) For all $p, q \in S$, there exists a unique $r \in S$ such that $(p, q, r) \in \mathfrak{Q}$.

Definition 2.2 (Symmetric quasigroup - algebraic definition)**.** *Let S be a nonempty set and $\circ : S \times S \to S$ a binary composition law on S. Then $(S, \circ)$ is called a* symmetric quasigroup *if the two following properties hold for all $p, q \in S$:*

(a) $p \circ q = q \circ p$.

(b) $p \circ (p \circ q) = q$.

We will now show that this two definitions, the geometric and the algebraic one, are equivalent.

Proof. We will prove it in the following sense:

1. Starting from a symmetric quasigroup $(S, \mathfrak{Q})$ as in definition 2.1, by denoting

   $$\circ : S \times S \to S \quad \text{the function defined through the property} \quad (p, q, p \circ q) \in \mathfrak{Q},$$

   we obtain a symmetric quasigroup $(S, \circ)$ as in definition 2.2.

2. Starting from a symmetric quasigroup $(S, \circ)$ as in definition 2.2, we denote

   $$\mathfrak{Q} := \{(p, q, p \circ q) : p, q \in S\},$$

   and we obtain a symmetric quasigroup $(S, \mathfrak{Q})$ as in definition 2.1.

We pass now to prove each point.

1. Consider the couple $(S, \mathfrak{Q})$ satisfying the properties (i) and (ii) of definition 2.1, we define $\circ$ as above. Using the condition (ii), we have that $\circ$ is well defined. What it remains to prove is that $\circ$ satisfies the properties (a) and (b) of definition 2.2.

   (a) Using the definition of $\circ$, we get that $(p, q, p \circ q)$ belongs to $\mathfrak{Q}$, and hence, by (i), also $(q, p, p \circ q)$ belongs to $\mathfrak{Q}$. This means that $p \circ q = q \circ p$, thanks to the property of unicity in the condition (ii).

   (b) Again we have that $(p, q, p \circ q)$ belongs to $\mathfrak{Q}$, and hence, by (i), also $(p, p \circ q, q)$ belongs to $\mathfrak{Q}$. This implies that $q = p \circ (p \circ q)$, using the unicity property in condition (ii).

2. Consider $(S, \circ)$ satisfying the properties (a) and (b) of definition 2.2. We have to check that $\mathfrak{Q}$ defined above satisfies (i) and (ii) of definition 2.1.

   (ii) The property (ii) follows directly by the definition of $\mathfrak{Q}$. Fix $p, q \in \mathfrak{Q}$. Then $(p, q, p \circ q)$ belongs to $\mathfrak{Q}$, and this element $p \circ q$ is unique with this property.

   (i) We have to prove that $\mathfrak{Q}$ remains stable under permutation. This means the following statement: if (p_1, p_2, p_3) are in $\mathfrak{Q}$, then $(p_{\sigma(1)}, p_{\sigma(2)}, p_{\sigma(3)})$ belongs to $\mathfrak{Q}$ too, for any permutation σ in the symmetric group S_3. Equivalently, if $p_3 = p_1 \circ p_2$, then we must have that $p_{\sigma(3)} = p_{\sigma(1)} \circ p_{\sigma(2)}$. We need to prove this only on a pair of generators of S_3, i.e. the two permutations (12) and (123). Assume then $p_3 = p_1 \circ p_2$. If $\sigma = (12)$, we have to show that $p_3 = p_2 \circ p_1$, equivalently $p_1 \circ p_2 = p_2 \circ p_1$, which is true by (a). If instead $\sigma = (123)$, the claim becomes $p_1 = p_2 \circ p_3$; using the property (a), this is equivalent to $p_1 = p_2 \circ (p_2 \circ p_1)$, which is true by (b).

□

Now we want to say what an abelian quasigroup is. To do this we need the following definitions.

Definition 2.3. *Let S be a symmetric quasigroup. For each $p \in S$, we define the following automorphism:*

$$\begin{array}{rccc} t_p\colon & S & \longrightarrow & S \\ & q & \longmapsto & p \circ q \end{array}$$

This map is an involution, i.e. $t_p^2 = id_S$ (this holds using the property (b) of definition 2.2 of a symmetric quasigroup).

We define then

$$\Gamma := \langle \{t_p : p \in S\} \rangle$$

where with the brackets $\langle\rangle$ we mean the group generated inside $\mathrm{Aut}(S)$*, the group of automorphisms of S, with composition of functions as multiplication.*

We finally define Γ^0 the subgroup of Γ consisting of elements that can be written as products of an even number of involutions t_p.

Definition 2.4. *We say that a symmetric quasigroup $(S, \circ)$ is **abelian**, if the group Γ^0 defined above is abelian.*

There are some equivalent useful definitions of an abelian symmetric quasigroup. Before stating them, it's nice to have the following lemma.

Lemma 2.5. *Let S be a symmetric quasigroup. Assume that we have a group law $\cdot$ on S, with unit element u. Assume furthermore that this group law is commutative. Then these three properties are equivalent:*

(a) For all $p, q \in S$, we have $p \cdot q = u \circ (p \circ q)$.

(b) For all $p, q \in S$, we have $p \circ q = (u \circ u) \cdot p^{-1} \cdot q^{-1}$.

(c) The evaluation map $\varphi_u : \Gamma^0 \to S$, defined by sending $\gamma \mapsto \gamma(u)$, is a group isomorphism.

Proof.

$a \Rightarrow b$ It is clear that it is equivalent to show that $(p \circ q) \cdot q \cdot p = u \circ u$. Using the hypothesis and the properties of symmetric quasigroup, we have that $(p \circ q) \cdot q \cdot p = (u \circ ((p \circ q) \circ q)) \cdot p = (u \circ p) \cdot p = u \circ ((u \circ p) \circ p) = u \circ u$.

$b \Rightarrow c$ We first see that, for all $p, q, s \in S$ we have

$$t_p t_q(s) = (p^{-1} q) s$$

Indeed, using the hypothesis, we have that

$$t_p t_q(s) = t_p\,(q \circ s) = t_p\left((u \circ u) \cdot q^{-1} \cdot s^{-1}\right) = (u \circ u) \cdot p^{-1} \cdot \left((u \circ u) \cdot q^{-1} \cdot s^{-1}\right)^{-1} =$$

$$= (u \circ u) \cdot p^{-1} \cdot s \cdot q \cdot (u \circ u)^{-1} = (p^{-1} \cdot q) \cdot s,$$

using the commutativity.

For each $p \in S$, we can then define

$$\tau_p \coloneqq t_u t_p$$

Observe that they are translations, because for any $s \in S$ we have $\tau_p(s) = t_u t_p(s) = u^{-1} \cdot p \cdot s = p \cdot s$.

Using this definition, we obtain that Γ^0 consists only of these kind of elements:

$$\Gamma^0 = \{\tau_s : s \in S\}$$

Indeed, any even product of our involutions can be rewritten as an element τ_s for a suitable $s \in S$. This is clear from these two facts: first we have that $t_p t_q = t_u t_{p^{-1}q} = \tau_{p^{-1}q}$; secondly we have that $\tau_p \tau_q = \tau_{pq}$, simply because these elements are translations.

After these general observations, we can define a map $\varphi_u : \Gamma^0 \to S$ sending $\tau_p \mapsto \tau_p(u) = p \cdot u = p$. Moreover φ becomes a group isomorphism from Γ^0 to S. Indeed, φ is surjective because, fixed $p \in S$, we have that $\varphi(\tau_p) = \tau_p(u) = p$; it is a group homomorphism because $\varphi(\tau_p \tau_q) = \varphi(\tau_{pq}) = \tau_{pq}(u) = pq = \tau_p(u)\tau_q(u)$. Finally, it is injective because, if $\varphi(\tau_p) = u$, then $\tau_p(u) = u$, that means $p = u$, as just seen.

$c \Rightarrow a$ We first observe that $p = u \circ (p \circ u) = t_u t_p(u)$. Hence, using the group homomorphism property of φ, we get for any $p, q \in S$ the following:

$$pq = t_u t_p(u) t_u t_q(u) = t_u t_p t_u t_q(u) = u \circ (p \circ (u \circ (q \circ u))) = u \circ (p \circ q)$$

□

We are now ready to state the equivalent definitions of an abelian symmetric quasigroup. Notice that the choice of an element transforms the abelian symmetric quasigroup into an abelian group.

Theorem 2.6 (Abelian Symmetric Quasigroup - equivalent definitions)**.** *Consider a symmetric quasigroup $(S, \circ)$. The following conditions are equivalent:*

(i) *S is an abelian symmetric quasigroup. By definition that Γ^0 is abelian.*

(ii) *For some element $u \in S$, there exists a structure of an abelian group on S with the three equivalent properties of lemma 2.5: the group law is defined by $pq := u \circ (p \circ q)$ and it has u as unit element; the law is induced by the bijection $\varphi_u : \Gamma^0 \to S$ where $\gamma \mapsto \gamma(u)$; and furthermore we have that $p \circ q = (u \circ u)p^{-1}q^{-1}$, for all $p, q \in S$.*

(iii) *For all $u \in S$, we have an abelian group law on S as in (ii).*

(iv) *For all $p, q, r \in S$, it holds $(t_p t_q t_r)^2 = id$.*

Furthermore, any such abelian group law, obtained once fixed an element of S, differs from the others by a translation. With this, we mean that, fixed two such abelian group laws on S, say $\cdot$ (with unit element e) and $*$ (with unit element u), the following diagram is commutative:

$$\begin{array}{ccc} S \times S & \xrightarrow{\cdot} & S \\ {\scriptstyle \psi_u \times \psi_u}\downarrow & & \downarrow{\scriptstyle \psi_u} \\ S \times S & \xrightarrow{*} & S \end{array}$$

where $\psi_u : s \mapsto u \cdot s$.

Proof.

i ⇒ *ii* Suppose Γ^0 abelian and, for fixed u, define $pq := u \circ (p \circ q)$. We will prove that this yields an abelian group law, and then the claim (*ii*) will follow using lemma 2.5. Consider $p, q, r \in S$. The commutativity holds because $pq = u \circ (p \circ q) = u \circ (q \circ p) = qp$. The unit element is u because $up = u \circ (u \circ p) = p$. The inverse of p is

$$p^{-1} := (u \circ u) \circ p$$

because $pp^{-1} = u \circ (p \circ (p \circ (u \circ u))) = u \circ (u \circ u) = u$. These properties hold for any symmetric quasigroup. What only remains to prove is the associativity: we have

$$(pq)r = u \circ (pq \circ r) = u \circ (r \circ pq) = u \circ (r \circ (u \circ (p \circ q))) = t_u t_r t_u t_p(q)$$

and

$$p(qr) = u \circ (p \circ qr) = u \circ (p \circ (u \circ (q \circ r))) = u \circ (p \circ (u \circ (r \circ q))) = t_u t_p t_u t_r(q)$$

We use now the hypothesis to conclude that the two expressions are the same, because $t_u t_r$ and $t_u t_p$ are elements of Γ^0 and hence commute.

ii ⇒ *iii* Suppose that $(S, \cdot)$ is our abelian group with unit element e and properties as in (*ii*). Fix $u \in S$. Define the following map:

$$\begin{array}{rccc} \psi_u : & S & \longrightarrow & S \\ & s & \longmapsto & u \cdot s \end{array}$$

This is clearly a bijection of S that sends e into u. It follows that ψ_u defines on S another abelian group law, with unit element u, that we will denote by $*$. Precisely we define

$$p * q := \psi_u \left(\psi_u^{-1}(p) \cdot \psi_u^{-1}(q) \right) = \psi_u(u^{-1} p u^{-1} q) = u^{-1} pq$$

where we write with p^{-1} the inverse of p with respect to the law $\cdot$. What we only need is to prove one of the equivalent conditions of lemma 2.5 for $*$, knowing that $\cdot$ has those properties. In this way we can conclude that also the group law $*$ has the desired properties.

We choose to prove the property (*c*) of lemma 2.5. We know by hypothesis that $\varphi_e : \Gamma^0 \to (S, \cdot)$ is a group isomorphism. We have to show that $\varphi_u : \Gamma^0 \to (S, *)$ is a group isomorphism too. Now $\psi_u : (S, \cdot) \to (S, *)$ is a group isomorphism, by definition of $*$ and because it is a translation. Hence the composition of group isomorphisms $\psi_u \circ \varphi_e : \Gamma^0 \to (S, *)$ is again a group isomorphism.fha We have only to prove now that

$$\varphi_u = \psi_u \circ \varphi_e$$

to conclude. Fix then an element $\gamma \in \Gamma^0$. We can write it as $\gamma = \tau_p$ for some $p \in S$, as in the proof of lemma 2.5. Hence we have that $\psi_u \circ \varphi_e(\tau_p) = u \cdot \tau_p(e) = u \cdot p = p \cdot u = e \circ (p \circ u) = t_e t_p(u) = \tau_p(u) = \varphi_u(\tau_p)$. This shows the identity we need to conclude.

iii $\Rightarrow$ *i* We have to show that Γ^0 is abelian. Using lemma 2.5, part (*c*), the groups Γ^0 and S are isomorphic once we have fixed an element in S. All of the group laws on S that we have obtained in this way are abelian, and hence also Γ^0 has to be it.

i $\Rightarrow$ *iv* Suppose that Γ^0 is abelian and recall that $t_p^2 = id$. Then we have:

$$(t_p t_q t_r)(t_p t_q t_r) = (t_p t_q)(t_r t_p)(t_q t_r) = (t_p t_q)(t_q t_r)(t_r t_p) = t_p t_p = id$$

iv $\Rightarrow$ *i* Our assumption is that $(t_p t_q t_r)^2 = id$, equivalently $(t_p t_q t_r)^{-1} = t_p t_q t_r$, i.e. $t_r t_q t_p = t_p t_q t_r$. We know by the proof of lemma 2.5 that $\Gamma^0 = \left\{ t_p t_q : p, q \in S \right\}$. Hence, to prove the abelianity of Γ^0, it is enough to prove the following: $(t_p t_q)(t_r t_s) = (t_r t_s)(t_p t_q)$ for any $p, q, r, s \in S$. This is equivalent to

$$(t_p t_q t_r t_s)(t_r t_s t_p t_q)^{-1} = id$$

Hence using the hypothesis $(t_p t_q t_r)^{-1} = t_p t_q t_r$, we get $(t_p t_q t_r t_s)(t_r t_s t_p t_q)^{-1} = (t_p t_q t_r t_s)(t_q t_p t_s t_r) = (t_p t_q t_r)^{-1}(t_s t_q t_p)^{-1} t_s t_r = t_r t_q (t_p t_p) t_q (t_s t_s) t_r = id$. This proves the commutativity of the multiplication on Γ^0.

□

2.2 Group law on cubic curves

We want now to give to the smooth K-rational points of an irreducible cubic curve the structure of an abelian symmetric quasigroup.

Let K be a field, $C \subset \mathbb{P}^2_K$ an absolutely irreducible plane cubic curve defined over K. Denote by $S \coloneqq C_{sm}(K) \subset C(K)$ the set of nonsingular K-points of C. Assume that this set is not empty. We define the *collinearity relation* $\mathfrak{L}$ in the following way:

$$(p, q, r) \in \mathfrak{L} \Leftrightarrow p + q + r \text{ is the intersection cycle of } C \text{ with a } K\text{-line}$$

We claim that $(S, \mathfrak{L})$ is an abelian symmetric quasigroup.

Proof. We start to prove that $(S, \mathfrak{L})$ is a symmetric quasigroup in the sense of definition 2.1: clearly any permutation of $(p, q, r) \in \mathfrak{L}$ stays in $\mathfrak{L}$, just because we can permute the terms of the intersection cycle $p + q + r$ without making any changes; furthermore, given $p, q \in S$, there exists only one $r \in S$ such that (p, q, r) belongs to $\mathfrak{L}$, because the intersection cycle of a cubic plane curve with a K-line gives exactly three points counted with multiplicity (Bezout theorem). We don't have any problem in the singular point because it has multiplicity 2, so any K-line passing through two (maybe equal) nonsingular points cannot pass through the singular one (by Bezout).

We have proved that $(S, \mathfrak{L})$ is a symmetric quasigroup. Hence it is defined a binary composition law $\circ$ on S through the formula $p \circ q = r \Leftrightarrow (p, q, r) \in \mathfrak{L}$. It remains to check that $(S, \circ)$ is also an abelian quasigroup.

By theorem 2.6, we can fix $u \in S$, and prove that the operation defined by $pq := u \circ (p \circ q)$ is a commutative group law. The commutativity, the existence of the unit element and of the inverse holds for any symmetric quasigroup, as showed in the first part of the proof of theorem 2.6. The only thing we need then to prove is the associativity: for any $p, q, r \in S$, it must hold $(pq)r = p(qr)$, or in other words $u \circ (pq \circ r) = u \circ (p \circ qr)$, equivalently $pq \circ r = p \circ qr$ (applying $u\circ$ to both sides).

Fix then p, q, r, any three points of S. We don't make any assumption on these points: some or all of them can be equal with each other or with u. Notice that, for any two points p_1, p_2 belonging to $S = C_{sm}(K)$, there is a unique K-line that passes through $p_1, p_2, p_1 \circ p_2$, even if $p_1 = p_2$. In this case, the line is the tangent line of C at p_1 (that has to be defined over K). Hence, we can define the cubic curve C_1 consisting of the following three lines: the line that passes through the points $p, q, p \circ q$, the line that passes through $u, q \circ r, qr$ and the line that passes through $r, pq, r \circ pq$. It is a reducible cubic curve defined over K. It can happen that some (or all) of the lines are the same, in which case we simply consider that line as a double (triple) line. Then C and C_1 determine a pencil of plane cubic curves: each cubic of this pencil passes through the nine points

$$p, q, p \circ q, u, q \circ r, qr, r, pq, r \circ pq$$

obtained intersecting C with C_1, and counted with multiplicity.

This means that the space of cubics obtained imposing the linear conditions of passage through those nine points contains, as a subspace, the space of the cubics belonging to our pencil. Now the dimension of the space of cubic forms is 9 (there are 10 coefficients in a cubic polynomial, but we can scale freely by an invertible element of K) and the dimension of the space of cubics in our pencil is clearly 1, hence there can be at most $8 = 9 - 1$ independent linear conditions on the cubics. We will indeed show that any cubic passing through eight of our points belong to the pencil of cubic, equivalently that the dimension of the two spaces are the same. Denote by d the dimension of the space of cubics obtained imposing the passage through eight of the nine points considered above. We know that $d \geq 1$. The effect of adding one linear condition to a space of cubics is to decrease its dimension by 1, but only if it is independent. We can then impose to our space of cubics passing through 8 points (we consider for instance $p, q, p \circ q, u, q \circ r, qr, r, pq$) to pass also in the point of intersection between the line that contains $p, q, p \circ q$ and the line that contains $u, q \circ r, qr$. By Bezout, any such cubic must contain all these two lines, and hence it must contain also another line, that is precisely the one passing through $r, pq, r \circ pq$. Hence this space consists only by one cubic (exactly C_1), and hence has dimension 0. This implies that we must have $d - 1 = 0$, and so $d = 1$.

Now that we have proved that any cubic that contains $p, q, p \circ q, u, q \circ r, qr, r$ belongs to our pencil of cubics. Consider then another reducible cubic, that we will call C_2, consisting of the following three K-lines: the line that passes through the points $q, r, q \circ r$, the line that passes through $u, p \circ q, pq$ and the line that passes through $p, qr, p \circ qr$. For what just done, it belongs to the pencil, and, due to the fact that any two cubics of the pencil intersect in the points $p, q, p \circ q, u, q \circ r, qr, r, r \circ pq$, while C and C_2 intersect in $p, q, p \circ q, u, q \circ r, qr, r, p \circ qr$,

then it has to be that $p \circ qr = r \circ pq$. This implies the associativity. □

This proves in particular that the choice of a smooth K-rational point transforms the cubic into an abelian quasigroup.

2.2.1 Cubic curves with a K-rational singular point

In what we will do in chapter 3 and 4, we are interested in the type of group that a singular cubic curve with K-rational singular point can assume.

Consider then an absolutely irreducible cubic curve, defined over a field K, in the Weierstrass model

$$C : zy^2 + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

with $a_i \in K$. Take $u := [0 : 1 : 0]$, the neutral element of our group law on $C_{sm}(K)$. Suppose that C is singular and that the (unique) singular point is defined over K (this is always true for fields of characteristic different from 2 and 3, and for perfect fields). It is easy to show that this point can never be u. Because the singular point has coordinates in K, we can move it in the origin of our plane, namely in $[0 : 0 : 1]$. We get the following equation for C:

$$zy^2 + bxyz + cx^2z = x^3$$

with $b := a_1, c := -a_2$.

The group structure varies with the kind of tangents that the singular point has.

Recall that we obtain the tangent cone at P moving this point in the origin of some system of affine equations, and then taking, from the affine equation, the terms of lowest degree.

In our situation, the notion of tangent cone at the singular point $p = [p_1, p_2, p_3]$ coincides by the notion of the polar at p defined by

$$\sum_{i=1}^{3} p_i \frac{\partial f}{\partial x_i}(x_1, x_2, x_3) = 0$$

where f is the equation of our cubic curve (or more generally of an hypersurface). See lemma 3.6 for the details.

In our case then, the tangent cone at the singular point $[0 : 0 : 1]$ satisfies the equation

$$y^2 + bxy + cx^2 = 0$$

It's not hard to see that, if we define s_1, s_2 as the two roots in $\bar{K}$ of the polynomial $t^2 + bx + c$, we have $y^2 + bxy + cx^2 = (y - s_1x)(y - s_2x)$, . Hence the splitting behaviour into lines of $y^2 + bxy + cx^2 = 0$ over K, depends exactly on what kind of roots $t^2 + bx + c$ has. Precisely the following cases can happen:

Definition 2.7. *1. C is of* multiplicative type*: $t^2 + at + b$ has two distinct solutions in K, the tangent cone consists of two distinct lines defined over K.*

2. *C is of* additive type*: $t^2 + at + b$ has one double root in K, the tangent cone consists of one double line defined over K.*

3. *C is of* twisted type*: $t^2 + at + b$ is irreducible over K. In particular:*

   3a) C is of twisted multiplicative type*: $t^2 + at + b$ has two distinct solutions in some quadratic extension of K but not in K. This means that the tangent cone consists of two distinct lines that are defined in some quadratic extension of K, but not in K.*

   3b) C is of twisted additive type*: $t^2 + at + b$ has one double solution in some quadratic extension of K but not in K. This means that the tangent cone consists of a double line that is defined in some quadratic extension of K, but not in K. This case can only happen in characteristic 2 (and furthermore the field has not to be perfect, in particular not finite).*

We will now specify some possibilities that can happen, concerning the above definition.

- If $\mathrm{char}(K) \neq 2$, we can obtain the solutions of $t^2 + at + b$ (in some quadratic extension of K) using the resolutive formula for quadratic equations:

$$t_{1,2} = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

  If there are two distinct solutions, and one of them is in K, then also the other belongs to K, because $\frac{\sqrt{\Delta}}{2} = t_1 - \frac{a}{2}$ belongs to K, where $\Delta = a^2 - 4b$.

  If instead we have a double root, then it has to be $t = -\frac{a}{2}$, and so it must live in K. This implies that in characteristic different from 2 the twisted additive case cannot happen.

- If $\mathrm{char}(K) = 2$, the polynomial $t^2 + at + b$ has two distinct roots (in its splitting field over K) if and only if $a \neq 0$.

  Indeed, let $\bar{t}$ a root of $t^2 + at + b$. Then $\bar{t} + a$ is the other solution of the polynomial:

$$(t + \bar{t})(t + \bar{t} + a) = (t + \bar{t})^2 + a(t + \bar{t}) = t^2 + \bar{t}^2 + at + a\bar{t} = t^2 + at + b$$

  The two solutions are distinct if and only if $a \neq 0$. Furthermore, they belong to the same quadratic extension of K.

The following theorem is the main result of this section.

Theorem 2.8 (group structures on $C_{sm}(K)$)**.** *Let C be an irreducible singular cubic curve, defined over a field K. Assume that the singular point of C is defined over K. Denote as usual by Γ^0 the abelian group associated with the symmetric quasigroup $C_{sm}(K)$.*

1. *If C is of multiplicative type, Γ^0 is isomorphic to $K^\times$.*
2. *If C is of additive type, Γ^0 is isomorphic to K^+.*
3. *If C is of twisted multiplicative type, Γ^0 is isomorphic to the group of elements of norm 1 of some quadratic extension of K (it is a subgroup of the multiplicative group of that extension).*
4. *If C is of twisted additive type (that implies $\mathrm{char}(K) = 2$), Γ^0 is isomorphic to*

$$\left\{(\alpha, \beta) \in K^2 : \alpha^2 = \beta + b\beta^2\right\}.$$

Proof. Recall that we have seen that we have a group isomorphism of $\Gamma^0 \to C_{sm}(K)$ once we have fixed an element u (and hence a group law) on $C_{sm}(K)$.

We start then from a cubic curve C of equation $x^3 = (y^2 + axy + bx^2)z$: it has the singular point in the origin $[0 : 0 : 1]$, and also only the point $u = [0 : 1 : 0]$ lies on the line at infinity $z = 0$ (observe that this u is a flex point: $u = u \circ u$, because $z = 0$ is its tangent).

First, we define the following map:

$$\begin{array}{rcl} \mathbb{P}^1(K)\setminus\{[1:\bar{m}] : \bar{m}^2 + a\bar{m} + b = 0\} & \longrightarrow & C_{sm}(K) \\ [\lambda : m] & \longmapsto & [(m^2 + am\lambda + b\lambda^2)\lambda :\ (m^2 + am\lambda + b\lambda^2)m :\ \lambda^3] \end{array}$$

This correspondence is obtained intersecting the smooth points $C_{sm}(K)$ of our cubic curve, with the pencil of projective lines over K through the singular point, namely the lines $\lambda y = mx$, with $\lambda, m \in K$ not both zero. Each line (except the tangents at the singular points) determines exactly one point on $C_{sm}(K)$, using Bezout's theorem. We obtain then the above correspondence between the set of projective lines through the origin (written as points of a $\mathbb{P}^1(K)$), with the smooth points of the cubic.

By this observation, it is then clear that the inverse of this map has to be:

$$\begin{array}{rcl} C_{sm}(K) & \longrightarrow & \mathbb{P}^1(K)\setminus\{[1:\bar{m}] : \bar{m}^2 + a\bar{m} + b = 0\} \\ [x : y : z] & \longmapsto & [x : y] \end{array}$$

We will now formally show that the two maps are bijections, one the inverse of the other. Indeed,

$$[x : y : z] \longmapsto [x : y] \longmapsto \left[(y^2 + axy + bx^2)x :\ (y^2 + axy + bx^2)y :\ x^3\right] =$$

$$= \left[(y^2 + axy + bx^2)x :\ (y^2 + axy + bx^2)y :\ (y^2 + axy + bx^2)z\right] = [x : y : z]$$

and

$$[\lambda : m] \longmapsto \left[(m^2 + am\lambda + b\lambda^2)\lambda :\ (m^2 + am\lambda + b\lambda^2)m :\ \lambda^3\right] \longmapsto$$

$$\longmapsto \left[(m^2 + am\lambda + b\lambda^2)\lambda :\ (m^2 + am\lambda + b\lambda^2)m\right] = [\lambda : m]$$

We have obtained a well defined bijection from $C_{sm}(K)$ to $\mathbb{P}^1(K)\setminus\{[1:\bar{m}] : \bar{m}^2 + a\bar{m} + b = 0\}$.

Observation. In the particular case of $K = \mathbb{F}_q$ finite field, from this map, we directly obtain the number of K-rational smooth points of our singular cubic curve:

- if C is of multiplicative type, we get

$$\#(C_{sm}(K)) = \#(\mathbb{P}^1(K)) - \#\Big(\{[1:\bar{m}] : \bar{m}^2 + a\bar{m} + b = 0\}\Big) = (q+1) - 2 = q - 1$$

- if C is of additive type, we get

$$\#(C_{sm}(K)) = \#(\mathbb{P}^1(K)) - \#\Big(\{[1:\bar{m}] : \bar{m}^2 + a\bar{m} + b = 0\}\Big) = (q+1) - 1 = q$$

- if C is of twisted type, we get

$$\#(C_{sm}(K)) = \#(\mathbb{P}^1(K)) - \#\Big(\{[1:\bar{m}] : \bar{m}^2 + a\bar{m} + b = 0\}\Big) = (q+1) - 0 = q + 1$$

Now we will see what happens in each case.

1. Suppose C of multiplicative type: then there are $s_1, s_2 \in K$ two distinct zeroes of the equation $t^2 + at + b = 0$. Notice that $[1 : s_1]$, $[1 : s_2]$ represent the inclinations of the two tangents at the singular point. With these assumptions, we can write the equation of C as
$$x^3 = (y - s_1 x)(y - s_2 x)z$$
We have already seen that we have a bijection between $C_{sm}(K)$ and $\mathbb{P}^1 \setminus \{[1 : s_1], [1 : s_2]\}$. To define a (group) isomorphism between $C_{sm}(K)$ and $K^\times$, we continue defining another map:
$$\begin{array}{rcl} \mathbb{P}^1 \setminus \{[1:s_1],[1:s_2]\} & \longrightarrow & K^\times \\ [\lambda : m] & \longmapsto & \frac{m - s_1\lambda}{m - s_2\lambda} \end{array}$$
The meaning of this is, sort of speaking, to move one of the problematic tangent to infinity, and the other to 0. This map is clearly a bijection (it comes from a projectivity).
It remains only to prove that the composition of the two maps
$$\begin{array}{rccl} \psi : & C_{sm}(K) & \longrightarrow & K^\times \\ & [x:y:z] & \longmapsto & \frac{y - s_1 x}{y - s_2 x} \end{array}$$
is now a group isomorphism. Recall that the unit element of the group law over $C_{sm}(K)$ is $u = [0 : 1 : 0]$. Writing the group law additively, and using the fact that $u = u \circ u$ and $-p := (u \circ u) \circ p = u \circ p$, then by definition $p + q := u \circ (p \circ q) = -(p \circ q)$. So the definition of the group law becomes equivalent to
$$p + q + (p \circ q) = u$$

Hence, to prove that ψ is a group homomorphism, it is enough to prove that $\psi(p)\psi(q)\psi(p \circ q) = \psi(u)$, for any $p, q \in C_{sm}(K)$.

Observe that $\psi(u) = \psi([0:1:0]) = 1$. It is then sufficient to show that, fixed any line not containing the singular point, and called p, q, r the three points of intersection of it with the cubic curve, we have always that

$$\psi(p)\psi(q)\psi(r) = 1$$

To do that, we can change the variables $y \mapsto y - s_2 x$. This gives in the new variables the equation of the cubic

$$x^3 = (y - sx)yz$$

where $s \coloneqq s_1 - s_2 \neq 0$, and now

$$\psi([x:y:z]) = \frac{y - sx}{y}$$

Furthermore the coordinates of the singular point and of the point at infinity are not changed. Now we don't have nonsingular points on the line $y = 0$, so we can pass to the affine coordinate system obtained sending that line to infinity: we get that the lines $z = \alpha x + \beta$, with $\beta \neq 0$, are all the lines that intersect the cubic curve but that do not contain the singular point. The affine equation of the curve has now become $x^3 = (1 - sx)z$ and $\psi([x:1:z]) = 1 - sx$.

We want to show that, for the three points of intersection of the line $z = \alpha x + \beta$ with the cubic curve, that are $p_i = [x_i : 1 : \alpha x_i + \beta]$ such that $x_i^3 = (1 - sx_i)(\alpha x_i + \beta)$ $(i = 1, 2, 3)$, we have that

$$\psi(p_1)\psi(p_2)\psi(p_3) = 1$$

equivalently

$$(1 - sx_1)(1 - sx_2)(1 - sx_3) = 1$$

Observing that the x_i are solution of $x^3 = (1 - sx)(\alpha x + \beta) = -s\alpha x^2 + (\alpha - s\beta)x + \beta$, then

$$x_1x_2x_3 = \beta \qquad x_1x_2 + x_1x_3 + x_2x_3 = s\alpha - \beta \qquad x_1 + x_2 + x_3 = -s\alpha$$

We get

$$(1 - sx_1)(1 - sx_2)(1 - sx_3) = 1 - s(x_1 + x_2 + x_3) + s^2(x_1x_2 + x_1x_3 + x_2x_3) - s^3x_1x_2x_3 =$$

$$= 1 - s(-s\alpha) + s^2(s\beta - \alpha) - s^3\beta = 1 + s^2(\alpha - \alpha) + s^3(\beta - \beta) = 1$$

as wanted.

We have proved that ψ is a group isomorphism between $C_{sm}(K)$ and $K^\times$.

2. Suppose C of additive type: then there exists $s \in K$ the unique zero of the equation $t^2 + at + b = 0$. Notice that $[1 : s]$ represents the inclination of the double tangent at the cusp. With these assumptions, we can write the equation of C as

$$x^3 = (y - sx)^2$$

We have already seen that we have a bijection between $C_{sm}(K)$ and $\mathbb{P}^1 \setminus \{[1 : s]\}$. To define a (group) isomorphism between $C_{sm}(K)$ and K^+, we continue defining another map:

$$\begin{array}{rcl} \mathbb{P}^1 \setminus \{[1 : s]\} & \longrightarrow & K^+ \\ [\lambda : m] & \longmapsto & \frac{\lambda}{m - s\lambda} \end{array}$$

Sort of speaking, we have moved the inclination of the tangent to infinity. This map is clearly a bijection (it comes from a projectivity).

It remains only to prove that the composition of the two maps

$$\begin{array}{rccc} \varphi : & C_{sm}(K) & \longrightarrow & K^+ \\ & [x : y : z] & \longmapsto & \frac{x}{y - sx} \end{array}$$

is now a group isomorphism. As before, it is enough to prove that $\varphi(p) + \varphi(q) + \varphi(p \circ q) = \varphi(u)$, for any $p, q \in C_{sm}(K)$. Observe that now $\varphi(u) = \varphi([0 : 1 : 0]) = 0$. So it is sufficient to show that, fixed any line not containing the singular point, if we call p, q, r the three points of intersection of it with the cubic curve, we have

$$\varphi(p) + \varphi(q) + \varphi(r) = 0$$

To do that, we can change the variables as $y \mapsto y - sx$. This gives, in the new variables, the equation of the cubic curve

$$x^3 = y^2 z$$

and now

$$\varphi([x : y : z]) = \frac{x}{y}$$

Furthermore the coordinates of the singular point and of the point at infinity are not changed. Now we don't have smooth points on the line $y = 0$, so we can pass to the affine coordinate system obtained sending that line at infinity: we get that the lines $z = \alpha x + \beta$, with $\beta \neq 0$, are all the lines that intersect the cubic curve but that do not contain the singular point. The affine equation of the curve has now become $x^3 = z$ and $\varphi([x : 1 : z]) = x$.

We want to show that, for the three points of intersection of the line $z = \alpha x + \beta$ with the cubic curve, that precisely are $p_i = [x_i : 1 : \alpha x_i + \beta]$ such that $x_i^3 = (1 - sx_i)(\alpha x_i + \beta)$ $(i = 1, 2, 3)$, we have that

$$x_1 + x_2 + x_3 = 0$$

This follows because $x^3 = (\alpha x + \beta)$ has no term of second degree.

We have proved that φ is a group isomorphism between $C_{sm}(K)$ and K^+.

3. Suppose C of twisted multiplicative type: there are no solutions in K of $t^2 + at + b = 0$, but there are two distinct solution s_1, s_2 in some quadratic extension of K.

   Define $L := K(s_1, s_2) = K(s_1)$, the quadratic extension of K that is also the splitting field of our polynomial. Over L our cubic curve is of multiplicative type, hence we can use the point 1., to get an isomorphism $\psi : C_{sm}(L) \cong L^\times$. This implies that $C_{sm}(K) \cong \psi(C_{sm}(K)) \subseteq L^\times$. We will now see that

   $$\psi(C_{sm}(K)) = \{l \in L^\times : N_{L/K}(l) = 1\}$$

   where $N_{L/K}$ indicates the Galois norm of L over K.

   One side of the inclusion is easy:

   $$N_{L/K}(\psi([x : y : z])) = N_{L/K}\left(\frac{y - s_1 x}{y - s_2 x}\right) = \frac{y - s_1 x}{y - s_2 x} \cdot \sigma\left(\frac{y - s_1 x}{y - s_2 x}\right) = \frac{y - s_1 x}{y - s_2 x}\frac{y - s_2 x}{y - s_1 x} = 1$$

   where σ is the K-automorphism of L that exchanges s_1 and s_2.

   Viceversa, notice that the inverse of the map ψ is the map

   $$\begin{array}{rccl} \psi^{-1}\colon & L^\times & \longrightarrow & C_{sm}(L) \\ & u & \longmapsto & [(s_1 - s_2)^2 u(1-u) : (s_1 - s_2)^2 u(s_1 - s_2 u) : (1-u)^3] \end{array}$$

   If $u = 1$, then $\psi^{-1}(1) = [0 : 1 : 0]$. If not, we can write

   $$\psi^{-1}(u) = \left[(s_1 - s_2)^2 \frac{u}{(1-u)^2} : (s_1 - s_2)^2 \frac{u}{(1-s)^2}\frac{s_1 - s_2 u}{1-u} : 1\right]$$

   Take then u an element of $L^\times$ of norm 1, precisely $u = a + bs_1 \in L^\times = K(s_1)^\times$ is such that $N_{L/K}(u) = u \cdot \sigma(u) = 1$. First, observe that $(s_1 - s_2)^2 = a^2 - 4b \in K$. Secondly, we have

   $$\frac{u}{(1-u)^2} = \frac{u}{1 - 2u + u^2} = \frac{u}{u\sigma(u) - 2u + u^2} = \frac{1}{\sigma(u) + u - 2} \in K$$

   because $u + \sigma(u) = \mathrm{Trace}_{L/K}(u) \in K$. Finally,

   $$\frac{s_1 - s_2 u}{1-u} = \frac{(s_1 - s_2 u)(1 - \sigma(u)}{(1-u)(1-\sigma(u)} = \frac{s_1 - s_2 u - s_1\sigma(u) + s_2 u\sigma(u)}{N(1-u)} =$$

   $$= \frac{s_1 + s_2 - (s_2 u) - (\sigma(s_2 u)}{N(1-u)} = \frac{-b - \mathrm{Trace}(s_2 u)}{N(1-u)} \in K$$

   Hence $\psi^{-1}(u) \in C_{sm}(K)$ for $u \in L^\times$ of norm 1, and we have proved that:

   $$C_{sm}(K) \cong \{l \in L^\times : N_{L/K}(l) = 1\} \subset L^\times$$

4. Suppose C of twisted additive type: the characteristic of K has to be 2, our polynomial has to be $t^2 + b = 0$ and is irreducible over K. It has a unique solution s in some quadratic extension of K. Precisely $s \notin K$ is such that $s^2 = b$.

   Define then $L := K(s)$.

   Over L our cubic curve is of additive type: we can then use the point 2., to get an isomorphism $\varphi : C_{sm}(L) \cong L^+$. This implies that $C_{sm}(K) \cong \varphi(C_{sm}(K)) \subseteq L^+$. We will now see that

$$\varphi(C_{sm}(K)) = \left\{ l = \alpha + \beta s \in L : \alpha^2 = \beta + b\beta^2 \right\}$$

   One side of the inclusion is easy: consider $[x : y : z] \in C_{sm}(K)$; we have

$$\varphi([x : y : z] = \frac{x}{y + sx} = \frac{x(y + sx)}{y^2 + bx^2} = \frac{xy}{y^2 + bx^2} + s\frac{x^2}{y^2 + bx^2}$$

   We can define $\alpha := \frac{xy}{y^2+bx^2}$ and $\beta := \frac{x^2}{y^2+bx^2}$. If we write $\gamma := \frac{x}{y+sx}$, we have that $\frac{y}{y+sx} = 1+s\gamma$ and we get

$$\alpha = \gamma(1 + s\gamma) \quad \text{and} \quad \beta = \gamma^2$$

   We obtain

$$\alpha^2 + \beta + b\beta^2 = \gamma^2 + b\gamma^4 + \gamma^2 + b\gamma^4 = 0$$

   what we want.

   For the converse, it is easy to check that the inverse of φ is the following map:

$$\begin{array}{ccc} L^+ & \longrightarrow & C_{sm}(L) \\ u & \longmapsto & [u : 1 + su : u^3] \end{array}$$

   Suppose $u = \alpha + s\beta$, with $\alpha, \beta \in K$, and $\alpha^2 + b\beta^2 = (\alpha + s\beta)^2 = \beta$. Then

$$\varphi^{-1}(u) = \varphi^{-1}(\alpha + s\beta) = [\alpha + s\beta : 1 + s(\alpha + s\beta) : (\alpha + s\beta)^3] =$$

$$= \left[1 : \frac{\alpha + s\beta + s(\alpha + s\beta)^2}{(\alpha + s\beta)(\alpha + s\beta)} : (\alpha + s\beta)^2\right] = \left[1 : \frac{\alpha}{\beta} : \beta\right] \in C_{sm}(K)$$

   as wanted.

□

3 Geometric Reconstruction of Cubic Surfaces

In the first part of this chapter, we will see a procedure to reconstruct a projective line, with its ground field K. We pass then to analyze the geometric reconstruction of a cubic surface. To do this we will need a (C_m, C_a)-configuration. We will explain precisely, in section 3.2, what this configuration is, but mainly it consists of two K-rational points of a cubic surface with their respective tangent plane sections, one of multiplicative type and the other one of additive type. The existence of this configuration allows us to reconstruct the field K (using a particular projective line). At the same time, if we have also two other K-rational points with respective tangent plane sections of additive or multiplicative type (i.e. in total a tetrahedral configuration), we can reconstruct uniquely our cubic surface, up to linear transformation.

3.1 Geometric reconstruction of a projective line

In this section, we will start from a geometric projective line. In the first construction, we will get from it the combinatorial data that we will need for the reconstruction. Then we will show explicitly how we can reconstruct our projective line starting from these combinatorial constraints.

Definition 3.1 (Geometric Projective Lines)**.** *Let K be a field with cardinality ≥ 4. Define $H := \mathbb{P}^1(K)$, that hence must contain at least 5 points. Choose five distinct points*

$$0_a, \infty_a, 0_m, 1_m, \infty_m \in \mathbb{P}^1(K)$$

We will call the data $\left(K, \mathbb{P}^1(K), \{0_a, \infty_a, 0_m, 1_m, \infty_m\}\right)$ a geometric projective line.

We will get now the combinatorial data we will need.

Construction 1. We can give to the set $A := H\backslash\{\infty_a\}$ a structure of abelian group. It is enough to choose an affine coordinate x_a on $\mathbb{P}^1(K)$ such that it has zero in 0_a and infinite in ∞_a. Precisely, we have a coordinate:

$$\begin{array}{rccc} x_a\colon & A \cup \{\infty_a\} & \longrightarrow & K \cup \{\infty\} \\ & 0_a & \longmapsto & 0 \\ & \infty_a & \longmapsto & \infty \end{array}$$

Such a map is fixed, once we fix the point of A that is sent to 1 in K. This point has to be different from 0_a and ∞_a. Using this coordinate, we define an additive group law on A transporting the addition on K^+. Namely, for any two points $p, q \in A$, we define

$$p +_A q := x_a^{-1}\left(x_a(p) + x_a(q)\right)$$

where here + is the addition in K. Furthermore, we will extend the group law of A on a partial law on $A \cup \{\infty_a\}$, setting for any $q \in A$

$$q \pm_A \infty_a := \infty_a$$

Similarly we can give to the set $M := H\backslash\{0_m, \infty_m\}$ a structure of abelian group. It is enough to choose an affine coordinate x_m on $\mathbb{P}^1(K)$ such that it has zero in 0_m, infinite in ∞_m and one in 1_m. Precisely, we have a unique such coordinate:

$$\begin{array}{rccc} x_m\colon & M \cup \{0_m, \infty_m\} & \longrightarrow & K^\times \cup \{0, \infty\} \\ & 0_m & \longmapsto & 0 \\ & \infty_m & \longmapsto & \infty \\ & 1_m & \longmapsto & 1 \end{array}$$

Using this coordinate, we define a multiplicative group law on M transporting the multiplication on $K^\times$. Namely, for any two points $p, q \in M$, we define

$$p \cdot_M q := x_m^{-1}\left(x_m(p) \cdot x_m(q)\right)$$

where here $\cdot$ is the multiplication in $K^\times$. Furthermore we will extend the group law of M to a partial law on $M \cup \{0_m, \infty_m\}$ setting for any $p \in M$

$$p \cdot_M 0_m := 0_m, \quad p \cdot_M \infty_m := \infty_m, \quad i_M(0_m) := \infty_m, \quad i_M(\infty_m) := 0_m$$

where we denote with i_M the inversion on $(M, \cdot_M)$.

Finally we have a well defined bijection

$$\mu\colon \quad M \cup \{0_m, \infty_m\} \quad \longrightarrow \quad A \cup \{\infty_a\}$$

that we can simply suppose to be the identity map $\mu = id$ on $H = \mathbb{P}^1(K)$.

Observation. To a geometric projective line $\left(K, \mathbb{P}^1(K), \{0_a, \infty_a, 0_m, 1_m, \infty_m\}\right)$ are always attached in a unique way the coordinate $x_m\colon M \cup \{0_m, \infty_m\} \to K \cup \{\infty\}$ and a class of coordinates $x_a\colon A \cup \{\infty_a\} \to K \cup \{\infty\}$ that varies up to which point is sent into 1. It is enough to act as in the construction above.

Observation. Given any bijection μ as above, it is always possible to reconduct ourselves to the case where μ becomes the identity, in the sense that, if this is not the case, we can suitably change the coordinate on M to reconduct ourselves in the desired situation.

To do this we will proceed in the following way: we start from the two abelian groups $(M, \cdot_M)$ and $(A, +_A)$, and we have also a bijection $\mu\colon M \cup \{0_m, \infty_m\} \to A \cup \{\infty_a\}$. We define the set $M' := \mu(M)$ and the points $0'_m := \mu(0_m)$ and $\infty'_m := \mu(\infty_m)$. It then holds that $M' \cup \{0'_m, \infty'_m\} = A \cup \{\infty_a\}$. We will put on M' the multiplication induced by M: namely, for any $p', q' \in M'$, we define $p' \cdot_{M'} q' := \mu\left(\mu^{-1}(p') \cdot_M \mu^{-1}(q')\right)$. This is equivalent to give to M' the multiplication induced by $K^\times$ using the affine coordinate $x'_m := x_m \circ \mu^{-1}$. Indeed by definition $p' \cdot_{M'} q' = \mu \circ x_m^{-1}\left(x_m \circ \mu^{-1}(p') \cdot x_m \circ \mu^{-1}(q')\right) = x_m'^{-1}\left(x'_m(p') \cdot x'_m(q')\right)$. Hence we have the following commutative diagram:

$$\begin{array}{ccccc} M \cup \{0_m, \infty_m\} & \xrightarrow{\mu} & M' \cup \{0'_m, \infty'_m\} & \xrightarrow{id} & A \cup \{\infty_a\} \\ & {\scriptstyle x_m}\searrow & \downarrow {\scriptstyle x'_m} & & \downarrow {\scriptstyle x_a} \\ & & K \cup \{\infty\} & & K \cup \{\infty\} \end{array}$$

Hence we can always assume that μ is the identity, with a suitable change of coordinate.

We will now state the lemma that sums up the procedure of reconstructing our projective line, together with the field of definition K.

Lemma 3.2 (Reconstruction of Projective Lines)**.** *Consider the data* $(M, A, \mu, \{0_a, \infty_a, 0_m, 1_m, \infty_m\})$ *that are obtained from a geometric projective line* $H = \mathbb{P}^1(K)$ *as in construction* 1*. Here* $\mu = id$*. We can define a map*

$$\nu \colon M \cup \{0_m, \infty_m\} \longrightarrow A \cup \{\infty_a\}$$

as follows:

1. *Define* $\nu_0 := id$*.*
2. *Fix* $\zeta \in A\backslash\{0_a, 0_m -_A \infty_m\}$*. Then for* $p \in M \cup \{0_m, \infty_m\}$*, we define*

$$\nu_1(p) := \infty_a \cdot_M i_M(\infty_m -_A \zeta) \cdot_M (p -_A \zeta)$$

   Now we have that $\nu_1(\infty_m) = \infty_a$*.*
3. *For* $p \in M \cup \{0_m, \infty_m\}$*, define*

$$\nu_2(p) := \nu_1(p) -_A \nu_1(0_m)$$

   Now we still have that $\nu_2(\infty_m) = \infty_a$ *and furthermore* $\nu_2(0_m) = 0_a$*.*
4. *For* $p \in M \cup \{0_m, \infty_m\}$*, define*

$$\nu(p) = \nu_3(p) := \nu_2(\nu_2^{-1}(1_a) \cdot_M p)$$

   where 1_a *is an element of* $A\backslash\{0_a\}$ *and precisely, for any* $q \in A \cup \{\infty_a\}$*,* $\nu_2^{-1}(q) = (q +_A \nu_1(0_m)) \cdot_M (\infty_m -_M \zeta) \cdot_M i_M(\infty_a) +_A \zeta$*.*

Then ν *is a well defined bijection, and it is such that*

$$\nu(0_m) = 0_a \qquad \text{and} \qquad \nu(\infty_m) = \infty_a$$

Using this bijection ν*,* $(M, \cdot_M)$ *induces on the set* $A\backslash\{0_a\}$ *the structure of a multiplicative abelian group: by definition we put*

$$p *_M q := \nu(\nu^p \cdot_M \nu^q)$$

for any $p, q \in A$*. We obtain then that* $A = H\backslash\{\infty\}$*, where* $\infty := \nu(\infty_m) = \infty_a$ *is a field, with zero* $0 := \nu(0_m) = 0_a$ *and unity* $1 := \nu(1_m)$*.*

Furthermore $H\backslash\{\infty\} \cong K$ *as fields through* x_a *(restricted to A). We get then our line back:*

$$\mathbb{P}^1(H\backslash\{\infty\}) \cong \mathbb{P}^1(K).$$

Proof. Observe that ν is always a well defined bijection, because it is the composition of translations by elements of M with the product $\cdot_M$, and of translations by elements of A using the sum $+_A$ (here we use the assumptions over ζ, to exclude the case of translations by improper elements, that are the constant map and hence not bijective).

In the geometric case we are considering, we can consider the fractional linear transformation, automorphisms of $K \cup \{\infty\}$, defined by the formula

$$f_i := x_a \circ \nu_i \circ x_m^{-1}$$

for each i we have considered.

Hence, for each i, we have the following commutative diagram:

$$\begin{array}{ccc} M \cup \{0_m, \infty_m\} & \xrightarrow{\nu_i} & A \cup \{\infty_a\} \\ x_m \downarrow & & \downarrow x_a \\ K \cup \{\infty\} & \xrightarrow{f_i} & K \cup \{\infty\} \end{array}$$

Now f_0 is a fractional linear transformation with no specific properties; f_1 sends ∞ to ∞, hence it has the form $x \mapsto ax + b$ for some $a, b \in K, a \neq 0$; f_2 sends ∞ to ∞ and 0 to 0, hence it has the form $x \mapsto ax$ for some $a \in K^\times$; finally f_3 sends ∞ to ∞, 0 to 0 and 1 to 1, hence f_3 is the identity on $K \cup \{\infty\}$. All these facts follow from the definition of f_i and from the properties of v_i: for example, $f_1(\infty) = f_1(x_m(\infty_m)) = x_a \circ \nu_1(\infty_m) = x_a(\infty_a) = \infty$.

Now $f_3 = x_a \circ \nu \circ x_m^{-1}$, hence we have that our ν is indeed the change of coordinates:

$$\nu = x_a^{-1} \circ x_m$$

We define on $(A, +_A)$ the multiplication $*_M$ induced by M through ν: by definition we have

$$p *_M q := \nu\left(\nu^{-1} \cdot_M \nu^{-1}\right)$$

for any $p, q \in A$. The coordinate x_a already defined induces a group isomorphism from $(A, +_A)$ to K^+, by definition of $+_A$. We will prove that it is also a field isomorphism from $(A, +_a, *_m)$ to K. Indeed, fix $p, q \in A$. We get, recalling also the definition of $\cdot_M$,

$$x_a(p *_M q) = x_a \circ \nu(\nu^{-1}(p) \cdot_M \nu^{-1}(q)) = x_a \circ \nu \circ x_m^{-1}\left(x_m \circ \nu^{-1}(p) \cdot x_m \circ \nu^{-1}(q)\right) = x_a(p) \cdot x_a(q)$$

We have proved that $(A, +_a, *_M)$ is a field isomorphic to the field K. □

Observation. We can rephrase lemma 3.2 in the case that $\mu \neq id$. What we only have to do is substituting $(M, \cdot_M)$ with $(M', \cdot_{M'})$, the respective points and the respective coordinate, as observed before the lemma, and in each step considering $\nu_i \circ \mu$ instead of ν_i only. Precisely:

1. $\nu_0 := \mu$.
2. Fixed $\zeta \in A \backslash \{0_a, \mu(0_m) -_A \mu(\infty_m)\}$, for $p \in M \cup \{0_m, \infty_m\}$,

$$\nu_1(p) := \mu\left(\mu^{-1}(\infty_a) \cdot_M i_M(\mu^{-1}(\mu(\infty_m) -_A \zeta)) \cdot_M \mu^{-1}(\mu(p) -_A \zeta)\right)$$

3. For $p \in M \cup \{0_m, \infty_m\}$, define

$$\nu_2(p) \coloneqq \nu_1(p) -_A \nu_1(\mu(0_m))$$

4. For $p \in M \cup \{0_m, \infty_m\}$, define

$$\nu(p) = \nu_3(p) \coloneqq \nu_2(\nu_2^{-1}(1_a) \cdot_M p)$$

where 1_a is an element of $A \backslash \{0_a\}$ and precisely, for any $q \in A \cup \{\infty_a\}$, we have $\nu_2^{-1}(q) = \mu^{-1}\left(\mu\left(\mu^{-1}(q +_A \nu_1(0_m)) \cdot_M \mu^{-1}(\mu(\infty_m) -_A \zeta) \cdot_M i_M(\mu^{-1}(\infty_a))\right) +_A \zeta\right)$.

Notice also that the f_is are not changed: what does change is the coordinate x_m instead.

$$\begin{array}{ccccc} M \cup \{0_m, \infty_m\} & \xrightarrow{\mu} & M' \cup \{0'_m, \infty'_m\} & \xrightarrow{\nu_i} & A \cup \{\infty_a\} \\ & {\scriptstyle x_m}\searrow & \downarrow x'_m & & \downarrow x_a \\ & & K \cup \{\infty\} & \xrightarrow{f_i} & K \cup \{infty\} \end{array}$$

So it is still true that the f_is remains fractional linear transformations.

3.2 (C_m, C_a)-configurations

We will now define the main tool for the reconstruction of cubic surfaces.

Definition 3.3. *We call a* (C_m, C_a)-configuration *the following family of subschemes in* $\mathbb{P}^3_K$*:*

- *Two distinct K-points* $p_m, p_a \in \mathbb{P}^3(K)$*;*
- *Two distinct K-planes* $P_m, P_a \subset \mathbb{P}^3$ *such that* P_m *contains* p_m *but not* p_a*, and* P_a *contains* p_a *but not* p_m*;*
- *Two geometrically irreducible cubic curves* C_m, C_a*, defined over K, and such that:*
  1. $C_m \subset P_m$ *is of multiplicative type with* $p_m \in C_m(K)$ *as its singular double point (its node);*
  2. $C_a \subset P_a$ *is of additive type with* $p_a \in C_a(K)$ *as its singular double point (its cusp);*

Furthermore we will call:

- $l \coloneqq P_m \cap P_a$ *the intersection line of our two planes;*
- $0_m, \infty_m$ *the intersection points of the two tangents to* C_m *at* p_m *with the line l;*
- ∞_a *the intersection point of the tangent to* C_a *at* p_a *with the line l.*

We will assume that the three points $0_m, \infty_m, \infty_a$ *are distinct.*

Definition 3.4. *A (C_m, C_a)-configuration is* tangent *to some (irreducible) cubic surface V if we add the assumptions that:*

- *P_m is the tangent plane to the surface at p_m, and C_m is the cubic curve obtained intersecting P_m and V;*
- *P_a is the tangent plane to V at p_a, and C_a is the cubic curve obtained intersecting P_a and V.*

3.2.1 (C_m, C_a)-configurations from cubic surfaces

We will analyze now which points of a cubic surface $V = Z(F)$ are of multiplicative type and which are of additive type. For a nonsingular K-point $p = (p_1, ..., p_4)$ in $V(K)$, we would like to define a quantity $\Delta(p)$ that stores the information about the tangents at p as a singular point on its tangent section. To do this we start defining the following geometric object.

Definition 3.5. *Consider a smooth point $p = (p_1, ..., p_4)$ in $V(K)$. We start defining a quadratic surface, called the* polar *at p, with the following equation:*

$$\mathfrak{P}_p(x_1, ..., x_4) : \sum_{i=1}^{4} p_i \frac{\partial}{\partial x_i} F(x_1, ..., x_4) = 0$$

Observe that a point $q = (q_1, ..., q_4)$ belongs to $\mathfrak{P}_p$ if and only if $\sum_{i=1}^{4} \frac{\partial}{\partial x_i} F(q_1, ..., q_4) p_i = 0$, that means that p belongs to the tangent plane at q. Furthermore all the singular point of the cubic surface belong to $\mathfrak{P}_p$ for any p.

We will need the following two lemmas:

Lemma 3.6. *Let S be a singular cubic hypersurface with an isolated singularity in the point P. Then the polar at P and the tangent cone at P have the same equation.*

Proof. We will do this for simplicity for plane cubic curves. Let F a form of degree three that defines a cubic curve C. We can suppose that it has singular point in the origin $[0 : 0 : 1]$. Hence C has equation $k_1x^3 + k_2x^3 + z^2(\lambda x + \mu y) + z(ax^2 + by^2)$. Furthermore $\lambda = \mu = 0$ because $\frac{\partial F}{\partial x}|_P = \frac{\partial F}{\partial y}|_P = 0$. Hence in affine coordinates $F = ax^2 + by^2 + k_1x^3 + k_2y^3$, so the tangent cone at P is, by definition, $ax^2 + by^2 = 0$, the same equation for the polar at $P = [0 : 0 : 1]$.

Notice that, for a generic hypersurface of degree three, we act exactly in the same way: we pass to affine coordinate with the singular point in the origin, the term of degree 2 in the variable z disappears imposing that the (other) partial derivatives are zero in the singular point, hence the tangent cone at P and the polar at P will have the same equation. □

Lemma 3.7. *An irreducible quadric is singular (degenerate) if and only if one (and then all) of its points has tangent section consisting of a double line.*

Proof. Suppose we have an irreducible quadric with singular point s. We can assume that the singular point has coordinates $[0:0:0:1]$, and that there is another point p with coordinates $[0:0:1:0]$, so the equation of the quadric has the shape $\alpha x^2 + \beta y^2 + axy + bxz + cyz$. The tangent plane at p is then $\beta x + \gamma y = 0$, so if we intersect it with the quadric we get the double line $x^2 = 0$ on that plane (or the whole plane, which we have supposed that is not possible).

Viceversa, consider a point p of the quadric. We can suppose that it has coordinates $p = [0:0:0:1]$ and that the tangent plane is $w = 0$. Suppose also that the intersection of the tangent plane with the quadric is a double line, i.e. $\alpha x^2 + \beta y^2 + \gamma z^2 + axy + bxz + cyz = (\lambda x + \mu y + \nu z)^2 = l(x,y,z)^2$. So the equation of the quadric is $l^2 + w(dx + ey + fz) = 0$. So the derivatives are $(2l(x,y,z)a\ 2l(x,y,z)b\ 2l(x,y,z)c\ dx + ey + fz)$. If $d = e = f$, quadric is a double line. If not, we get a singular point intersecting the line $dx + ey + fz = 0$ with $l(x,y,z) = 0$, that lies on the same plane. □

This two lemmas implies that:

Theorem 3.8. *Consider a smooth K-rational point $p = (p_1, ..., p_4)$ of an irreducible cubic surface V. Then the tangent cone at p in the tangent plane consists of two distinct lines if and only if the polar quadric is non-degenerate; the tangent cone at p in the tangent plane consists of one double line if and only if the polar quadric is degenerate.*

Proof. Consider the singular cubic curve C that is the tangent section at p with V. In the tangent plane, C has a tangent cone in the singular point that is precisely the polar quadric $\mathfrak{P}_p$ intersected with the tangent plane. It is a reducible conic consisting of two (maybe equal) lines, so it is the tangent section at p of the polar $\mathfrak{P}_p$. By the second lemma above, the polar is then degenerate if and only if the tangent cone at p to the tangent section C in V consists of one double line. □

Observation. If p as above do not line on a line in V, then it has tangent section of multiplicative type if and only if the polar quadric at p is non-degenerate, it has tangent section of additive type if and only if the polar quadric at p is degenerate.

We will adopt two different approaches, depending on the characteristic of the ground field K.

- We suppose first that the characteristic of the field is different from 2.

  In this case, to any quadric $\sum_{i\leq j=1}^{4} a_{ij}x_ix_j$ is associated a 4x4 symmetric matrix P in a way that we can write the equation defining the surface in the following way: $F(x_1, ..., x_4) = (x_1x_2x_3x_4)P(x_1x_2x_3x_4)$. This matrix is precisely

$$P = \begin{pmatrix} a_{11} & \frac{a_{12}}{2} & \frac{a_{13}}{2} & \frac{a_{14}}{2} \\ \frac{a_{12}}{2} & a_{22} & \frac{a_{23}}{2} & \frac{a_{24}}{2} \\ \frac{a_{13}}{2} & \frac{a_{23}}{2} & a_{33} & \frac{a_{34}}{2} \\ \frac{a_{14}}{2} & \frac{a_{24}}{2} & \frac{a_{34}}{2} & a_{44} \end{pmatrix}$$

Recall that the quadric associated to that matrix is degenerate if and only if the determinant of P is 0.

Hence from the polar $\mathfrak{P}_p$ at the point $p = (p_1, ..., p_4)$ we can construct a matrix with entries that depends linearly from the coefficients $p_1, ..., p_4$. We will call then $\Delta(p) \in K$ the determinant of the matrix associated to the polar at p. It is a form of degree 4 in the variables $(p_1, ..., p_4)$.

We have then that,

- $\Delta(p) \neq 0$ if and only if the tangent section at p to the cubic surface V is of (maybe twisted) multiplicative type, or is reducible containing two distinct lines that intersect in p.
- $\Delta(p) = 0$ if and only if the tangent section at p to the cubic surface V is of addivite type, or is reducible containing one double line that passes through p.

So the points of additive types are contained in the intersection between the quadric $\Delta(x_1, ..., x_4) = 0$ and our cubic surface. In particular, they are contained in a Zarinski closed subset of V.

- Suppose now that the characteristic of K is 2, so we cannot act as above. However, to a quadric over a field of characteristic two, defined by a quadratic form $Q(x_1, ..., x_4) = 0$ is associated a bilinear form $B(v, w) \coloneqq F(v+w)-F(v)-F(w)$, where $v, w \in K^4$. (Observe that if characteristic is different then 2, $B(v, v) = F(2v)-2F(v) = 4F(v)-2F(v) = 2F(v)$). To this bilinear form, it exists a matrix R such that $B(v, w) = v^t Rw$. Here we have

$$R = \begin{pmatrix} 0 & a_{12} & a_{13} & a_{14} \\ a_{12} & 0 & a_{23} & a_{24} \\ a_{13} & a_{23} & 0 & a_{34} \\ a_{14} & a_{24} & a_{34} & 0 \end{pmatrix}$$

if we write $Q(x_1, ..., x_4) = \sum_{i \leq j=1}^{4} a_{ij} x_i x_j$.

We will prove the following lemma.

Lemma 3.9. *A quadric (in $\mathbb{P}^3_K$) defined by a quadratic equation $Q(x_1, ..., x_4) = 0$ is singular if and only if $Rv = 0$ for some K-point v of the quadric.*

Proof. The quadric is singular if and only if it exists a point $v = (v_1, ..., v_4)$ of the quadric such that $\frac{\partial Q}{\partial x_i}|_p = 0$ for $i = 1, ..., 4$. This last condition in characteristic two is equivalant to $\sum_{j \neq i, j=1}^{4} a_i j v_j$ for $i = 1, ..., 4$, and this is equivalent in saying that $Rv = 0$. This gives the proof. □

We will show that, in characteristic two, every quadric that is a polar to a point p of an irreducible cubic surface is singular.

Theorem 3.10. *Over a field of characteristic 2, for any smooth point p of an irreducible cubic curve V, we have always that the tangent section at p is of (maybe twisted) addivite type, or is reducible containing one double line that passes through p.*

Proof. We will show that, if R is the matrix associated to the quadric $\mathfrak{P}_p$, then $\det(R) = 0$. Once proved this, lemma 3.9 will state that a quadric is singular if and only if has a K-rational point, hence it has to be singular because p belongs to it.

So, it remains to prove that $\det(R) = 0$. It is a straightforward calculation. Using Laplace expansion on the first row, we get for a general R coming from any quadric:

$$\det(R) = a_{12}^2a_{34}^2 - a_{12}a_{23}a_{34}a_{14} - a_{12}a_{13}a_{34}a_{24} + a_{13}^2a_{24}^2 - a_{13}a_{14}a_{23}a_{24} - a_{13}a_{24}a_{34}a_{12} +$$

$$+a_{14}^2a_{23}^2 - a_{14}a_{12}a_{23}a_{34} - a_{14}a_{13}a_{24}a_{23} = a_{12}^2a_{34}^2 + a_{13}^2a_{24}^2 + a_{14}^2a_{23}^2 =$$

$$= (a_{12}a_{34} + a_{13}a_{24} + a_{14}a_{23})^2$$

If now we suppose that the quadric is a polar at some point $p = (p_1, ..., p_4)$ to a cubic surface V, a_{ij} is the coefficient of x_ix_j of the polar. We can obtain this monomials of the polar only from deriving things of the type $x_ix_jx_k$ in the equation of the cubic surface, because we obtain zero when we derive things like $x_i^2x_j$ in x_i in characteristic 2. If we take $\{i, j, k, l\} = \{1, 2, 3, 4\}$, and we define λ_i the coefficient of the monomial $x_jx_kx_l$ in the equation of the cubic surface, then we get that

$$a_{ij} = \lambda_k p_l + \lambda_l p_k$$

So $a_{ij}a_{kl} = \lambda_k\lambda_i p_l p_j + \lambda_k\lambda_j p_l p_j + \lambda_l\lambda_i p_k p_j + \lambda_l\lambda_j p_k p_j$. And if we sum up the terms that we will need in the expression of our discriminant $a_{12}a_{34} + a_{13}a_{24} + a_{14}a_{23}$ we see that each of the possible terms $\lambda_i\lambda_j p_k p_j$ appear twice in that formula, so we get that $a_{12}a_{34} + a_{13}a_{24} + a_{14}a_{23} = 0$ and so

$$\det(R) = (a_{12}a_{34} + a_{13}a_{24} + a_{14}a_{23})^2 = 0$$

what we wanted. □

3.2.2 Reconstruction of the configuration

We want now to reconstruct this (C_m, C_a)-configuration, up to isomorphism. To do this we only need two 0-cycles on l: the three points of intersection of l with C_m and the three points of intersection of l with C_a. We have to suppose that these points are defined over K.

We can choose projective coordinates over K on P_m; we will call them $[x : y : z]$ and impose that l has the equation $z = 0$, thinking it as the line at infinity. Furthermore we can assume that the singular K-point p_m of our cubic curve has coordinate $[0 : 0 : 1]$. This

implies that the coefficient of the monomials in the equation of our cubic z^3, xz^2, yz^2 are zero. Hence our cubic has an equation of this form: $zg_2(x,y) + g_3(x,y) = 0$, where g_n is some form of degree n ($n = 2, 3$). We can observe also that the tangents at the singular point $[0:0:1]$ are defined by $g_2(x,y) = 0$. We finally suppose that these tangents are exactly $x = 0$ and $y = 0$ obtaining an equation of C_m of the form

$$xyz + g_3(x,y) = 0$$

We can do the same for C_a, choosing projective coordinates over K on P_a such that l has equation $z' = 0$ and the point p_a has coordinate $[0:0:1]$. We suppose now instead that the tangent is $x' = 0$ obtaining an equation of C_a of the form

$$y'^2 z' + g'_3(x', y') = 0$$

In both equations, giving the three points of intersection $C_m \cap l$, respectively $C_a \cap l$, is the same as determining the cubic form g_3, resp. g'_3. This gives $g_3(x,y)$ up to a nonzero scalar factor of K, in the equation of our cubic curve. But z is defined up to multiplication by constants from $K^\times$, then C_m and C_a are defined by the two equations we have obtained, up to isomorphism. We have showed that, using the two 0-cycles of intersection allows us to reconstruct the configuration up to isomorphism.

Observation. If a (C_m, C_a)-configuration is tangent to some cubic surface, then the two 0-cycles coincide: we have only the three point of intersection of l with the surface.

3.3 Geometric reconstruction of K from a (C_m, C_a)-configuration

Consider now a (C_m, C_a)-configuration. We would like to reconstruct the ground field K. Denote by $M \coloneqq C_{m,sm}(K)$ and by $A \coloneqq C_{a,sm}(K)$ the sets of smooth points of the two cubic curves, and give to them respectively the two group structures that are obtained choosing a base point, that we will call 1_m and 0_a respectively, as done in section 2.2. We will then define the following two bijections:

- Consider $\tilde{C}_m$ the normalization of C_m. Notice that we have already seen its construction in the proof of lemma 2.8. We define the map $\alpha : \tilde{C}_m(K) \to l(K)$, that sends each smooth K-point q of C_m to the point obtained intersecting l with the K-line passing through q and p_m, and sending the two K-points of $\tilde{C}_m$ that lie over p_m to the two points obtained intersecting l with the two tangent lines at p_m. This is clearly a bijection.

- We define the map $\beta : C_a(K) \to l(K)$, sending each smooth K-point q of C_a to the point obtained intersecting l with the K-line passing through q and p_a, and sending the p_a to the point obtained intersecting l with the tangent at p_a. This is clearly a bijection.

If we call 0_m and ∞_m the images through α of the two points over p_m, and ∞_a the image of p_a through β, then we have a bijection

$$\mu \coloneqq \beta^{-1} \circ \alpha : M \cup \{0_m, \infty_m\} \to A \cup \{\infty_a\}$$

This gives to (M, A, μ), through the projective line l, the combinatorial data that we need to reconstruct the ground field K, as done in the reconstructing lemma 3.2. Hence we have reconstructed isomorphic versions of the field K and of the projective line l.

3.4 Geometric reconstruction of the cubic surface V

If we add to a (C_m, C_a)-configuration two other tangent plane sections of either additive or multiplicative type, we can reconstruct uniquely our cubic surface. In this section, we will explain how. We need a definition first.

Definition 3.11. *We call a* tetrahedral configuration *the following family of subschemes in* $\mathbb{P}^3_K$*:*

- *four distinct K-points* $p_1, p_2, p_3, p_4 \in \mathbb{P}^3(K)$*;*
- *four distinct K-planes* $P_1, P_2, P_3, P_4 \subset \mathbb{P}^3$ *with the property that* P_i *contains* p_i *but not* p_j *with* $j \neq i$ *(this for each* $i = 1, 2, 3, 4$*);*
- *four geometrically irreducible cubic curves* C_1, C_2, C_3, C_4*, defined over K, with the property that* $C_i \subset P_i$ *is of multiplicative type or is of additive type, with singular point in* $p_i \in C_i(K)$ *(this for each* $i = 1, 2, 3, 4$*). Furthermore we assume that at least one of them is of multiplicative type, and at least another one is of additive type.*

Definition 3.12. *Consider now an irreducible cubic surface V defined over K. We say that the tetrahedral configuration* $(p_i, C_i, P_i)_{i=1,...,4}$ *is* tangent *to V if:*

- $V(K)$ *contains the four points* p_1, p_2, p_3, p_4*;*
- P_1, P_2, P_3, P_4 *are the tangent planes to V at* p_1, p_2, p_3, p_4 *(respectively);*
- C_1, C_2, C_3, C_4 *are the tangent sections* $C_i = P_i \cap V$ *(this for each i).*

We will now describe how actual reconstruction works.

Construction 2 (Reconstruction of the surface). Consider an irreducible cubic surface V, defined over K, a field with more than four elements. Our starting point is a tetrahedral configuration $(p_i, C_i, P_i)_{i=1,...,4}$ that is tangent to V. Knowing this configuration, we want to reconstruct our surface back.

We start choosing a suitable system of coordinates $x_1, ..., x_4$ over $\mathbb{P}^3_K$, in such a way that the equation of each plane P_i is $x_i = 0$. We know that V is a cubic surface in $\mathbb{P}^3$, so it is defined by an equation $F(x_1, ..., x_4) = 0$, where F is a cubic form with coefficients in K. We can also write for each $i = 1, ..., 4$

$$F(x_1, ..., x_4) = f_3^{(i)}(x_j : j \neq i) + x_i h_2^{(i)}(x_1, ..., x_4)$$

where $f_3^{(i)}$ is a form of degree 3 and $h_3^{(i)}$ is a form of degree two. Observe that, from this formula, we could easily obtain the equation of the tangent section C_i: it is enough to

intersect the tangent plane $x_i = 0$ with the surface $F = 0$ where F is written as above. So C_i has equation $f_3^{(i)}(x_j : j \neq i) = 0$ (inside the plane P_i).

Conversely, if we know the equation of C_i, we know the polynomial $f_3^{(i)}(x_j : j \neq i)$, up to a scalar factor.

We can go further. We can also write $h_2^{(i)}(x_1, ..., x_4) = g_2^{(k)}(x_j \neq k) + x_k h_1^{(k)}(x_1, ..., x_4)$ and $h_1^{(k)}(x_1, ..., x_4) = g_1^{(l)}(x_j \neq l) + g_0^{(l)} x_l$, where the pedices in the expressions h_n and g_n indicate that they are forms of degree n over K. We then obtain the following formula for F:

$$F(x_1, ..., x_4) = f_3^{(i)}(x_j \colon j \neq i) + x_i g_2^{(k)}(x_j \colon j \neq k) + x_i x_k g_1^{(l)}(x_j \colon j \neq l) + g_0^{(l)} x_i x_k x_l$$

for any $i, k, l = 1, ..., 4$.

Observe also that we have $f_3^{(k)}(x_j \colon j \neq k) = \left(f_3^{(i)}(x_j \colon j \neq i, x_k = 0)\right) + x_i g_2^{(k)}(x_j \colon j \neq k)$ intersecting with $x_k = 0$, and we have $f_3^{(l)}(x_j \colon j \neq l) = \left(f_3^{(i)}(x_j \colon j \neq i, x_l = 0) + x_i g_2^{(k)}(x_j \colon j \neq k, x_l = 0)\right) + x_i x_k g_1^{(l)}(x_j \colon j \neq l)$. intersecting with $x_l = 0$.

If we know these four polynomials $f_3^{(1)}(x_i \colon j \neq 1), ..., f_3^{(4)}(x_i \colon j \neq 4)$, we can then reconstruct the polynomial F in the following way:

1. Fix i. Start considering $f_3^{(i)}(x_j \colon j \neq i)$.

2. Consider $k \neq i$. Add to the previous polynomial the expression $x_i g_2^{(k)}(x_j \colon j \neq k)$, using the formula of $f_3^{(k)}(x_j \colon j \neq k)$ written before.

3. Take $l \neq i, k$. Add $x_i x_k g_1^{(l)}(x_j \colon j \neq l)$ to what we just obtained, using the expression of $f_3^{(l)}(x_j \colon j \neq l)$ written before.

4. It remains $t \neq i, k, l$. Add to all the expression the term $g_0^{(l)} x_i x_k x_l$ if is present in $f_3^{(t)}(x_j \colon j \neq t)$.

For how we have reconstructed F, we know that it is the right one.

But we do not have the polynomials $f_3^{(i)}(x_j : j \neq i)$; what we have are the equations of the C_i: to get them it is enough to consider two tangent sections of the configuration of different types, reconstruct the projective line between them (the line of intersection of the two tangent planes) as done in 3.3, in order to be able to reconstruct the two equations acting as in section 3.2.2.

Hence we have $f_3^{(i)}(x_j : j \neq i)$ up to nonzero element of K. Because we do not know this scalar, some ambiguities can arise in reconstructing our surface V. However, under certain conditions, we can reconstruct V uniquely. Precisely, if there is a common monomial with nonzero coefficient two equations of the tangent section of the configuration, then we can multiply one of the two expressions with a nonzero scalar in order to have the same constant in front of that monomial. If we can do this for all the expressions, then we can reconstruct V uniquely: we can glue correctly the equations of the C_i because we can 'connect' the four equations with those common monomials.

We will now state this in a more formal way making use of a graph G with four vertices $(1, ..., 4)$. We will say that two (distinct) vertices i and j are *connected by an edge* if there exists a cubic monomial that has nonzero coefficient in both $f_3^{(i)}$ and $f_3^{(j)}$. The only possible monomials that can achieve this result are those in the variables $(x_k : k \neq i, j)$. We have to choose an ordered set $\{i, k, l, t\}$ of vertices such that each element is connected by an edge to the previous and to the following one (all the elements are distinct). So, using this ordered set, we act as in the points 1), ..., 4) above. Since there exists an edge connecting the previous and the following equations of our configuration, the same monomial is present in the two equations, hence it is enough to multiply one of them by a nonzero scalar to get the same coefficient as the other one. In this way, there is a unique way to reconstruct the equation F.

The condition to reconstruct uniquely and without ambiguities F, up to a nonzero scalar factor, i.e. the existence of that ordered set, is then clear to be equivalent to the fact that G is connected. If so, we can glue in a unique way all the four equations of the tetrahedral configuration to get our F back.

We have proved that:

Proposition 3.13. *A tetrahedral configuration, tangent to an irreducible cubic surface V and with connected graph G, allows us to reconstruct uniquely the equation of V, up to isomorphism.*

Example. We will show this procedure now in an example. Suppose we have obtained the following tangent sections:

$$\begin{cases} x_1 = 0 \\ x_4^3 = x_2^2x_4 + x_2^2x_3 + \sqrt{2}x_2x_3x_4 \end{cases}$$

$$\begin{cases} x_2 = 0 \\ x_1x_3^2 - x_4^3 + 3x_1^2x_4 - 2x_1^3 = 0 \end{cases}$$

$$\begin{cases} x_3 = 0 \\ x_4^3 - 3x_1^2x_4 + 2x_1^3 = x_2^2x_4 \end{cases}$$

$$\begin{cases} x_4 = 0 \\ 2x_1^3 = x_2^2x_3 + x_1x_3^2 \end{cases}$$

1. We start writing: $f_3^{(1)}(x_2, x_3, x_4) = x_4^3 - x_2^2x_4 - x_2^2x_3 - \sqrt{2}x_2x_3x_4$.
2. We rescale multiplying by -1 and add the monomials of $f_3^{(2)}$ that do not appear already: $x_4^3 - x_2^2x_4 - x_2^2x_3 - \sqrt{2}x_2x_3x_4 - 3x_1^2x_4 + 2x_1^3 - x_1x_3^2$.
3. All monomials of $f_3^{(3)}$ appears already: $x_4^3 - x_2^2x_4 - x_2^2x_3 - \sqrt{2}x_2x_3x_4 - 3x_1^2x_4 + 2x_1^3 - x_1x_3^2$.
4. All monomials of $f_3^{(3)}$ appears already. The equation of the cubic surface is finally:

$$x_4^3 - x_2^2x_4 - x_2^2x_3 - \sqrt{2}x_2x_3x_4 - 3x_1^2x_4 + 2x_1^3 - x_1x_3^2.$$

This results holds for more general 'configurations':

Proposition 3.14. *Consider a configuration made of four K-planes $P_1, ..., P_4$ and four irreducible cubic curves $C_1, ..., C_4$ over them, with given equations. Set $l_{ij} := P_i \cap P_j$ the line of intersection of the two planes.*

If we suppose that $C_i \cap l_{ij} = C_j \cap l_{ij}$ for any $i, j = 1, ..., 4$, then we can uniquely construct a cubic surface V, such that $V \cap P_i = C_i$.

Furthermore, if the cubic C_i is singular, then the plane P_i is tangent to V.

Proof. Without loss of generality we can assume that P_i is the coordinate plane defined by the equation $x_i = 0$. We will use the following:

Lemma 3.15. *The fact that $C_1, ..., C_4$ are irreducible cubic curves, implies that the graph G of the configuration is connected.*

Proof. We will prove this by absurd: suppose then that the graph G is not connected. Two situations can occur:

- One of the vertices of G is not connected to anything: we can and will suppose that this vertex is 4. We will analyze now the expression of $f_3^{(4)}(x_1, x_2, x_3)$. Saying that 4 is not connected in G means that, if we consider the monomials $x_1^l x_2^m$, $x_1^l x_3^m$, $x_2^l x_3^m$ of degree 3 for suitable $l, m \in \mathbb{Z}_{\geq 0}$, they don't have nonzero coefficient in $f_3^{(4)}(x_1, x_2, x_3)$, and because x_4 doesn't appear in this expression, the only possibility is that

  $$f_3^{(4)}(x_1, x_2, x_3) = \lambda x_1x_2x_3$$

  with $\lambda \in K^\times$. Hence the equation of C_4 is $\lambda x_1x_2x_3 = 0$ for some $\lambda \in K^\times$. This means that C_4 is a reducible cubic curve, which is not possible.

- Every vertex of G is connected to another one, but only one and not more. We can assume that 1 is connected to 2, 3 is connected to 4 and there are no other segments that could connect them. Consider again $f_3^{(4)}(x_1, x_2, x_3)$. Saying that 4 is not connected to 1 nor 2, means that the degree-3 monomials $x_2^l x_3^m$, $x_1^l x_3^m$ don't have nonzero coefficient in $f_3^{(4)}(x_1, x_2, x_3)$, for any suitable $l, m \in \mathbb{Z}_{\geq 0}$. Hence $f_3^{(4)}(x_1, x_2, x_3) = \delta x_1x_2x_3 + h^{(4)}(x_1, x_2)$ where $\delta \in K$ and $h^{(4)}$ is a cubic form of degree 3 in the variables x_1,x_2. We can use the same reasoning as in the previous point, to get that $f_3^{(1)}(x_2, x_3, x_4) = \alpha x_2x_3x_4 + h^{(1)}(x_3, x_4)$, $f_3^{(2)}(x_1, x_2, x_3) = \beta x_1x_3x_4 + h^{(2)}(x_3, x_4)$, where $\alpha, \beta \in K$ and $h^{(1)}, h^{(2)}$ are two cubic forms of degree 3 in the variables x_3,x_4. From the expression of $f_3^{(1)}$ we see that x_2^3 doesn't appear in $f_3^{(4)}$; from the expression of $f_3^{(2)}$ we see that x_1^3 doesn't appear in $f_3^{(4)}$, hence

  $$f_3^{(4)}(x_1, x_2, x_3) = \delta x_1x_2x_3 + ax_1^2x_2 + bx_1x_2^2$$

  with $a, b \in K$. The equation of C_4 is then $\delta x_1x_2(x_3 + ax_1 + bx_2)$ hence C_4 is a reducible cubic curve, which is not possible.

□

So, we have showed that G is connected. However, if we try to construct the equation of a cubic surface with four given plane sections as in construction 2, another problem can occur. Indeed, we can patch the four equation in a unique way thanks to the connectedness of G, but only once we have fixed an order of patching: some of the monomials can be left out. For example, if we have started writing $f_3^{(1)}(x_2, x_3, x_4) = x_2^3 - x_3^2 x_4$ and we have that $f_3^{(2)}(x_1, x_3, x_4) = x_1^3 - x_3^2 x_4 + x_3^3$, then we will get the intermediate expression for F that is $x_2^3 - x_3^2 x_4 + x_1^3$, but the monomial x_3^3 do not appear and could never do.

We will show now that this is avoided when we make the assumption that $C_i \cap l_{ij} = C_j \cap l_{ij}$ for any $i, j = 1, ..., 4$. Indeed, now l_{ij} has equation $x_i = 0 \wedge x_j = 0$, so the condition is equivalent to the fact that the monomials in the two other variables have the same coefficients (after rescaling). This implies that all the monomials in one or two variable can be patch together. It remains the problem of monomials in three variable, but it is not: these monomials can only appear in one of the four expressions $f_3^{(i)}(x_j \colon j \neq i)$, hence they have to be written in the final equation of F.

Hence this assumption assures that the constructed surface V is such that $V \cap P_i = C_i$, and also that the construction is independent by the choice of the order of our actions.

Finally, the only possibility for a section of a cubic surface that is an irreducible singular cubic is that it was obtained by intersecting V with a tangent plane. □

Corollary 3.16. *A tetrahedral configuration, tangent to an irreducible cubic surface V, allows us to reconstruct uniquely the equation of V, up to isomorphism.*

Proof. By the lemma in the proof, a tetrahedral configuration has graph G connected. So we can take off this hypothesis in proposition 3.13. Notice also that we use the singularity of the cubics only to reconstruct the lines l_{ij}, in order to get the equations of the configuration. □

4 Combinatorial Reconstruction of Cubic Surfaces

In this chapter, we will rephrase all the geometric constructions of chapter 3 in a combinatorial language, doing some refinements in particular in the reconstruction of K.

4.1 Combinatorial Projective Line

We now store in the following definition, the combinatorial data that we need to reconstruct a projective line, and that we can obtain through the construction 1 of chapter 3.

Definition 4.1 (Combinatorial projective line)**.** *Consider an abstract set H, with five elements in it denoted as*

$$0_a, \infty_a, 0_m, 1_m, \infty_m$$

Suppose that $A = H\backslash\{\infty_a\}$ has a structure of (additive) abelian group with unit element 0_a, and $M = H\backslash\{0_m, \infty_m\}$ has a (multiplicative) abelian group structure with unit element 1_m, and with inversion map $i : M \to M$. Furthermore suppose that we have a bijection

$$\mu : M \cup \{0_m, \infty_m\} \to A \cup \{\infty_a\}$$

connecting the two sets. We extend the group law of M in a partial one on $M \cup \{0_m, \infty_m\}$ putting, for any $p \in M$,

$$p \cdot 0_m := 0_m, \quad p \cdot \infty_m := \infty_m, \quad i(0_m) := \infty_m, \quad i(\infty_m) := 0_m$$

In a similar way we extend the group law of A in a partial one on $A \cup \{\infty_a\}$ putting, for any $q \in A$,

$$q \pm \infty_a := \infty_a$$

We call the data $(A, M, \mu, \{0_a, \infty_a, 0_m, 1_m, \infty_m\})$ a combinatorial projective line *if furthermore the resulting bijection ν, obtained using lemma 3.2 (see also the observation after it), gives to A a structure of a field, with sum the sum on A and with multiplication the multiplication of M induced on $A\backslash\{0_a\}$ using ν: we set*

$$p *_M q := \nu\,(\nu^p \cdot_M \nu^q)$$

for any $p, q \in A$.

The following lemma states that from these combinatorial data we can construct uniquely a geometric projective line, while lemma 3.2 states that, if these data comes from a geometric projective line, then we have constructed exactly that line.

Lemma 4.2. *Consider a combinatorial projective line $(A, M, \mu, \{0_a, \infty_a, 0_m, 1_m, \infty_m\})$. Recall that in oarticular the set A with its own addition and multiplication induced from M through ν is a field, where ν: $M \cup \{0_m, \infty_m\} \longrightarrow A \cup \{\infty_a\}$ is the bijection of lemma 3.2. Then we get a natural identification*

$$A \cup \{\infty_a\} = \mathbb{P}^1(A).$$

4.2 Combinatorial Cubic Surfaces

We will now define the combinatorial equivalent of a geometric cubic surface (precisely the combinatorial equivalent of the smooth part of its K-rational points).

Definition 4.3. *A* combinatorial cubic surface *is a non-empty set S with the following two structures:*

- *A symmetric ternary relation $\mathfrak{L} \subset S^3$ that we will call* collinearity. *Three elements $p, q, r \in S$ are collinear if $(p, q, r) \in \mathfrak{L}$.*
- *A collection $\mathfrak{P}$ of subsets of S whose elements we will call* plane sections.

Furthermore we assume that $(S, \mathfrak{L}, \mathfrak{P})$ satisfies the following axioms:

1. ***Collinearity axioms.***
   - *(i) For any $p, q \in S$, there exists an element $r \in S$ such that $(p, q, r) \in \mathfrak{L}$.*
   - *(ii) We will call a triple $(p, q, r) \in \mathfrak{L}$* strictly collinear *if r is uniquely determined by p and q and all the three elements are dinstict. Furthermore we will denote by $\mathfrak{L}_s$ the subset of $\mathfrak{L}$ that consists of all the triples that are strictly collinear. We assume that this set $\mathfrak{L}_s$ is a symmetric ternary relation (the unicity property has to be respected by symmetries in L).*
   - *(iii) Consider two distinct elements $p, q \in S$ and suppose that there exist two elements $r_1 \neq r_2$ in S satisfying $(p, q, r_1) \in \mathfrak{L}$ and $(p, q, r_2) \in \mathfrak{L}$. With these assumptions, we will call a* line *in S the set of all such r's: precisely $l = l(p, q) := \{r \in S : (p, q, r) \in \mathfrak{L}\}$. Furthermore, we assume that $l^3 \subset \mathfrak{L}$: this means that any three points of l are collinear.*
2. ***Plane sections axioms.***
   - *(i) For any $p \in S$, we will call the set $C_p := \{q \in S : (p, p, q) \in \mathfrak{L}\}$ a* tangent plane section *and we assume any such C_p belongs to $\mathfrak{P}$.*
   - *(ii) Composition axiom.*
     - *Consider $C \in \mathfrak{P}$ a plane section that is not a tangent one and that does not contain any line in S. Then, if we denote $\mathfrak{L}_C := \{(p, q, r) \in \mathfrak{L} : p, q, r \in C\}$ the ternary relation induced by $\mathfrak{L}$ on C, the couple $(C, \mathfrak{L}_C)$ is an abelian symmetric quasigroup.*
     - *Consider $C_p \in \mathfrak{P}$ a tangent plane section that does not contain any line in S and denote $C_p^0 := C_p \backslash \{p\}$. Then, if we denote $\mathfrak{L}_{C_p^0} := \{(p, q, r) \in \mathfrak{L} : p, q, r \in C_p^0\}$ the ternary relation induced by $\mathfrak{L}$ on C_p^0, the couple $(C_p^0, \mathfrak{L}_{C_p^0})$ is an abelian symmetric quasigroup.*
   - *(iii) Fix $\lambda := (p, q, r) \in \mathfrak{L}$ where at least two of the points p, q, r are distinct. We will call a* pencil of plane sections *the following subset of $\mathfrak{P}$:*

$$\Pi_\lambda := \{C \in \mathfrak{P} : p, q, r \in C\}$$

We assume the two following properties:

– *If $\lambda = (p, q, r)$ do not lie on a line in S, then*

$$S \backslash \{p, q, r\} = \coprod_{C \in \Pi_\lambda} (C \backslash \{p, q, r\})$$

– *If $\lambda = (p, q, r)$ belongs to a line l in S, then*

$$S \backslash l = \coprod_{C \in \Pi_\lambda} (C \backslash l)$$

4.2.1 Combinatorial cubic surfaces of geometric origin

We start from a field K and from an irreducible cubic surface V defined over it.

Proposition 4.4. *We will give the following definitions:*

- *Denote by $S \coloneqq V_{sm}(K)$ the set of nonsingular K-points of V.*
- *Define the symmetric ternary relation $\mathfrak{L}$ in this way: $(p, q, r) \in \mathfrak{L}$ if and only if $p + q + r$ is the complete intersection cycle of V with a K-line in $\mathbb{P}^3$ or if p, q, r lie on a K-line contained in $V(K)$.*
- *All the elements of $\mathfrak{P}$ are obtained in the following way. Consider a K-plane $P \subset \mathbb{P}^3$ that contains two distinct K-points of S, or that is tangent to a K-point of S, or contains one of the tangent lines to the singular point of a tangent section, that belongs to S. Then $C \coloneqq P(K) \cap S$ is an element of $\mathfrak{P}$.*

Then $(S, \mathfrak{L}, \mathfrak{P})$ is a combinatorial cubic surface.

Proof. It is clear that all the Collinearity axioms and Plane section axiom (*iii*) hold for all the smooth points of a cubic surface (mainly by Bezout). It is also clear that if a point is non-singular, the definition of its tangent section of Plane section axiom (*i*) is the right one. Finally, in Plane section axiom (*ii*), we assume that the plane sections do not contain any line, hence they are irreducible cubic curves, singular if the plane was tangent, hence their smooth points forms a symmetric quasigroup as in section 2.2. □

Observation. Also ruled cubic surfaces are combinatorial cubic surfaces, but observe that Plane section axiom (*ii*) does not make any request for them.

4.3 Combinatorial (C_m, C_a)-configurations

Now we will define the combinatorial equivalent of a (C_m, C_a)-configuration.

Definition 4.5. *Consider $(S, \mathfrak{L}, \mathfrak{P})$ a combinatorial cubic surface. Suppose we have the following data:*

- *Two distinct elements $p_m, p_a \in S$, that are not lying on a line in S.*
- *The two respective tangent plane sections $C_{p_m}, C_{p_a} \in \mathfrak{P}$.*

Let $r \in S$ be the unique element of S such that $\lambda := (p_a, p_m, r) \in \mathfrak{L}$, and denote by Π_λ the respective pencil of plane sections. Define $C^0_{p_m} := C_{p_m} \backslash \{p_m\}$ and $C^0_{p_a} := C_{p_a} \backslash \{p_a\}$.

Furthermore consider the binary relation $R \subset C_{p_a} \times C_{p_m}$, where by definition we have, for $p \in C^0_{p_m}$ and $q \in C^0_{p_a}$, that $(p, q) \in R$ if and only if there exists a plane section $P \in \Pi_\lambda$ with $p, q \in P$, that $(p_a, q) \in R$ if and only if $(p, q) \notin R$ for all $p \in C^0_{p_a}$, and that $(p, p_m) \in R$ if and only if $(p, q) \notin R$ for all $q \in C^0_{p_m}$.

*We will then call $(p_m, p_a, C_{p_m}, C_{p_a})$ a (C_m, C_a)-*configuration *if the following conditions are satisfied:*

(i) R is a graph of some function $\rho \colon C_{p_a} \to C_{p_m}$ which is bijective except in two points that are both sent to p_m. We will call these two points 0_m and ∞_m (they are such that $\rho(0_m) = \rho(\infty_m) = p_m$). Let $\infty_a := \rho(p_a)$. Assume also that $0_m, \infty_m \neq p_a$ and $\infty_a \neq p_m$, in other words, $0_m, \infty_m \in C^0_{p_a}$ and $\infty_a \in C^0_{p_m}$.

(ii) Denote $A := C^0_{p_a}$ and $M := C^0_{p_m}$ and choose two points $0_a \in A$ and $1_m \in M$. By the composition axiom of our combinatorial cubic surface, we can give to A and to M the structure of abelian groups, choosing respectively 0_a and 1_m as the zero and the one of the group laws. Define $\mu : M \cup \{0_m, \infty_m\} \to A \cup \{\infty_a\}$ as the bijection that is ρ^{-1} on M and on 0_m and ∞_m is the identity of A (restricted to those two points).

(iii) Finally assume that $C_{p_m} \cap C_{p_a}$ consists of three distinct points.

4.4 Combinatorial Tetrahedral Configurations

Finally we define the combinatorial equivalent of a geometric tetrahedral configuration.

Definition 4.6. *Consider $(S, \mathfrak{L}, \mathfrak{P})$ a combinatorial cubic surface. Suppose we have the following data:*

- *Four distinct elements $p_1, p_2, p_3, p_4 \in S$ that pairwise do not lie on a line in S.*
- *The four respective tangent plane sections $C_{p_1}, C_{p_2}, C_{p_3}, C_{p_4} \in \mathfrak{P}$, which have attached to them a fixed label of being "multiplicative" or of being "additive", and furthermore they cannot have all the same label.*

For any p_i, p_j with $i \neq j$, we have the following. Let $r_{ij} \in S$ be the unique element of S such that $\lambda_{ij} := (p_i, p_j, r_{ij}) \in \mathfrak{L}$, and denote by $\Pi_{\lambda_{ij}}$ the respective pencil of plane sections. Define $C^0_{p_i} := C_{p_i} \backslash \{p_i\}$ and $C^0_{p_j} := C_{p_j} \backslash \{p_j\}$.

Furthermore consider the binary relation $R_{ij} \subset C_{p_i} \times C_{p_j}$, where by definition we have, for $p \in C^0_{p_i}$ and $q \in C^0_{p_j}$, that $(p, q) \in R_{ij}$ if and only if there exists $P \in \Pi_{\lambda_{ij}}$ with $p, q \in P$, that

$(p_i, q) \in R_{ij}$ *if and only if* $(p, q) \notin R_{ij}$ *for all* $p \in C^0_{p_i}$*, and that* $(p, p_j) \in R_{ij}$ *if and only if* $(p, q) \notin R_{ij}$ *for all* $q \in C^0_{p_j}$.

We will then call $(p_1, p_2, p_3, p_4, C_{p_1}, C_{p_2}, C_{p_3}, C_{p_4})$ *a* combinatorial tetrahedral configuration *if the following conditions are satisfied:*

(i) $R_{ij}|_{C^0_{p_i} \times C^0_{p_j}}$ *is a graph of some function* $\rho_{ij} \colon C^0_{p_i} \to C^0_{p_j}$ *that is bijective. Furthermore, we define the improper points of* C_{p_i}*, one improper point if* C_{p_i} *is additive and two if it is multiplicative, in the following way: they are the (one or two) points of* C_{p_j} *that are in relation with* p_i *in the sense of* R_{ij}*. In the same way, we also define the improper points of* C_{p_j}*: one if* C_{p_j} *is additive, two if it is multiplicative. So they are the points of* C_{p_i} *that are in relation with* p_j *in the sense of* R_{ij}*.*

(ii) Now, using the composition axiom on our combinatorial cubic surface, we can give to $C^0_{p_i}$ *and to* $C^0_{p_j}$ *the structure of abelian groups, choosing one element in each set to become the neutral element. Define then* $\mu_{ij} : C^0_{p_i} \cup \{\text{its improper points}\} \to C^0_{p_j} \cup \{\text{its improper points}\}$ *as the bijection, that is* ρ *on* $C^0_{p_i}$ *and the identity on the improper points of* C_{p_i} *(identity on* C_{p_j} *restrected too those points.*

(iii) Finally assume that $C_{p_i} \cap C_{p_j}$ *consists of three pairwise distinct points.*

It is obvious that a combinatorial tetrahedral configuration contains in itself a combinatorial (C_m, C_a)-configuration.

5 Reconstruction Theorems

In the previous chapter, we have given all the definitions that we will need now, definitions that store the combinatorial information required for the reconstruction.

The lemma of section 5.1 shows how we can construct a field K and a cubic surface V in a unique way using the given combinatorial data. The theorem of section 5.2 shows that the construction explained in the lemma has the properties that are needed for reconstruction: so the first part shows how we can derive the combinatorial data we need from our starting geometric objects. The second part states that if we do derive this combinatorial data from a cubic surface and then we apply the construction in the lemma, we get a field K' and a surface V' that are isomorphic to the original field K and to the original surface V.

5.1 Construction of a geometric cubic surface from combinatorial data

Lemma 5.1 (Part 1 - Construction of the ground field)**.** *Suppose that we are given a combinatorial cubic surface and a combinatorial* (C_m, C_a)*-configuration in it.*

If the data $(A, M, \mu, \{0_a, \infty_a, 0_m, 1_m, \infty_m\})$*, that we can get from the definition of combinatorial* (C_m, C_a)*-configuration, yields a structure of combinatorial projective line, then we can use lemma* 3.2 *to construct a field* K*, together with a geometric projective line* $\mathbb{P}^1(K)$*.*

Proof. This lemma is tautological. It follows directly from the definition of a combinatorial projective line. □

Observe that now we do not need any more the line of intersection of the two planes of the configuration, but we use the pencil of plane sections between our two points to get a bijection between the two singular curves, to represent a combinatorial projective line.

Lemma 5.2 (Part 2 - Construction of the cubic surface)**.** *Suppose that we are given a combinatorial cubic surface and a combinatorial tetrahedral configuration. Assume that each tangent plane section defines, together with a section of the other type in the configuration, a combinatorial projective line as in the previous lemma.*

If the graph G *of the configuration is connected, then we can uniquely construct a cubic surface* V*.*

Proof. The first assumption guarantees the reconstruction of the configuration as in section 3.2.2 (and a bit also in construction 2). Then we can look at theorem 3.14: G is connected by hypothesis, and the other assumption of the theorem is true by (*iii*) in the definition of a combinatorial tetrahedral configuration. So a cubic surface V can always be uniquely constructed in this way. □

5.2 Reconstruction of the cubic surface

Theorem 5.3 (Part 1 - Combinatorial data from a geometric cubic surface)**.** *We start from a field K with more than four points and from an irreducible cubic surface V defined over it.*

If there exists a geometric (C_m, C_a)-configuration or a geometric (tangent) tetrahedral configuration, over K, such that every three points of intersection between the tangent sections are defined over K, then we can derive a combinatorial (C_m, C_a)-configuration or a combinatorial tetrahedral configuration.

Proof. As done in section 4.2.1, we have that $(V_{sm}(K), \mathfrak{L}, \mathfrak{P})$ is a combinatorial cubic surface. If we have a geometric (C_m, C_a)-configuration or a geometric (tangent) tetrahedral configuration as above, then it is straightforward that the definitions given in section 4.2.1 lead to a combinatorial (C_m, C_a)-configuration and to a combinatorial tetrahedral configuration. Observe that condition (*iii*) in the definition of a combinatorial (C_m, C_a)-configuration and of a combinatorial tetrahedral configuration requires that each three points of intersection between the sections are K-rational. □

Observation. We can slightly improve this statement, if these geometric configurations are not defined over K but they are defined over the algebraic closure of K. Then it exists a finite extension of K, over which the geometric and then the combinatorial configurations exists.

We can further observe that there exists some irreducible cubic surfaces that do not have these geometric configuration even on the algebraic closure of K. It is the case of ruled cubic surfaces: each tangent section contains a K-line, and then it is a reducible cubic, neither of multiplicative, nor additive type.

Furthermore, for fields of characteristic 2, reconstruction is never possible, because there never exist points of multiplicative types in this situation (look at theorem 3.10).

Theorem 5.4 (Part 2 - Combinatorial Reconstruction of Cubic Surfaces)**.** *Consider a field K with more than four elements and an irreducible cubic surface V defined over it. Suppose we are given a combinatorial (C_m, C_a)-configuration and a combinatorial tetrahedral configuration of geometric origin, i.e. that can be obtained as in Part 1 of the Theorem. (This is possible if and only if such configurations do exists.)*

Then it is possible to uniquely construct a field K' and a cubic surface V', as in the construction lemma of the previous section (section 5.1*). Furthermore we have a natural identification between the fields K' and K and between the cubic surfaces V' and V.*

Proof. For the part regarding the ground field K, it follows directly from what we have done for the projective lines (sections 3.1 and 4.1)). For what concerning the cubic surface, from the combinatorial data of geometric origin, we can construct uniquely a cubic surface, as in the second part of the lemma of the previous section 5.1, because the graph

G has to be connected (theorem 3.13) and because a (C_m, C_a)-configuration do define a geometric projective line. This surface V' is tangent to the given (reconstructed) tetrahedral configuration, as in theorem 3.14. Hence V' has to be isomorphic to V, the cubic surface we started with. This ends the proof. □

References

[1] Yu. I. Manin, *Combinatorial cubic surfaces and reconstruction theorems*, Preprint, arxiv: 1001.0223, 2010;

[2] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1992.