UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

Galois points

Alex Freitas de Campos

Tese de Doutorado do Programa de Pós-Graduação em Matemática (PPG-Mat)

ICMC USP SÃO CARLOS

Alex Freitas de Campos

Galois points

Thesis submitted to the Instituto de Ciências Matemáticas e de Computação – ICMC-USP – in accordance with the requirements of the Mathematics Graduate Program, for the degree of Doctor in Science. *EXAMINATION BOARD PRESENTATION COPY*

Concentration Area: Mathematics

Advisor: Prof. Dr. Herivelto Martins Borges Filho

USP – São Carlos
August 2022

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

d198g

de Campos, Alex Freitas
Galois points / Alex Freitas de Campos; orientador Herivelto Martins Borges Filho. -- São Carlos, 2022.
121 p.

Tese (Doutorado - Programa de Pós-Graduação em Matemática) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2022.

1. Algebraic curves. 2. Galois theory. 3. Finite fields. 4. Algebraic function fields. I. Borges Filho, Herivelto Martins, orient. II. Título.

Bibliotecários responsáveis pela estrutura de catalogação da publicação de acordo com a AACR2:
Gláucia Maria Saia Cristianini - CRB - 8/4938
Juliana de Souza Moraes - CRB - 8/6176

Alex Freitas de Campos

Pontos de Galois

Tese apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Doutor em Ciências – Matemática. *EXEMPLAR DE DEFESA*

Área de Concentração: Matemática

Orientador: Prof. Dr. Herivelto Martins Borges Filho

USP – São Carlos
Agosto de 2022

ACKNOWLEDGEMENTS

A realização deste trabalho foi possível graças ao auxílio financeiro do CNPq, identificado sob GM/GD 141676/2019-1, e ao qual sou grato.

ABSTRACT

CAMPOS, A. F. **Galois points**. 2022. 121 p. Tese (Doutorado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2022.

The text with which this thesis is made up may be seen as a unifying reference for some of the most important results about Galois points for plane algebraic curves, a relatively recent research topic, as of the time this thesis was submitted. Emphasis is given to the case of curves over fields of positive characteristic. The core of the work is the classification of curves in terms of the quantity and nature of their Galois points. For smooth curves, such classification was completely obtained around 2012. As opposed, the same enterprise for singular curves does not seem to be so promising, except when we restrict ourselves to the so-called extendable Galois points, which will be studied in detail in this work.

Keywords: Algebraic curves, Galois theory, Algebraic function fields, Finite fields.

RESUMO

CAMPOS, A. F. **Pontos de Galois**. 2022. 121 p. Tese (Doutorado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2022.

O texto que compõe esta tese pode ser encarado como uma referência unificadora de alguns dentre os mais importantes resultados sobre pontos de Galois em curvas algébricas planas, um tópico de pesquisa relativamente recente, partindo de quando esta tese foi apresentada. Ênfase é dada no caso de curvas sobre corpos de característica positiva. O cerne do trabalho é a classificação de curvas em termos das quantidade e natureza de seus pontos de Galois. Para curvas não singulares, tal classificação foi completamente obtida por volta de 2012. Em contrapartida, o mesmo empreendimento para curvas singulares não aparenta ser tão promissor, exceto quando nos restringimos aos assim chamados pontos de Galois extensíveis, que serão estudados detalhadamente neste trabalho.

Palavras-chave: Curvas algébricas, Teoria de Galois, Corpos de funções algébricas, Corpos finitos.

CONTENTS

CHAPTER

1

INTRODUCTION AND SURVEY

The main object of study in the present work is that of a Galois point for **plane** algebraic curves, a concept developed in the late 1990s by Japanese mathematicians Kei Miura and Hisao Yoshihara, which first appeared in (MIURA; YOSHIHARA, 2000). The motivation for the definition of such a concept seems to come from the study of the **gonality** of plane curves (cf. (MIURA; YOSHIHARA, 2000) and (FUKASAWA, 2009, p. 211)). More specifically, and under the hypothesis that the characteristic of the base field is zero, the authors of (MIURA; YOSHIHARA, 2000) were interested in the study of maximal (with respect to inclusion) rational subfields F_{MRat} of an algebraic function field F in one variable. The least degree of the degrees $[F : F_{\mathrm{Mrat}}]$ is the gonality of F. If a plane model C for the curve associated to F is non-singular, then the gonality of F coincides with the gonality of C and any extension F/F_{Mrat} is "realized" as the projection from a point $P \in \mathbb{P}^2$. The authors, then, study the extensions F/F_{MRat} from a geometric point of view, *i.e.*, indirectly via these projections. In particular, they investigated conditions for these extensions to be Galois, which led to the definition of Galois point.

The above emphasis on the word plane was given in order to point out that there do exist analogues of the concept for curves embedded in higher dimensional projective spaces; for instance, for spacial curves (those in $\mathbb{P}^3$) one may consider Galois lines (cf. (DUYAGUIT; YOSHIHARA, 2005)).

The two aspects that influence the most on the overall behavior of Galois points are: the (positivity or not of the) characteristic of the field, an arithmetic aspect, and the singularity or smoothness of the curve, a geometric aspect. Within the scenario of positive characteristic, even characteristic also tends to add another layer of complication to the analysis. As the reader will be able to see in the first chapters, things usually get a bit more complicated in passing from zero to positive characteristic, as well as from smooth to singular curves.

Throughout the text, the results will be presented in an order reflecting this complication of things: in Chapter 3, we will first consider smooth curves over fields of zero characteristic (cf. section 3.1), then smooth curves in positive characteristic (cf. section 3.2). These will further be divided according to the class of the degree of the curve modulo the characteristic (cf. subsection 3.2.2, subsection 3.2.3 and subsection 3.2.4). A special family of curves in even characteristic will have to be considered separately (cf. section 3.3).

Finally, singular curves are studied in Chapter 4. There, we study Galois points under the additional assumption of it being an **extendable** Galois point (cf. Definition 5), and a few novel results are presented (cf. Theorem 8, Theorem 7 and Theorem 9).

This order in the exposition also reflects the actual development of the area.

As for its importance, it is sufficient to say that for smooth curves in arbitrary characteristic a complete classification in terms of the distribution of Galois points was achieved *circa* 2012 (cf. (FUKASAWA, 2013)).

CHAPTER

2

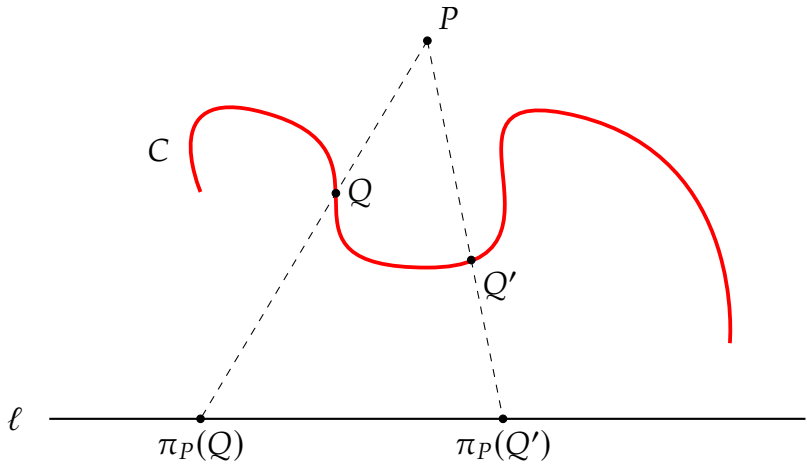
GALOIS POINTS

From now on, the word field will always mean algebraically closed field, and it will be made very clear when not (if ever). We denote a field by k and the finite field by with q elements by $\mathbb{F}_q$, as usual. Similarly, curve is to be understood as projective, plane and geometrically irreducible curve. The capitalized letters X, Y and Z will be used to represent variables for polynomials. We usually make no distinction between a matrix $M \in PGL(3,k)$ and its corresponding projective transformation. Whenever we say automorphism group, we mean full automorphism group.

2.1 Projection from a point

Let $\mathbb{P}^2 = \mathbb{P}^2(k)$ be the projective plane over k. We start with the following

Definition 1. For a point $P \in \mathbb{P}^2$ and a line $\ell \subset \mathbb{P}^2$ not containing P, the map $\pi_{P,\ell} : \mathbb{P}^2 \setminus P \to \ell$ which takes a point Q and sends it to the point $\pi_{P,\ell}(Q) \stackrel{\text{def}}{=} \overline{PQ} \cap \ell$ is called the projection with center P to the line ℓ, or simply projection from P to ℓ.



Given a curve C with degree at least 2, restriction of the projection $\pi_{P,\ell}$ to C gives a dominating rational map from C to ℓ (recall that C has degree at least two and that $\pi_{P,\ell}$ is defined everywhere on C except for, possibly, P). This restriction will be denoted also by $\pi_{P,\ell}$. The induced morphism of function fields, $\pi^*_{P,\ell} : k(\ell) \to k(C)$, allows us to identify $k(\ell)$ with a (rational) subfield of $k(C)$, which will be denoted by $k_P(\ell)$. In other words, given $\pi_{P,\ell}$ and C we obtain an extension of function fields $k(C)/k_P(\ell)$, with $k_P(\ell)$ rational. The degree of such extension is the degree of the rational map $\pi_{P,\ell}$, which, for its turn, equals the cardinality of its generic fiber, except only when C is a strange curve and P is the common point of all tangent lines at non-singular points (we discuss this exception further below). But for a point $Q \in \ell$, we have $\pi^{-1}_{P,\ell}(Q) = \overline{PQ} \cap (C \setminus \{P\})$, and once there is a bijective correspondence between the lines through P and the points in ℓ, it follows that the cardinality of a generic fiber of $\pi_{P,\ell}$ is given by the cardinality of $\ell_P \cap (C \setminus \{P\})$, where ℓ_P is a generic line through P. Finally, an invocation of Bézout's theorem is used to conclude that

$$\deg \pi_{P,\ell} = [k(C) : k_P(\ell)] = \deg C - m_P(C) \tag{2.1}$$

where $m_P(C)$ is the multiplicity of P in C, with the convention that $m_P(C) = 0$ if $P \notin C$. Now, for that exception mentioned earlier, recall that a *strange* curve is a curve for which there exists a point "making" the tangent lines at all non-singular points concurrent; strangeness occurs only in positive characteristic. More about this phenomenon can be learned in (HIRSCHFELD; KORCHMáROS; TORRES, 2013, p. 12). If P, the center of the projection $\pi_{P,\ell}$, coincides with the common point of all tangent lines of a strange curve, (2.1) still holds; the only difference is that, now, the degree of $\pi_{P,\ell}$ won't exactly be the cardinality of the generic fiber. We can take a generic line ℓ to be not any tangent line to C at P and intersecting $C \setminus \{P\}$ only at non-singular points. Then, Bézout's theorem again gives

$$\sum_{Q \in C \setminus \{P\} \cap \ell} I_Q(C \cap \ell) = d - I_P(C \cap \ell) = d - m_P(C) \tag{2.2}$$

And thanks to our choice of ℓ, the left hand side of (2.2) gives the degree of $\pi_{P,\ell}$, even though each of the intersection multiplicities is ≥ 2 (actually $\geq \operatorname{char} k$), for which reason that same left hand side is not the cardinality of $C \setminus \{P\} \cap \ell$. The algebraic aspect behind such behavior is that of inseparability of $k(C)/k_P(\ell)$; separable extensions are almost everywhere unramified, which translates to $I_Q(C \cap \overline{PQ}) = 1$ but for finitely many Q.

In particular, if C is smooth the possibilities given by (2.1) are

$$[k(C) : k_P(\ell)] = \begin{cases} \deg C & \text{if } P \notin C \\ \deg C - 1 & \text{if } P \in C \end{cases} \tag{2.3}$$

With respect to its algebraic properties, and that's all that will concern us, the extension $k(C)/k_P(\ell)$ does not depend on the line ℓ onto which the projection goes. We

just saw, for instance, that its degree depends only upon P. That this is the case can be seen by simply noting that for lines $\ell_1 \neq \ell_2$ not containing P it holds $\pi_{P,\ell_2} \circ \pi_{P,\ell_1} = \pi_{P,\ell_2}$. This implies that the fields $k_P(\ell_1)$ and $k_P(\ell_2)$ are isomorphic subfields of $k(C)$.

We may, thus, speak of the rational subfield k_P of $k(C)$, where k_P can be "realized" via $\pi_{P,\ell}$ for the line ℓ suiting best our needs. Oftentimes $\pi_{P,\ell}$ will also be denoted by π_P only. This, together with the fact that projectively equivalent curves have isomorphic function fields, allows us to always consider, after a projective transformation, $P = (1:0:0)$ and ℓ given by $X = 0$. Before we take a better look at this particular projection, it is time for a definition.

Definition 2. With $P \in \mathbb{P}^2$ and C a curve with degree at least two, the point P will be called a Galois point with respect to C, or a Galois point for C, if the extension $k(C)/k_P$ is a Galois extension. We may also say that P is inner or outer depending on whether $P \in C$ or not.

Now, consider $P = (1:0:0)$ and $\ell : X = 0$. Take any point $Q_0 = (x_0 : y_0 : z_0) \in \mathbb{P}^2$ distinct from P. The line $\overline{PQ}$ is given by $z_0 Y - y_0 Z = 0$ (note that one of y_0 or z_0 is not zero, for otherwise $Q_0 = P$). Its points are P and $(t : y_0 : z_0)$ for any $t \in k$. Therefore $\pi_{P,\ell}(Q) = (0 : y_0 : z_0)$. Suppose $z_0 \neq 0$; moreover, and without loss of generality, suppose $z_0 = 1$. We consider the affine chart $Z \neq 0$, and let $y = Y/Z$ and $x = X/Z$. As y_0 "runs over" k, the functions $y - y_0$ (coming from the lines $Y - y_0 Z = 0$) run over a set of uniformizing parameters for all places of $k(\ell)$, except for the place at infinity (cf. (STICHTENOTH, 2009, Theorem 1.2.2): $k(\ell)$ is rational). The function $y - y_0$ is taken, via $\pi^*_{P,\ell}$, to the same function, but now viewed as a function on the field $k(C)$ (note that none of these functions vanishes in $k(C)$, otherwise C would have a line as a component and, thus, would not be irreducible). The analysis for the pole of y is similar. Therefore, if C is given by the affine equation $f(x, y) = 0$, where x and y generate $k(C)/k$, we see that the extension $k(C)/k_P$ is given by

$$k(x, y)/k(y), \quad \text{with } f(x, y) = 0$$

Remark 1. If $\operatorname{char} k \neq 2$ and if C has degree exactly two, then any point $P \in \mathbb{P}^2$ is a Galois point for C. The reason for it is that $k(C)/k_P$ will always have degree one or two, hence will always be Galois because $\operatorname{char} k \neq 2$. For the same reason, if C is a cubic curve then any point $P \in C$ is a (an inner) Galois point for C.

As was noted when we were considering the degree of $\pi_{P,\ell}$, if C is strange and the center of the projection coincides with the common point of all tangent lines to non-singular points, then $k(C)/k_P$ is not a separable field extension, and hence, under such circumstances P will never be a Galois point for C. In order to avoid any doubts on its truthfulness, what was just asserted will now be proved; but before, notice the

following: we say "**the** common point of all tangent lines" because it is indeed unique (cf. (HIRSCHFELD; KORCHMáROS; TORRES, 2013, Theorem 1.28)). After a projective transformation, we may suppose $P = (1:0:0)$; let also $F = 0$ be the (irreducible) equation of C. The conditions on C and P imply that the polar curve of P with respect to C vanishes. But this amounts to $F_X \equiv 0$, which, for its turn, leads us to conclude that F may be written as ($p = \operatorname{char} k$):

$$F(X,Y,Z) = H_d(Y,Z) + H_{d-p}(Y,Z)X^p + \ldots + H_{d-rp}(Y,Z)X^{rp}$$

where $H_j(Y,Z)$ is homogeneous, on Y and Z only, of degree j. The field extension $k(C)/k_P$ is, therefore, given by $k(x,y)/k(y)$ with x a root of

$$F(T,y,1) = H_d(y,1) + H_{d-p}(y,1)T^p + \ldots + H_{d-rp}(y,1)T^{rp} \in k(y)[T]$$

which is not a separable polynomial, and we are finished. It must be kept in mind that strange curves are all singular, except for conics in characteristic 2 (cf. (BAYER; HEFEZ, 1991) and references therein).

Quite often the condition $\deg C \geq 4$ will be required. Although there is another good reason for such a requirement (cf. the beginning of section 2.3), Remark 1 is enough for a justification as to why not bother with conics and cubics (at least with inner points in cubics).

The following, despite being obvious, will prove to be useful enough to be stated on its own.

Proposition 1. The property of being a Galois point is invariant under projective transformations, *i.e.*, if P is a Galois point for a curve C and T is a projective transformation, then $T(P)$ is a Galois point for $T(C)$.

It is time for us to consider an example.

Example 1. Let $k = \mathbb{C}$ and C be the curve given by $X^d + Y^d + Z^d = 0$, for any $d \geq 3$, *i.e.*, the Fermat curve of degree d. Then $(1:0:0)$ is an outer Galois point for C. Indeed, the corresponding extension is $k(x,y)/k(y)$ with $x^d + y^d + 1 = 0$, and this is a Kummer extension (recall that $\mathbb{C}$ contains all roots of 1): the polynomial $T^d + y^d + 1$ is irreducible in $k(y)[T]$ once $y^d + 1 \neq u^n$ for any $u \in k(y)$ and any divisor $n > 1$ of d ($y^d + 1$ splits into d distinct linear factors in $k[y]$). By considering the permutations of $\{X, Y, Z\}$, which are all projective transformations fixing C, we see that Proposition 1 implies that the points $(0:1:0)$ and $(0:0:1)$ are also outer Galois points for C.

The discussion following the next few lines comes from (MIURA; YOSHIHARA, 2000). Let K/k be an algebraic function field in one variable and denote by $\operatorname{Rat}(K)$ the set of subfields of K that are rational. Any subfield of a rational function field, for which

the corresponding extension is finite, is itself rational; this is known as Lüroth's theorem (cf. (STICHTENOTH, 2009, Proposition 3.5.9)) In view of it, we denote by $\mathrm{MRat}(K)$ the set of those fields L in $\mathrm{Rat}(K)$ such that the extension K/L does not contain any proper intermediate field $F \in \mathrm{Rat}(K)$, *i.e.*, $\mathrm{MRat}(K)$ consist of those fields in $\mathrm{Rat}(K)$ which are maximal with respect to inclusion.

Definition 3. The number

$$\mathrm{gon}(K) = \min\{[K : L] \mid L \in \mathrm{MRat}(K)\}$$

is called the gonality of the function field K.

If $\mathrm{char}\, k = 0$ and $K = k(C)$ is the function field of a smooth plane curve C of degree at least 2, we have that $\mathrm{gon}(k(C)) = \deg C - 1$. Moreover, any rational subfield $L \in \mathrm{MRat}(k(C))$ is "realized" as k_P for some $P \in C$ (see, for example, (NAMBA, 1984, Theorem 5.3.17)). As a consequence the task of describing (inner) Galois points for a smooth curve is equivalent to detecting all the Galois coverings $C \to \mathbb{P}^1$ having minimal degrees (cf. (FUKASAWA; MIURA, 2014, p. 62)).

2.2 The Galois group of a Galois point and its action

Definition 4. If P is a Galois point for a curve C, the Galois group of the extension $k(C)/k_P$ will be denoted by G_P.

Recall that $\pi_P^* : k_P(\ell) \to k_P \subset k(C)$ is an isomorphism of fields. Consider the following subgroup:

$$\mathrm{Aut}_{\pi_P^*}(k(C)) \stackrel{\mathrm{def}}{=} \{\sigma \in \mathrm{Aut}(k(C)) \mid \sigma\pi_P^* = \pi_P^*\} \tag{2.4}$$

It is clear that $G_P = \mathrm{Aut}_{\pi_P^*}(k(C))$. Let us denote by $\hat{\pi} : \hat{C} \to C$ the non-singular model of C and by $\hat{\pi}_P$ the composition $\pi_P \circ \hat{\pi}$. Under the identification $\mathrm{Aut}(k(C)) \simeq \mathrm{Aut}(\hat{C})$, the subgroup of $\mathrm{Aut}(k(C))$ defined in (2.4) corresponds to the following subgroup of $\mathrm{Aut}(\hat{C})$ (cf. (HOMMA, 2006, Definition 2.2)):

$$\mathrm{Aut}_{\hat{\pi}_P}(\hat{C}) \stackrel{\mathrm{def}}{=} \{\sigma \in \mathrm{Aut}(\hat{C}) \mid \hat{\pi}_P\sigma = \hat{\pi}_P\} \tag{2.5}$$

so that $G_P \simeq \mathrm{Aut}_{\hat{\pi}_P}(\hat{C})$. Note that, in case $P \in C$, the condition $\hat{\pi}_P\sigma = \hat{\pi}_P$ implies that σ is a bijection on the set $\hat{C} \setminus \hat{\pi}^{-1}(P)$, because π_P is not defined on P (i.e. $\hat{\pi}_P$ is not defined on $\hat{\pi}^{-1}(P)$). Let $C_{\mathrm{Smooth}} \subset C$ be the open set of all non-singular points of C. Given $\sigma \in \mathrm{Aut}(\hat{C})$, we can define a morphism $\sigma_C : C_{\mathrm{Smooth}} \to C$ as follows

$$\sigma_C(Q) \stackrel{\mathrm{def}}{=} \hat{\pi}(\sigma(\hat{\pi}^{-1}(Q))) \tag{2.6}$$

where $\hat{\pi}^{-1}(Q)$ is the **unique** point of $\hat{C}$ corresponding to $Q \in C_{\text{Smooth}}$. With this in mind, let us see how an element of G_P acts on the points of C_{Smooth}; take $\sigma \in \text{Aut}_{\hat{\pi}_P}(\hat{C})$ and $Q \in C_{\text{Smooth}}$ such that $Q \neq P$. The condition in (2.5), together with (2.6), gives (recall that, once $\sigma \in G_P$, $\sigma(\hat{\pi}^{-1}(Q)) \notin \hat{\pi}^{-1}(P)$)

$$\pi_P(\sigma_C(Q)) = \pi_P(Q) \tag{2.7}$$

The above (2.7) tells us that Q and $\sigma_C(Q)$ lie on the same line through P. To put in another way: σ_C permutes the points of $\ell_P \cap C \setminus \{P\}$ for each line ℓ_P containing P.

We will be mainly concerned with linear automorphisms, *i.e.*, those that come from projective transformations and are represented, as usual, by the elements of the matrix group $PGL(3,k)$. This turns out to be the case, for instance, for the automorphisms of non-singular curves of degree at least four. Indeed, if C is smooth and has degree at least four, then **every** automorphism of C comes from a unique projective transformation, a result to be found in (CHANG, 1978). For singular curves, we will study those points P for which the maps σ_C, where σ runs over the elements of G_P, come from projective transformations, *i.e.*, can be extended to some projective transformation, for which reason they will be called extendable Galois points. The reason for such concern is that any linear automorphism acts also on the tangent lines of C, whereupon geometric constraints will emerge; and in case G_P consists entirely of linear automorphisms, even more can be said.

Lemma 1. Suppose P is a Galois point with respect to a curve C. Let $\sigma \in G_P$ be such that σ_C is the restriction of a projective transformation (which will be denoted by σ_C also) and $C \ni Q(\neq P)$; denote by ℓ the line $\overline{PQ}$. Then $I_Q(C \cap \ell) = I_{\sigma_C(Q)}(C \cap \ell)$. In particular, if ℓ is (the) tangent (resp. transversal) at Q it will also be (the) tangent (resp. transversal) at $\sigma_C(Q)$.

Proof. We denote σ_C by σ only, and maintain this notation from now on. It is sufficient to prove that σ fixes every line through P, for if this is the case then

$$I_Q(C \cap \ell) = I_{\sigma(Q)}(C \cap \sigma(\ell)) = I_{\sigma(Q)}(C \cap \ell),$$

where the first equality holds by the linearity of σ. We now proceed to this proof.

As P is a Galois point for C, P is not the common point of all tangent lines to C (cf. the discussion on page 17), and therefore there is only a finite number of non-singular points of $C \setminus \{P\}$ whose tangent lines pass through P (cf. (HIRSCHFELD; KORCHMáROS; TORRES, 2013, Theorem 1.26)); and since C has infinite non-singular points, there is an infinite number of points Q such that $\overline{PQ}$ intersects C at Q transversally. If the multiplicity of P is $< d-1$, Bézout's theorem implies that there will, then, be infinite lines ℓ through P such that $\ell \cap C \setminus \{P\}$ consists of at least two points. By what

we saw a few lines above, that σ permutes the elements of $\ell \cap C \setminus \{P\}$, we conclude that σ fixes an infinite number of lines passing through P: if ℓ is one of the preceding lines and $Q \neq Q' \in \ell \cap C \setminus \{P\}$, then

$$\ell = \overline{QQ'} = \overline{\sigma(Q)\sigma(Q')} = \sigma(\ell)$$

This, for its turn, leads to σ fixing **all** lines through P. Now, if the multiplicity of P is $d-1$, the same conclusion holds: there will be infinite lines ℓ through P such that $\ell \cap C \setminus \{P\}$ consists of a single point, which will be fixed by σ. But P will also be fixed by σ: for otherwise, σ being linear, $\sigma(P)$ would be another point of C with multiplicity $d-1$; but for any curve there is at most one such point. Hence we have, again, that σ fixes an infinite number of lines passing through P, which assures **every** line through P is fixed. Note that in this last case, σ will be the identity once it fixes four points such that no three of them are collinear. In fact, $|G_P| = d - m_P = d - (d-1) = 1$ (cf. (2.1)).

□

If $\sigma \in G_P$ is not linear, a weaker version of Lemma 1 still holds. It goes as follows.

Lemma 2. Let C and P be as in Lemma 1. If Q_1 and $Q_2 \in C \setminus \{P\}$ are **non-singular** points of C lying on the same line ℓ through P, *i.e.*, with $\pi_P(Q_1) = \pi_P(Q_2)$, then

$$I_{Q_1}(C \cap \ell) = I_{Q_2}(C \cap \ell) \tag{2.8}$$

Proof. Let $\hat{\pi} : \hat{C} \to C$ be the non-singular model of C and denote by $\hat{\pi}_P$ the composition $\pi_P \circ \hat{\pi}$, as before. For $Q \in C \setminus \{P\}$ and $q \overset{\text{def}}{=} \pi_P(Q)$, G_P acts transitively on the set $\hat{\pi}_P^{-1}(q) = \{\hat{Q}_1, \ldots, \hat{Q}_s\}$, because $k(C) = k(\hat{C})/k_P$ is a Galois extension (cf. (STICHTENOTH, 2009, Theorem 3.7.1)). Moreover, the ramification indices $e(\hat{Q}_i)$ are all the same (cf. (STICHTENOTH, 2009, Corollary 3.7.2)), and we denote it by $e(q)$ only, so that it holds $s \cdot e(q) = \deg \pi_P$. When Q is non-singular, $\hat{\pi}^{-1}(Q) = \{\hat{Q}\}$ consists of a single linear branch, and the ramification index $e(\hat{\pi}_P(\hat{Q}))$ will be just $I_Q(C \cap \overline{PQ})$, for the line $\overline{PQ}$ gives a uniformizing parameter (on the line we are projecting C, *i.e.*, on the image of π_P) at q. But this is exactly what (2.8) says.

□

Remark 2. With C and P still satisfying the above conditions, a generic line ℓ through P will be such that $C \cap \ell$ consists entirely of non-singular points, and ℓ will intersect them all transversally, if C is not strange. Another thing that must be pointed out is that it is useful to think of Lemma 2 as a means of testing the possibility of P to be a Galois point. Indeed, suppose there is a line ℓ through P such that there are two non-singular points Q_1 and $Q_2 \in \ell \cap C \setminus \{P\}$ such that $I_{Q_1}(C \cap \ell) \neq I_{Q_2}(C \cap \ell)$, which is the case, for example, if ℓ intersects transversally one of them and is tangent at the other. Then Lemma 2 implies that P **is not** a Galois point for C.

Back to the scenario of Lemma 1, the projective transformation corresponding to σ can be easily characterized, as we are now going to check. Without loss of generality, we may suppose $P = (1:0:0)$ is the Galois point for C. Take $\sigma \in G_P$ such that the corresponding automorphism of C is the restriction of a projective transformation represented by the following matrix

$$A_\sigma = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

The projective transformation A_σ above leaves invariant every line through P (cf. the proof of Lemma 1). These lines are all given by an equation like $\alpha Y + \beta Z = 0$, for some pair $(\alpha, \beta) \neq (0,0)$. That A_σ leaves each of these lines invariant is equivalent to the following equations

$$\begin{cases} \alpha a_{21} + \beta a_{31} = 0 \\ \alpha a_{22} + \beta a_{32} = s\alpha \\ \alpha a_{23} + \beta a_{33} = s\beta \end{cases} \quad \text{for some } s \neq 0 \text{ and every } (\alpha, \beta) \neq (0,0)$$

Taking $\alpha = 1$ and $\beta = 0$, for instance, we conclude that $a_{21} = 0 = a_{23}$. Note that this choice of α and β corresponds to the line $Y = 0$. Swapping the previous values, we obtain $a_{31} = 0 = a_{32}$. Finally, for $\alpha = 1 = \beta$, $a_{22} = a_{33}$, which we may consider to be 1, for $A_\sigma \in PGL(3,k)$. Below we sum all this up.

Lemma 3. Under the same hypothesis of Lemma 1, if $A_\sigma \in PGL(3,k)$ is a projective transformation extending $\sigma \in G_P$, where $P = (1:0:0)$, then

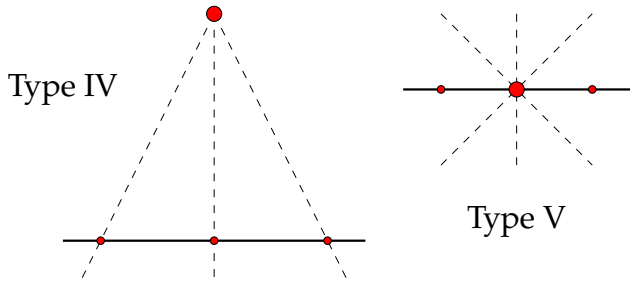
$$A_\sigma = \begin{pmatrix} a & b & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Moreover, all powers of σ have extensions to projective transformations too, and it is easy to see that $A_{\sigma^n} = A_\sigma^n$. Once G_P has finite order, σ has equally so, say k, and the last equality implies that a must be a k-th root of 1.

To Lemma 3 is attributable the title of "cornerstone of this work": it is the crucial result used to determine the structure of G_P and the equation of C (under projective equivalence) in the case of an extendable Galois point P (cf. Theorem 3). Almost all else will make use of such information.

Remark 3. Any projective transformation of the plane is fully determined (for all $p \neq 2$) according to its *invariant figure*; for an account of such classification, we refer to (MITCHELL, 1911). There are five types of invariant figures, and we will assign to any transformation the same type of the figure it leaves invariant. Amid these five, only

two, which correspond to types IV and V in (MITCHELL, 1911, § 2), contain every line through a point, *i.e.*, they fix every line through a point P and, additionally, those of type IV fix all points on a line *not passing* through P, while those of type V fix all points on a line *passing* through P.



Within this context, what we did in the proof of Lemma 1 was to show that if $\sigma \in G_P$ can be extended to a projective transformation, then this will be of type IV or of type V. But those of type V do not have finite order if $\operatorname{char} k = 0$. Moreover, if $\operatorname{char} k = p > 0$ (and we may not worry about $p \neq 2$ for this restriction applies only to the transformations of type III), then all transformations of type V have order p. These transformations are explicitly given, in terms of their matrices (and upon conjugation by a suitable matrix; notice that conjugated transformations leave the same figure invariant), as

$$A_{\alpha,IV} = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad A_V = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where $\alpha \neq 0$. With the above representation, it is clear that $A_{\alpha,IV}$ fixes every line through $P = (1:0:0)$ and every point in the line $X = 0$, which does not contain P; moreover, it will have finite order if, and only if, α is a root of 1. As for A_V, it again fixes every line through $P = (1:0:0)$, but as opposed to the former, it now fixes every point in the line $Y + Z = 0$, which does contain P. Compare with Lemma 3.

We finish this section by stating two results concerning unusual behavior exhibited exclusively by (some) strange curves. In (FUKASAWA; HASEGAWA, 2010) the following characterization is shown.

Theorem 1. Let C be a curve of degree ≥ 4 and denote by Δ the set of all inner Galois points for C. Then Δ is a non-empty (Zariski) open set of C if, and only if, $\operatorname{char} k = p > 0$ and C is projectively equivalent to the curve given by $ZX^{q-1} - Y^q = 0$, for a power q of p.

The curve C_S given by $ZX^{q-1} - Y^q = 0$ as in Theorem 1 above, is a strange curve. The point $Q = (0:1:0)$ is the common point of all tangent lines at non-singular points. It is also a rational curve: its only singular point $P = (0:0:1)$ has multiplicity a unit less

than its degree. We indicate, and the reader is invited to take a look at (FUKASAWA; HASEGAWA, 2010) for the proofs, that

- **every** point of C_S is an inner Galois point for it (note that projection from P, the only singular point, yields a birational morphism between C_S and a line), whose Galois group is cyclic and
- **every** point in the line $Z = 0$ different from P and Q is an outer Galois point, whose Galois group is elementary abelian of exponent p. Also
- the condition "Δ is a non-empty open set of C" in Theorem 1 may be weakened to "Δ is an infinite set of C".

Let us denote by Δ' the set of outer Galois points for a curve C. The other work following the same lines as before, (FUKASAWA, 2011), states, among other things, what follows.

Theorem 2. Within the scenario set up in Theorem 1, Δ' is an infinite set if, and only if, C is a rational strange curve such that there is a line containing infinite outer Galois points and passing through the common point of all tangent lines at non-singular points.

The characterizations given by Theorem 1 and Theorem 2 fully answer the question of which curves admit infinite Galois points: they are all strange and rational. For $\operatorname{char} k = 0$ and non-singular curves, the quantity of Galois points is not only finite but bounded by 4 (for inner Galois points) and by 3 (for outer Galois points). For positive characteristic, and still restricting ourselves to non-singular curves, the quantity will always be finite too, and a similar boundedness will hold for "almost all" curves.

2.3 Extendable Galois points

In the case of a smooth curve C of degree $d \geq 4$, any automorphism of C is the restriction of some projective transformation of $\mathbb{P}^2$ (cf. (CHANG, 1978) and (ARBARELLO *et al.*, 2010, Appendix A, 17 and 18)). For an arbitrary irreducible curve C we have the following definition, which was first considered in (YOSHIHARA, 2009).

Definition 5. Let C be a curve of degree $d \geq 3$ and let $P \in \mathbb{P}^2$ be a Galois point with respect to C, with Galois group G_P. We will call the point P an extendable Galois point if for any $\sigma \in G_P$, the corresponding morphism σ_C (cf. (2.6)) of C extends to a projective transformation of $\mathbb{P}^2$.

Remark 4. 1. As was noted in the beginning of this section, for a smooth curve of degree $d \geq 4$ any Galois point is extendable.

2. It is also obvious that for $d = 2$ any automorphism is linear, once the curve is rational in this case. That is why we considered only $d \geq 3$ in Definition 5.

3. If C is a curve of degree $d \geq 2$ and $\phi : C \to C$ is an automorphism that extends to some projective transformation T_ϕ, then this projective transformation is unique. Indeed let T_1 and T_2 be two projective transformations extending ϕ. Then $T_1 T_2^{-1}$ extends $\phi\phi^{-1} = \mathrm{id}_C$. But then, as id_C fixes a set of four distinct points of C such that no three of them are collinear, $T_1 T_2^{-1} = \mathrm{Id}$, *i.e.*, $T_1 = T_2$.

Our next result unifies, but in no way generalizes, a handful of results appearing throughout distinct works; among them we cite (YOSHIHARA, 2001, Theorems 4, 4' and Propositions 5, 5'), (FUKASAWA, 2007, Theorem 2) and (YOSHIHARA, 2009, Lemma 1 and Proposition 1). If the curve C admits an extendable Galois point P, then its equation and corresponding Galois group are characterized by the following

Theorem 3. Let C be a curve of degree $d \geq 3$ in characteristic $p \geq 0$. Suppose P is an extendable Galois point for C with multiplicity m and Galois group G_P. Then it holds what comes below.

1. If $p = 0$ or $p > 0$ and $p \nmid (d - m)$, then G_P is cyclic. Moreover, C is projectively equivalent to the curve given by $G_m(Y, Z)X^{d-m} + G_d(Y, Z) = 0$, where $G_m(Y, Z)$ and $G_d(Y, Z)$ are homogeneous polynomials of degree m and d, respectively, $P = (1 : 0 : 0)$ and a generator for G_P is given by the matrix $\mathrm{diag}(\zeta_{d-m}, 1, 1)$. Conversely, if C is given by an irreducible equation like the previous one, then $(1 : 0 : 0)$ is an m-fold extendable Galois point for C whose Galois group is cyclic and generated by $\mathrm{diag}(\zeta_{d-m}, 1, 1)$.

2. If $p > 0$ and $p \mid (d - m)$, then, writing $d - m = p^e l$ where $p \nmid l$, G_P is isomorphic to $(\oplus^e \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/l\mathbb{Z}$. Moreover, $l \mid (p^e - 1)$ and C is projectively equivalent to the curve given by $G_m(Y, Z) f(X, Y, Z)^l + G_d(Y, Z) = 0$, where $G_m(Y, Z)$ and $G_d(Y, Z)$ are homogeneous polynomials of degree m and d respectively, and $f(T, y, 1) \in k[y][T]$ is an additive separable polynomial of degree p^e whose roots are linear polynomials in y with coefficients in some finite extension of $\mathbb{F}_p$, and $P = (1 : 0 : 0)$. Conversely, if C is given by an irreducible equation like the previous one, with $l \mid (p^e - 1)$, then $(1 : 0 : 0)$ is an m-fold extendable Galois point for C whose Galois group is (isomorphic to) $(\oplus^e \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/l\mathbb{Z}$.

Proof. After a projective transformation, we may suppose that $P = (1 : 0 : 0)$. The projection π_P has degree $d - m$, so that the order of G_P is, by assumption, $d - m$. Take $\sigma \in G_P$. Once P is extendable, let $A_\sigma = (a_{ij}) \in PGL(3, k)$ be a matrix representing the projectivity

associated to σ (it is unique, cf. item 3 of Remark 4). By Lemma 3, we have that

$$A_\sigma = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{2.9}$$

Lemma 3 also tells us that a_{11} is a k-th root of 1, for some $k \mid (d-m)$, by Lagrange's theorem. Consider the following map

$$\psi : \begin{cases} G_P & \to & k^\times \\ \sigma & \mapsto & a_{11} \end{cases} \tag{2.10}$$

It is well defined since the association $\sigma \mapsto A_\sigma$ is injective and we have fixed $a_{22} = 1 = a_{33}$, so that the a_{11} appearing in (2.9) is uniquely determined by σ. It is obvious that ψ is a group homomorphism (ψ is simply the determinant of A_σ).

If $\operatorname{char} k = 0$, then ψ is injective. Indeed, if $a_{11} = 1$, then

$$A_\sigma^s = \begin{pmatrix} 1 & s \cdot a_{12} & s \cdot a_{13} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and once the order of σ divides $d-m$, the same holds all the more so for A_σ, so that $(d-m)\cdot a_{12} = 0 = (d-m)\cdot a_{13}$, which is possible, once $\operatorname{char} k = 0$, if and only if $a_{12} = 0 = a_{13}$, *i.e.*, if and only if A_σ is the identity matrix. This same reasoning applies if $\operatorname{char} k = p > 0$, provided that $p \nmid (d-m)$. In both cases the group G_P is cyclic, for it is isomorphic to a finite subgroup of the multiplicative group of the field k. A generator for G_P is $\sigma \in G_P$ such that $a_{11} = \zeta_{d-m}$ is a primitive $(d-m)$-th root of unity. We note that in this case A_σ is diagonalizable [1]. Moreover, there exists a matrix Q that fixes $P = (1:0:0)$ and diagonalizes A_σ: just take

$$Q = \begin{pmatrix} 1 & -a_{12}/(\zeta_{d-m}-1) & -a_{13}/(\zeta_{d-m}-1) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

So, in item 1 we can suppose not only that the Galois point P is $(1:0:0)$, but that a generator for G_P is given by the following matrix (recall that the elements of $\operatorname{Aut}(C)$ and those of $\operatorname{Aut}(Q(C))$ are conjugated, by Q, of one another):

$$Q^{-1} A_\sigma Q = \begin{pmatrix} \zeta_{d-m} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

[1] Recall that if $\lambda_1, \ldots, \lambda_k$ are the *distinct* eigenvalues of a matrix A, then A is diagonalizable if, and only if, the matrix $(A - \lambda_1 \mathrm{id}) \ldots (A - \lambda_k \mathrm{id})$ is the zero matrix.

Hence, to the projection π_P there corresponds a Kummer extension $k(x,y)/k(y)$, whose Galois group is generated by the automorphism $\sigma(x) = \zeta_{d-m}x$. Therefore, $x^{d-m} = f(y)/g(y)$, with f and g polynomials in y without common factors, and the curve has (affine) equation

$$g(Y)X^{d-m} - f(Y) = 0 \tag{2.11}$$

Indeed, the function $g(y)x^{d-m} - f(y)$ is regular and vanishes everywhere on C. Therefore $F(X,Y)$ divides $g(Y)X^{d-m} - f(Y)$, where $F(X,Y) = 0$ is the (irreducible) equation of C. But $g(Y)X^{d-m} - f(Y)$ is itself irreducible, otherwise $k(x,y)/k(y)$ would have degree less than $d-m$. Hence (2.11) is the equation of C. Note that, since C has degree d, $g(Y)$ has degree $\leq m$, $f(Y)$ has degree $\leq d$ and at least one of the previous bounds is attained (otherwise the curve would not be irreducible: it would contain the line $Z = 0$). As the converse is just a matter of routine algebraic verifications, we are done proving item 1.

Back to the homomorphism in (2.10), if $\operatorname{char} k = p > 0$ and $p \mid (d-m)$, then ψ may, and it most certainly will, have nontrivial kernel. We notice that any matrix belonging to $\operatorname{Ker}(\psi)$ satisfies $a_{11} = 1$, *i.e.*, it has the following form:

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

The set of all matrices having the above form constitute an abelian subgroup of $PGL(3,k)$, and they all have order $p = \operatorname{char} k$. By the fundamental theorem on finitely generated abelian groups we have that $\operatorname{Ker}(\psi) \simeq \oplus^{e'}\mathbb{Z}/p\mathbb{Z}$, for some $e' \leq e$ (recall that $|G_P| = d - m = p^e l$, with $p \nmid l$). For $\sigma \in G_P$, we have that $\sigma^{p^e l} = 1$, hence $A_\sigma^{p^e l} = 1$, which implies that $a_{11}^{p^e l} = 1$, and finally that $a_{11}^l = 1$. So, for any $\sigma \in G_P$, we have that $\sigma^l \in \operatorname{Ker}(\psi)$. This implies that $\operatorname{Ker}(\psi)$ is nontrivial, for otherwise all elements in G_P would have order l or a divisor of l, which is in contradiction with Cauchy's theorem: $p \mid |G_P|$ implies that there is an element whose order is p.

We also know that $\operatorname{Im}(\psi) \simeq G_P/\operatorname{Ker}(\psi)$ is cyclic because it is a finite subgroup of $k^\times$. Therefore, there are at most l elements in the quotient group $G_P/\operatorname{Ker}(\psi) \simeq \operatorname{Im}(\psi)$. Denote by l' the order of $\operatorname{Im}(\psi)$. We have that $p^e l = |G_P| = |\operatorname{Ker}(\psi)||\operatorname{Im}(\psi)| = p^{e'} l' \leq p^{e'} l$, so that $e' \geq e$, and therefore $e' = e$. It then follows that $l = l'$. Take $\sigma \in G_P$ such that the powers of σ form a set of representatives for the cosets of $\operatorname{Ker}(\psi)$ in G_P. We then have that $\sigma^i \notin \operatorname{Ker}(\psi)$ for $i = 1, \ldots, l-1$ and $\sigma^l \in \operatorname{Ker}(\psi)$. Consider the homomorphism

$$\iota : \begin{cases} \mathbb{Z}/l\mathbb{Z} & \to & G_P \\ \bar{s} & \mapsto & \sigma^s \end{cases}$$

The quotient homomorphism (which is induced by ψ) $q : G_P \to \mathbb{Z}/l\mathbb{Z}$ is simply given by $\phi \mapsto s$, where s the unique positive integer $\leq l-1$ such that $\phi \in \sigma^s \operatorname{Ker}(\psi)$. It is clear that

$q \circ \iota = \mathrm{id}$. Therefore the following exact sequence splits

$$1 \to \oplus^e \mathbb{Z}/p\mathbb{Z} \hookrightarrow G_P \xrightarrow{q} \mathbb{Z}/l\mathbb{Z} \to 1$$

and we can finally conclude that

$$G_P \simeq \left(\bigoplus_{i=1}^{e} \frac{\mathbb{Z}}{p\mathbb{Z}} \right) \rtimes \frac{\mathbb{Z}}{l\mathbb{Z}}$$

If $l \neq 1$, we may proceed as we did in item 1 and suppose, without loss of generality, that a generator τ for $C_l \overset{\text{def}}{=} \mathbb{Z}/l\mathbb{Z} \leq G_P$ is given by the following matrix

$$D_\tau = \begin{pmatrix} \zeta_l & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{2.12}$$

where ζ_l is a primitive l-th root of unity. Indeed, a generator for C_l is given by a matrix of the following form:

$$A_\tau = \begin{pmatrix} \zeta_l & a_\tau & b_\tau \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

which is diagonalizable (cf. the footnote at page 26). As before, the projective transformation given by

$$T_\tau = \begin{pmatrix} 1 & -a_\tau/(\zeta_l - 1) & -b_\tau/(\zeta_l - 1) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{2.13}$$

fixes the Galois point $P = (1 : 0 : 0)$ and diagonalizes A_τ. Moreover, once T_τ is a matrix of the same form as those in $\mathrm{Ker}(\psi)$, and all the matrices of this particular form commute with one another, it follows conjugation by T_τ leaves the matrices in $\mathrm{Ker}(\psi)$ unchanged.

The extension associated to π_P is thus $k(x, y)/k(y)$, with Galois group as above. Notice that if $l \geq 2$, then G_P is not abelian. The subgroup $\mathrm{Ker}(\psi)$ has the following $\mathbb{F}_p$-vector space structure (cf. page 85): addition is given by matrix multiplication, and scalar multiplication is given by multiplication of the off diagonal elements by the given scalar, which is the same as exponentiating the matrix by the given scalar. We have that $\dim_{\mathbb{F}_p} \mathrm{Ker}(\psi) = e$. But we can actually define an $\mathbb{F}_p(\zeta_l)$-vector space structure in it. Indeed, taking D_τ a generator for $\mathbb{Z}/l\mathbb{Z}$ as before (cf. (2.12)) and $A_\sigma \in \mathrm{Ker}(\psi)$, we have that

$$D_\tau A_\sigma D_\tau^{-1} = \begin{pmatrix} 1 & \zeta_l a & \zeta_l b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

which belongs to $\mathrm{Ker}(\psi)$. So that after defining addition and multiplication by a scalar $f(\zeta_l) \in \mathbb{F}_p(\zeta_l)$ as before, $\mathrm{Ker}(\psi)$ is endowed with an $\mathbb{F}_p(\zeta_l)$-vector space structure. Let

$\lambda \stackrel{\text{def}}{=} [\mathbb{F}_p(\zeta_l) : \mathbb{F}_p]$, which coincides with the order of p in the group $(\mathbb{Z}/l\mathbb{Z})^\times$ (recall that a finite extension of finite fields is **always** cyclic with Galois group generated by the Frobenius automorphism). Let also $s \stackrel{\text{def}}{=} \dim_{\mathbb{F}_p(\zeta_l)} \text{Ker}(\psi)$. We have that

$$p^e = |\text{Ker}(\psi)| = |\mathbb{F}_p(\zeta_l)|^s = (|\mathbb{F}_p|^\lambda)^s = p^{\lambda s}$$

or, in other words, λ divides e. But once λ is the order of p in $(\mathbb{Z}/l\mathbb{Z})^\times$, we have that $p^\lambda \equiv 1 \bmod l$, so that $p^e \equiv 1 \bmod l$ too. Equivalently: $l \mid (p^e - 1)$. If $l \mid (p^e - 1)$ it is obvious that λ divides e.

Consider now the normal subgroup $C_p^e \stackrel{\text{def}}{=} \oplus^e(\mathbb{Z}/p\mathbb{Z}) \lhd G_P$, that is, $\text{Ker}(\psi)$. By the fundamental theorem of Galois theory, the extension $k(x,y)^{C_p^e}/k(y)$ is a Galois extension with Galois group (isomorphic to) $G_P/C_p^e \simeq C_l$.

$$\begin{array}{c} k(x,y) \\ \Big| \; C_p^e \\ k(x,y)^{C_p^e} \\ \Big| \; C_l \\ k(y) \end{array}$$

Let us give an explicit description of the field $k(x,y)^{C_p^e}$: the fixed field by C_p^e. We will denote a matrix

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in C_p^e$$

and the associated automorphism of $k(C) = k(x,y)$ by $\sigma_{a,b}$. Its action is given by $\sigma_{a,b}(x) = x + ay + b$. As was noted before, C_p^e is an e-dimensional $\mathbb{F}_p$-vector space. Choose a basis $\sigma_{a_1,b_1}, \ldots, \sigma_{a_e,b_e}$. Then, any element in C_p^e is uniquely written as

$$\sigma_{a,b} = \sigma_{a_1,b_1}^{\mu_1} \circ \ldots \circ \sigma_{a_e,b_e}^{\mu_e}$$

for some $(\mu_1, \ldots, \mu_e) \in \mathbb{F}_p^e$. Remember that the $\sigma_{a,b}$'s all commute, so the order of the above composition is irrelevant. We can then write

$$\prod_{\sigma_{a,b} \in C_p^e} \sigma_{a,b}(x) = \prod_{(\mu_1,\ldots,\mu_e) \in \oplus^e \mathbb{F}_p} (\sigma_{a_1,b_1}^{\mu_1} \circ \ldots \circ \sigma_{a_e,b_e}^{\mu_e})(x)$$

for the norm of x relative to the extension $k(x,y)/k(x,y)^{C_p^e}$. But

$$(\sigma_{a_1,b_1}^{\mu_1} \circ \ldots \circ \sigma_{a_e,b_e}^{\mu_e})(x) = x + \sum_{i=1}^{e} \mu_i(a_i y + b_i)$$

so that

$$f(x,y)=\prod_{(\mu_1,\dots,\mu_e)\in\oplus^e\mathbb{F}_p}\left(x+\sum_{i=1}^{e}\mu_i(a_iy+b_i)\right)$$

is the norm of x. Note that $f(T,y)\in k(y)[T]$ is an additive separable polynomial of degree p^e such that its roots are all linear polynomials in y with coefficients in some finite extension of $\mathbb{F}_p$. This also gives us the description we were looking for: $k(x,y)^{C_p^e}=k(f(x,y),y)$. The automorphisms from the quotient group G_P/C_p^e act by taking x to $\zeta_l^i x$. Hence the norm of $f(x,y)$ relative to the extension $k(x,y)^{C_p^e}/k(y)$ is simply

$$\hat{f}(x,y)=\prod_{i=0}^{l-1}f(\zeta_l^i x,y)$$

Note that the element $\hat{f}(x,y)$ is now fixed by all of G_P: it is the norm of x relative to the extension $k(x,y)/k(y)$. We can simplify the above expression. As we already saw, there is an $\mathbb{F}_p(\zeta_l)$-vector space structure in C_p^e. In particular, the association $\sigma_{a,b}\mapsto\zeta_l^i\sigma_{a,b}=\sigma_{\zeta_l^i a,\zeta_l^i b}$ is an $\mathbb{F}_p(\zeta_l)$-automorphism of C_p^e for all $1\le i\le l-1$. Hence

$$\begin{aligned}
f(\zeta_l^j x,y)&=\prod_{(\mu_1,\dots,\mu_e)\in\oplus^e\mathbb{F}_p}\left(\zeta_l^j x+\sum_{i=1}^{e}\mu_i(a_iy+b_i)\right)\\
&=\zeta_l^{jp^e}\prod_{(\mu_1,\dots,\mu_e)\in\oplus^e\mathbb{F}_p}\left(x+\sum_{i=1}^{e}\mu_i(\zeta_l^{-j}a_iy+\zeta_l^{-j}b_i)\right)\\
&=\zeta_l^{(p^e-1)j}\zeta_l^j\prod_{(\mu_1,\dots,\mu_e)\in\oplus^e\mathbb{F}_p}\left(x+\sum_{i=1}^{e}\mu_i(a_iy+b_i)\right)\\
&=\zeta_l^j f(x,y)
\end{aligned}$$

for all $1\le j\le l-1$. Therefore $\hat{f}(x,y)=\left(\prod_{i=0}^{l-1}\zeta_l^i\right)f(x,y)^l=(-1)^{l-1}f(x,y)^l$. Note that, once $k(x,y)^{C_p^e}/k(y)$ is a degree l cyclic extension, with l and $\operatorname{char}k$ coprime, it is a Kummer extension. Being so, there exists an element $\tilde{x}\in k(f(x,y),y)\setminus k(y)$ such that $k(f(x,y),y)=k(\tilde{x},y)$ and $\tilde{x}^l\in k(y)$. We just found such an $\tilde{x}$: $f(x,y)$ itself! This gives us a description for both the original curve C and for the quotient curve C/C_p^e. Let's see. Once $f(x,y)^l\in k(y)$, write $f(x,y)^l=\alpha(y)/\beta(y)$ with $\alpha(y)$ and $\beta(y)\in k[y]$ without common factors. Then C has (affine) equation

$$\beta(Y)f(X,Y)^l-\alpha(Y)=0 \tag{2.14}$$

The reason is the same as before: the function $\beta(y)f(x,y)^l-\alpha(y)$ vanishes everywhere on C and is irreducible once $f(T,y)^l-\alpha(y)/\beta(y)$ is the minimal polynomial of x in $k(y)$.

We point out that, as in item 1, $\alpha(y)$, resp. $\beta(y)$, has degree $\le d$, resp. $\le m$, and either $\alpha(y)$ has degree d or $\beta(y)$ has degree m. The quotient curve C/C_p^e, for its turn, has affine equation

$$\beta(y)x^l + \alpha(y) = 0$$

Conversely, if C is given by the (2.14) above, with $d - m = p^e l$ and $l \mid (p^e - 1)$, where $\beta(y)$, $\alpha(y)$ and $f(T, y)$ are as before, it is again a matter of (somehow cumbersome) verification to see that the extension $k(x, y)/k(y)$ is Galois whose automorphisms are, as before, linear, hence the point $(1 : 0 : 0)$ is an m-fold extendable Galois point.

□

We state the result just proved for the curve corresponding to the intermediate field $k(x, y)^{C_p^e}$ more explicitly.

Proposition 2. For a curve C as in item 2 of Theorem 3, the quotient curve C/C_p^e, where $C_p^e \simeq \oplus^e \mathbb{Z}/p\mathbb{Z}$ is the "kernel" of G_P, is projectively equivalent to the curve given by the following affine equation

$$g_m(y)x^l + g_d(y) = 0$$

where $g_m(y) = G_m(y, 1)$ and $g_d(y) = G_d(y, 1)$.

Remark 5. We draw the reader's attention to the following observations regarding Theorem 3.

1. As we saw, for smooth curves of degree $d \geq 4$ any Galois point is extendable, so we can use Theorem 3 to decide whether C has Galois points if we also know its automorphism group. More specifically, and restricting ourselves to $p = 0$, if we know that $\mathrm{Aut}(C)$ does not have any cyclic subgroup of order d (resp. $d - 1$), then C cannot have any outer Galois point (resp. any inner Galois point). For example, for any three **distinct** elements α, β and $\gamma \in k$ the following quartic curve in characteristic 0

   $$X^4 + Y^4 + Z^4 + \alpha X^2Y^2 + \beta X^2Z^2 + \gamma Y^2Z^2 = 0$$

   is non-singular and has the Klein four-group as its automorphism group (cf. section 2.5). Hence it does not have any Galois points at all.

2. In item 2, the divisibility condition $l \mid (p^e - 1)$ can also be used to decide whether C has an m-fold extendable Galois point: if $d - m = p^e l$ with $p \nmid l$ **and** $l \nmid (p^e - 1)$, then there cannot exist an m-fold extendable Galois point for C. For instance, if C is a degree 15 curve in characteristic 3, then, once $5 \nmid (3 - 1)$, C does not have any extendable **outer** Galois point. More generally, if $d - m = p \cdot l$ with $l > p$, then no curve of degree d has a Galois point of multiplicity m. Nevertheless, for every pair $(e, l) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 1}$ such that $p \nmid l$ and $l \mid (p^e - 1)$ there exist non-singular plane curves C and C' such that C has degree $p^e l + 1$ and an inner Galois point and C' has degree $p^e l$ and an outer Galois point (cf. (FUKASAWA, 2007, Example 1)).

3. It is necessary, but not sufficient, that the polynomials $G_m(Y,Z)$ and $G_d(Y,Z)$ be coprime in order for the curves in Theorem 3 to be irreducible. As an example, if we take $G_2(Y,Z) = Z^2$ and $G_{20}(Y,Z) = (Y+Z)^{20}$, then the following curve in characteristic 3

$$Z^2(X^9 - X(Y+Z)^8)^2 + (Y+Z)^{20} = 0$$

has equation like the one in item 2, and satisfies the divisibility condition $l|(p^e-1)$ (which, in this case, reduces to $2|(3^2-1)$). But this curve is reducible (over $\mathbb{F}_9$), once it is a difference of two squares, even though G_2 and G_{20} do not share any common factor. Indeed, denoting by s a square root of 2 in $\mathbb{F}_9$, we have that

$$\begin{aligned}
&Z^2(X^9 - X(Y+Z)^8)^2 + (Y+Z)^{20} = \\
&(Z(X^9 - X(Y+Z)^8))^2 - (s(Y+Z)^{10})^2 = \\
&(Z(X^9 - X(Y+Z)^8) - s(Y+Z)^{10}) \cdot (Z(X^9 - X(Y+Z)^8) + s(Y+Z)^{10})
\end{aligned}$$

The reader is invited to take a look at (DEOLALIKAR, 2002) for an irreducibility criterion that contemplates the case $l = 1$.

4. There are curves admitting non-extendable Galois points; any such curve will necessarily be singular. The following example is due to Kei Miura (cf. (YOSHIHARA, 2001, Remark 1)). Let $k = \mathbb{C}$ and C_n be the degree $2n+1$ curve with the following (affine) equation

$$C_n : yx^{2n} + (y^{n+1}+1)x^n + y(y^2+1)^n = 0$$

This curve is singular (for example, the points $(0 : \pm i : 1)$ are singular). The point $(1:0:0) \in C_n$ is non-singular, and we now show that it is a Galois point for it. The corresponding field extension is (cf. the discussion after Definition 2 at page 17) $k(x,y)/k(y)$, where x is a root of

$$p(T) \stackrel{\text{def}}{=} yT^{2n} + (y^{n+1}+1)T^n + y(y^2+1)^n \in k(y)[T]$$

The polynomial $p(T)$ is separable. Its irreducibility will be shown after a few considerations (it does not follow directly from the irreducibility criterion *à la* Eisenstein given in (STICHTENOTH, 2009, Proposition 3.1.15)). Let r_1 be any of its roots. Then $r_2 \stackrel{\text{def}}{=} (y^2+1)/r_1$ is also a root, and the set of all roots of $p(T)$ is $\{\zeta_n^i r_j \mid i = 0,\ldots,n-1 \text{ and } j = 1,2\}$, ζ_n being a primitive n-th root of 1 ($\zeta_n = \exp(2\pi i/n)$, for instance). From these considerations we see that the extension is normal (recall that $k = \mathbb{C}$ contains all roots of 1), and therefore Galois of degree $2n$, provided that we show $p(T)$ is irreducible. By what we just saw, it suffices to show that $p(T)$ does not have any root in $k(y)$. Suppose, for us to obtain a contradiction, that $p(\varphi) = 0$ for some $\varphi \in k(y)$. Then

$$y\varphi^{2n} + (y^{n+1}+1)\varphi^n = -y(y^2+1)^n$$

Considering the values on both sides of the equation above at P_0, the place corresponding to the zero of y in $k(y)$, we obtain the contradiction we were seeking: for the value (at P_0) of the function on the right hand side is 1, while the value of the function on the left hand side is $\neq 1$, no matter which $\varphi \in k(y)$ is taken. Hence $k(x,y)/k(y)$ is a degree $2n$ Galois extension. The corresponding Galois group is the dihedral group of order $2n$. To see this, note that the maps σ and $\psi \in \mathrm{Gal}(k(x,y)/k(y))$ defined by

$$\sigma(r_1) \stackrel{\text{def}}{=} r_2 \quad \text{and} \quad \psi(r_1) \stackrel{\text{def}}{=} \zeta_n r_1$$

are such that

- σ has order 2,
- ψ has order n and
- $\sigma\psi\sigma = \psi^{-1}$ (by the definitions of r_2 and of ψ, $\psi(r_2) = \zeta_n^{-1} r_2$).

So that $\mathrm{Gal}(k(x,y)/k(y)) = \langle \sigma, \psi \rangle \simeq D_{2n}$, where the first equality follows from the two groups, $\mathrm{Gal}(k(x,y)/k(y))$ and $\langle \sigma, \psi \rangle$, having the same order $2n$. If $P = (1:0:0)$ was to be an extendable point, $G_P = \mathrm{Gal}(k(x,y)/k(y))$ would be cyclic and, in particular, abelian, which is not the case. The reader may already have noticed that the "lack of extendability" comes from σ, for ψ can clearly be extended to a projective transformation. A similar example, but with a non-extendable **outer** point, is given in (YOSHIHARA, 2009, Example 1).

5. This was said while we were proving item 2 of Theorem 3, and we say it once again not so much as to attach it to the reader's mind, but as to reference it in the future if necessary: for those curves within the scope of item 2, if $l \geq 2$ then G_P is *not* an abelian group.

The corollary below is an easy direct consequence of Theorem 3; nonetheless it gives a tremendous restriction on the geometry of a curve with an inner extendable Galois point. We recall that a non-singular point P of a curve C is called a *flex* of C if $I_P(C \cap T_P C) \geq 3$; when this intersection multiplicity has the greatest possible value, namely $\deg C$, P will be called a *total flex* of C.

Corollary 1. If P is an inner extendable Galois point for C, then all tangent lines to C at P intersect C only at P. In particular, if P is non-singular this amounts to P being a total flex of C.

Proof. We may suppose, after a suitable projective transformation, that $P = (1:0:0)$ and C has equation

$$G_m(Y,Z)X^{d-m} + H(X,Y,Z) = 0$$

where $H(X,Y,Z)$ has degree $> m$ when viewed as a polynomial in Y and Z. But then the tangent lines to C at P are the factors of $G_m(Y,Z)$. As the equation of C is either

$$G_m(Y,Z)X^{d-m} + G_d(Y,Z) = 0 \quad \text{or} \quad G_m(Y,Z)f(X,Y,Z)^l + G_d(Y,Z) = 0$$

and once G_m and G_d share no factor, the result follows. In fact, if $Q = (x_0 : y_0 : z_0) \neq P$ (notice that this inequality implies that $(y_0, z_0) \neq (0,0)$) would be such that $Q \in C \cap \ell$, where ℓ is a factor of G_m, then G_m and G_d would share the line $\ell = z_0Y - y_0Z$.

□

2.4 The intermediate extension

We study in more detail the intermediate extension that appears in the proof of item 2 of Theorem 3, that is, the extension $k(x,y)/k(x,y)^{C_p^e}$ where C_p^e is the elementary abelian group of exponent p given by the matrices of the form

$$A_{(a,b)} = \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where a and $b \in k$ belong to some finite extension of $\mathbb{F}_p$.

If $(x : y : z) \in C$ corresponds to a ramified place of $k(C)$ relative to the extension under consideration, then it is fixed by at least one non-trivial element of C_p^e, say, $A_{(a,b)}$. But $A_{(a,b)}$ takes the point $(x : y : z)$ to $(x + ay + bz : y : z)$; hence, $(x : y : z)$ is fixed by $A_{(a,b)}$ if, and only if, $ay + bz = 0$, *i.e.*, if, and only if, the point $(x : y : z)$ lies on the line $aY + bZ = 0$ (cf. Remark 3: $A_{(a,b)}$, being a transformation of type V, fixes all the points of a line passing through $(1 : 0 : 0)$, which is precisely $aY + bZ = 0$). In this way we see that the ramified points of the extension all lie on the union of the lines $aY + bZ = 0$, where (a,b) runs over the elements of C_p^e. But there are some redundant lines in the previous union. Indeed, as we saw in the proof of Theorem 3, the group C_p^e has an $\mathbb{F}_p(\zeta_l)$-vector space structure and hence, if $A_{(a,b)} \in C_p^e$, then we also have $A_{(\zeta a,\zeta b)} \in C_p^e$ for all $\zeta \in \mathbb{F}_p(\zeta_l)$; and the lines corresponding to $A_{(a,b)}$ and $A_{(\zeta a,\zeta b)}$ are the same, namely $aY + bZ = 0$. So if we take an $\mathbb{F}_p(\zeta_l)$-basis of C_p^e, say $A_{(a_1,b_1)}, \ldots, A_{(a_s,b_s)}$, then all ramification points of the extension lie in the union of ℓ_i, where $\ell_i : a_iY + b_iZ = 0$. There may still be some redundant lines among the ℓ_i, but the "redundancy factor" won't belong to $\mathbb{F}_p(\zeta_l)$. Each of these lines contain the Galois point $(1 : 0 : 0)$, which is a $(d-m)$-fold point of C. Therefore each line ℓ_i intercepts C in at most $\lfloor m/2 \rfloor$ points different from $(1 : 0 : 0)$ and we see that there will be at most $\lfloor m/2 \rfloor s$ ramification points.

There is nothing much to say about the a's and b's that appear as entries in the matrices of C_p^e. In fact, we can construct a "valid" group C_p^e whose matrices are such that

their entries belong to *any* finite extension $\mathbb{F}_{p^{Nk}}$ of $\mathbb{F}_{p^k} = \mathbb{F}_p(\zeta_l)$ (from now on we make no distinction between $\mathbb{F}_{p^k}$ and $\mathbb{F}_p(\zeta_l)$) as long as $N \geq s/2$ where $s = e/k$ (remember that s is the dimension of C_p^e as an $\mathbb{F}_{p^k}$-vector space). Let us see how this can be done. Take $a_1, \ldots, a_N \in \overline{\mathbb{F}_p}$ such that they are linearly independent over $\mathbb{F}_{p^k}$. The $2N$ matrices $\{A_{(a_i,0)} \mid i = 1, \ldots, N\} \cup \{A_{(0,a_i)} \mid i = 1, \ldots, N\}$ are, therefore, linearly independent over $\mathbb{F}_{p^k}$. Once $2N \geq s$, the space spanned (over $\mathbb{F}_{p^k}$) by any s of them will give a valid group C_p^e.

We will now attempt to find an expression for the element $f(x,y)$ that appears in item 2 of Theorem 3, *i.e.*, for the norm of x relative to the extension we are studying. For this, we start by picking an $\mathbb{F}_p$ basis of C_p^e, consisting of $A_{(a_i,b_i)}$, $i = 1, \ldots, e$. In order to relieve a little bit the notation, we will denote the matrix $A_{(a,b)}$ by (a,b). Remind that

$$f(x,y) = \prod_{(\mu_1,\ldots,\mu_e)\in\mathbb{F}_p^e} \left(x + \sum_{i=1}^{e} \mu_i (a_i y + b_i) \right)$$

Consider for a moment a basis element, say, (a_1, b_1). The above product will contain the following "sub-product"

$$\prod_{(0\neq\nu,0,\ldots,0)\in\mathbb{F}_p^e} (x + \nu(a_1 y + b_1)) = \prod_{\nu\in\mathbb{F}_p^\times} (x + \nu(a_1 y + b_1)) = x^{p-1} - (a_1 y + b_1)^{p-1}$$

It then follows that $f(x,y)$ consists entirely of factors like the above one. In fact, there will be one such a factor for every 1-dimensional subspace of C_p^e, and once every vector of C_p^e lies in one and only one 1-dimensional subspace of C_p^e, we can write

$$f(x,y) = x \prod_{i=1}^{N} (x^{p-1} - (A_i y + B_i)^{p-1})$$

where $N = N(p,e) = (p^e - 1)/(p-1)$ is the total number of 1-dimensional subspaces of C_p^e and $\{(A_i, B_i) \in C_p^e \mid i = 1, \ldots, N\}$ is a system of representatives for the classes of 1-dimensional subspaces of C_p^e (*i.e.*, the points of $\mathbb{P}(C_p^e)$, when C_p^e is viewed as an $\mathbb{F}_p$-vector space). The factor x comes from the trivial subspace.

This reasoning can be applied using the $\mathbb{F}_{p^k}$-vector space structure of C_p^e. It gives

$$f(x,y) = x \prod_{i=1}^{\tilde{N}} (x^{p^k-1} - (\tilde{A}_i y + \tilde{B}_i)^{p^k-1})$$

where $\tilde{N} = N(k,s) = (p^{ks} - 1)/(p^k - 1) = (p^e - 1)/(p^k - 1)$ is the total number of (non-trivial) 1-dimensional $\mathbb{F}_{p^k}$-subspaces of C_p^e and the pairs $(\tilde{A}_i, \tilde{B}_i)$ are, *mutatis mutandis*, as before.

If $e = k$ (which happens, for instance, for $(p,e,l) = (3,2,4)$), then the above product will consist of only one factor, say $x^{p^e-1} + (Ay + B)^{p^e-1}$. Therefore the curve will have the

following equation

$$G_m(Y,Z)(X^{p^e}+(AY+BZ)^{p^e-1}X)^l+G_d(Y)=0$$

which is projectively equivalent to

$$G_m(Y,Z)(X^{p^e}+Y^{p^e-1}X)^l+\tilde{G}_d(Y)=0$$

The lines ℓ_i defined earlier in this section will come back again in section 3.2, where they will play a non-negligible role.

2.5 Non-singular plane quartics

Exploring further the first item in the previous Remark 5, we can use the classification of non-singular plane quartics in characteristic 0 by their automorphism group to decide whether or not a given plane non-singular quartic C has Galois points: if the automorphism group does not contain any cyclic subgroup of order 4 (resp. 3), then C has no outer (resp. inner) Galois points. For such classification, we recommend the reader to check (BARS, 2005) and (DOLGACHEV, 2012).

The groups appearing as the automorphism group of a non-singular plane quartic are listed below (cf. (BARS, 2005, p. 10)); but before showing the table, some words concerning notation are necessary. The `IdSmallGroup`(G) pair corresponds to the identification number of the group G in `GAP`'s Small Group Library. The group can then be accessed in `GAP` by the fuction call `SmallGroup(IdSmallGroup)`. More information can be found in the embedded link here. The letters C, S, D and A appearing in the second column are to be read as cyclic, symmetric, dihedral and alternating, respectively. If its subindex is n, its order is n, $n!$, $2n$ and $n!/2$, with respect to the previous ordering. The group $PSL(3,2)$ is the projective special linear group of 3 by 3 matrices over $\mathbb{F}_2$. We recall that $GL(3,2)=PGL(3,2)=PSL(3,2)\simeq PSL(2,7)$, where this last isomorphism is well known. Finally, $A\circledcirc B$ is a central extension of B by A. In the case of $C_4\circledcirc(C_2\times C_2)$, it also has a $D_8\rtimes C_2$ structure. We will also give a description of $C_4\circledcirc(C_2\times C_2)$ and of $C_4\circledcirc A_4$ as subgroups of $PGL(3,\mathbb{C})$. (cf. (BARS, 2005, Theorem 29)). The group $C_4\circledcirc(C_2\times C_2)$ is isomorphic to the subgroup of $PGL(3,\mathbb{C})$ generated by

$$\begin{pmatrix}-1&0&0\\0&1&0\\0&0&1\end{pmatrix},\quad \begin{pmatrix}i&0&0\\0&-i&0\\0&0&1\end{pmatrix}\quad\text{and}\quad \begin{pmatrix}0&-1&0\\1&0&0\\0&0&1\end{pmatrix}$$

and the group $C_4\circledcirc A_4$ is isomorphic to the subgroup of $PGL(3,\mathbb{C})$ generated by

$$\begin{pmatrix}\frac{\sqrt{2}}{2}\zeta_8&\frac{\sqrt{2}}{2}\zeta_8^3&0\\\frac{\sqrt{2}}{2}\zeta_8&\frac{\sqrt{2}}{2}\zeta_8^7&0\\0&0&\zeta_3\end{pmatrix}\quad\text{and}\quad \begin{pmatrix}\frac{\sqrt{2}}{2}\zeta_8&\frac{\sqrt{2}}{2}\zeta_8^5&0\\\frac{\sqrt{2}}{2}\zeta_8^3&\frac{\sqrt{2}}{2}\zeta_8^3&0\\0&0&\zeta_3^2\end{pmatrix}$$

where $\zeta_n = \exp(2\pi i/n)$. And now the table can be made sense of.

$\lvert G\rvert$	Structure of G	`IdSmallGroup`(G)
2	C_2	$[2,1]$
3	C_3	$[3,1]$
4	$C_2 \times C_2$	$[4,2]$
6	C_6	$[6,2]$
6	S_3	$[6,1]$
8	D_4	$[8,3]$
9	C_9	$[9,1]$
16	$C_4 \circledcirc (C_2 \times C_2)$	$[16,13]$
24	S_4	$[24,12]$
48	$C_4 \circledcirc A_4$	$[48,33]$
96	$(C_4 \times C_4) \rtimes S_3$	$[96,64]$
168	$PSL(3,2)$	$[168,42]$

Table 1 – Automorphism groups of non-singular plane quartics

It is also possible to characterize the equations of the curves for each of the groups above. Such information, which will be implicitly used in the sequence, is to be found in (BARS, 2005, Theorem 16) and (DOLGACHEV, 2012, Theorem 6.5.2).

In what follows, we analyze whether or not a plane non-singular quartic whose automorphism group is G has or has not Galois points, for each and every one of the groups above. We must check, at first, if G has cyclic subgroups of order 3 (for the existence of inner points) or 4 (for the existence of outer points). This condition is necessary for the existence of Galois points, but not sufficient, as it happens to happen for some cases (for example that of S_3). The following lemma guarantees that to each cyclic subgroup there is at most one Galois point associated to it.

Lemma 4. Let $P_1 \neq P_2$ be two distinct extendable Galois points with respect to the curve C. Then $G_{P_1} \cap G_{P_2} = 1$.

Proof. Suppose $\sigma \in G_{P_1} \cap G_{P_2}$. Then $\sigma(\ell_i) = \ell_i$ for every line ℓ_i passing through P_i (cf. the proof of Lemma 1). Taking $\ell_i \neq \overline{P_1P_2}$, we have that $\ell_1 \neq \ell_2$, and therefore $\ell_1 \cap \ell_2 = Q$ consists of a unique point. Applying σ we obtain

$$\sigma(Q) = \sigma(\ell_1 \cap \ell_2) = \sigma(\ell_1) \cap \sigma(\ell_2) = \ell_1 \cap \ell_2 = Q$$

In other words: σ fixes every point not in $\overline{P_1P_2}$. As it is a projective transformation, σ is the identity.

□

One last thing for which we draw the reader's attention is that we will make use of a few results to be proved in Chapter 3. More specifically, we will use propositions 4 through 7.

C_2: These curves do not have any Galois point at all;

C_3: These curves do not have outer Galois points and can have at most one inner Galois point (cf. Lemma 4). Indeed, they have exactly one inner Galois point: their equation is like the one from item 1 in Theorem 3 (cf. (BARS, 2005)).

$C_2 \times C_2$: These curves, as was noted in Remark 5, do not have any Galois points.

C_6: Once C_6 has exactly one subgroup of order 3 and no subgroup of order 4, these curves do not have any outer Galois point and can have at most one inner Galois point. Indeed, they have exactly one inner Galois point, as one may check in item 1, Theorem 3 (and, of course (BARS, 2005), where its equation is given).

S_3: the group S_3 has no cyclic subgroup of order 4, hence it cannot have any outer Galois point. On the other hand, it has just one cyclic subgroup of order 3. From this and from Lemma 4, we can infer that the curves in this family can have at most one inner Galois point. It turns out that the curves in this family have no inner Galois point at all; this is what will now be shown. Suppose that a curve in this family has an inner Galois point P. Then, as Theorem 3 (item 1) states, we can suppose that the Galois point is $(1:0:0)$, that the curve is projectively equivalent to the one given by $F_1(Y,Z)X^3 + F_4(Y,Z) = 0$, and that a generator for G_P is given by the projectivity whose matrix is $\mathrm{diag}(\zeta_3, 1, 1)$. There is no loss in generality in supposing that $F_1(Y,Z) = Z$ also, *i.e.*, that the tangent line of C at P is $Z = 0$. Indeed, as $F_1(Y,Z)$ is a homogeneous *linear* polynomial in Y and Z only, it will suffice to take a projective transformation such as

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}$$

which fixes P, has inverse of the same type and commutes with $\mathrm{diag}(\zeta_3, 1, 1)$ (there is a similar discussion in the proof of Theorem 3 at page 26). Now take an involution in S_3 and suppose that it is given by the matrix $A = (a_{ij})$ (notice that $S_3 \setminus G_P$ consists of involutions only). Once C has only one inner Galois point, the involution A fixes the Galois point P (recall that $A(P)$ is another inner Galois point by Proposition 1), so that $a_{21} = a_{31} = 0$, and we can suppose that $a_{11} = 1$. So up to now we have that

$$A = \begin{pmatrix} 1 & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{pmatrix}$$

We also know that A must leave the equation of C invariant. But among the possibilities for A given above, only those in with $a_{12} = 0 = a_{13}$ can possibly be an automorphism of $ZX^3 + F_4(Y,Z) = 0$, a straightforward assertion left to the reader (cf. the proof of Proposition 3). So we have that

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{pmatrix}$$

But then A and $\mathrm{diag}(\zeta_3, 1, 1)$ commute, which is a contradiction once no transposition commutes with any 3-cycle in S_3.

D_4 : these curves can have only outer Galois points. In fact, they can have at most one outer Galois point, since D_4 has only one cyclic subgroup of order 4 (D_4 has three subgroups of order four: one cyclic and two isomorphic to the Klein four group). The same reasoning used as before (for the case of S_3) can be applied here to conclude that any curve in this family has no Galois points at all. So suppose P is an outer Galois point for a curve C in this family, whose Galois group we will denote by $C_4 \leq D_4$. Take any automorphism M of D_4 not in C_4. We know that M has order 2 (hence $M^{-1} = M$) and fixes the Galois point (otherwise there would be another outer Galois point), which we suppose to be $(1:0:0)$. We also suppose that C is given by $X^4 + F_4(Y,Z) = 0$ and that C_4 is generated by $\mathrm{diag}(\zeta_4, 1, 1)$. Also, denote by $M = (a_{ij})$ the projectivity associated to the automorphism M; from the fact that M fixes $(1:0:0)$, we conclude that $a_{21} = 0 = a_{31}$. It is clear also that, for M to be an automorphism of C, we must have $a_{12} = 0 = a_{13}$. So that

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}$$

But any matrix having the above form commutes with $\mathrm{diag}(\zeta_4, 1, 1)$, which is a contradiction since the center of D_4 has order 2.

C_9 : the curves in this family can have at most one inner Galois point, since C_9 has only one cyclic subgroup of order 3. In fact, there is only one curve in this family (up to projectivity), namely, the curve given by $YX^3 + Z^4 + ZY^3 = 0$ (cf. (BARS, 2005)) which clearly has $(1:0:0)$ as (its unique) inner Galois point, by item 1 of Theorem 3.

$C_4 \circledcirc (C_2 \times C_2)$: this group has `IdSmallGroup` (16,13) in `GAP`'s Small Group Library. More information about this specific group can be obtained in The Group Properties Wiki. For our purposes, it suffices to know that this group

- has order 16, so that curves in this family can only have outer Galois points and
- has only 4 cyclic subgroups of order 4. But any two of them intersect non-trivially, so that the curves in this family can have at most one outer Galois point (since the Galois groups at different Galois points intersect trivially; cf. Lemma 4).

In fact, any curve in this family is projectively equivalent to a curve given by $X^4+Y^4+Z^4+\delta Y^2Z^2$ for some $k \ni \delta \neq 0, \pm 2, \pm 6, \pm(2\sqrt{-3})$, and we see that $(1:0:0)$ is an outer Galois point for any of them by item 1 of Theorem 3, and the only by what was just argued.

S_4 : once S_4 has cyclic subgroups of orders 3 and 4, it may have inner and outer Galois points. We show that any curve in this family does not have any Galois point whatsoever. First of all, we know that the number of inner Galois points is 0, 1 or 4, and the curve with 4 inner Galois points is unique up to projective transformation: it is the curve given by $ZX^3+Y^4+Z^4=0$ (cf. Proposition 4 and Proposition 5). But the automorphism group of this last curve has order 48 (cf. the next item $C_4 \circledcirc A_4$), so no curve of the present family can have 4 inner Galois points: they can have at most 1 of them. If there was only one inner Galois point, any other automorphism of the curve not in the Galois group G_P would commute with G_P (to see this, just proceed as in the previous cases of S_3 and D_4). But G_P would be one of the four 3-Sylow subgroups of S_4, none of which has as its centralizer the whole of S_4, so no curve in this family has inner Galois points. Similarly to the case of inner Galois points, the number of outer Galois points can be 0, 1 or 3, and any curve having 3 outer Galois points would be projectively equivalent to a Fermat curve of degree d (cf. Proposition 6 and Proposition 7). In our case, $d=4$. So if any curve in this family had 3 outer Galois points, it would be projectively equivalent to the Fermat quartic, whose automorphism group has order $6\cdot 4^2 = 96$ (cf. (TZERMIAS, 1995)). Hence, no curve in this family can have 3 outer Galois points: they can have at most one. But, as before, there cannot be any outer Galois point at all: if there was one outer Galois point Q, G_Q would commute with a 3-Sylow, which would imply the existence of a non-existent element of order 12 in S_4.

$C_4 \circledcirc A_4$: there is only one curve in this family (up to projective transformation). Its equation is given by $ZX^3+Z^4+Y^4=0$ (cf. (BARS, 2005)), and it is well known that this curve has exactly four inner Galois points and one outer Galois point (cf. Proposition 4 and Proposition 5). It may be worth noting that this group is a semi-direct product $(C_4 \circledcirc (C_2 \times C_2)) \rtimes C_3$, where $C_4 \circledcirc (C_2 \times C_2)$ is the earlier group of order 16 and the only 2-Sylow of $C_4 \circledcirc A_4$.

$(C_4 \times C_4) \rtimes S_3$: there is only one curve in this family (up to projective transformation): the Fermat quartic (cf. (TZERMIAS, 1995)). It is well known that it has 3 outer Galois points and no inner Galois point (cf. Proposition 7)

$PSL(3,2)$: the only curve in this family (up to projective transformation) is the Klein quartic (cf. (BARS, 2005)). It is well known that $PSL(3,2)$ is a simple group. It cannot have 4 inner Galois points, otherwise it would be projectively equivalent to a curve whose automorphism group has order 48, as we saw previously. So it can have at most one inner Galois point. Likewise, it cannot have 3 outer Galois points, otherwise it would be projectively equivalent to the Fermat quartic whose automorphism group has order 96. So it can have at most one outer Galois point. But it cannot have one inner Galois point P, otherwise any element $\sigma \in \mathrm{Aut}(C) \setminus G_P$ would commute with all elements in the Galois group G_P, and therefore G_P would be a normal subgroup of order 3. Likewise, it cannot have one outer Galois point Q, otherwise G_Q would be a normal subgroup of order 4. So the Klein quartic has no Galois points at all.

2.6 Automorphisms commuting with G_P

We may generalize what happened in the cases where the automorphism group of the curve was one of S_3, D_4, S_4 and $PSL(3,2)$.

Proposition 3. Let C be a non-singular plane curve of degree $d \geq 4$. Suppose that

- C has just one inner Galois point P and $d-1 \not\equiv 0 \bmod p$ or
- C has just one outer Galois point Q and $d \not\equiv 0 \bmod p$.

Then the centralizer of G_P (or G_Q) in $\mathrm{Aut}(C)$ is all of $\mathrm{Aut}(C)$.

Proof. We will restrict ourselves to the case where the first condition is met. The case of an outer point is completely analogous and the reader will not face any difficulties in proving it by himself. By Theorem 3, we can suppose that $P = (1:0:0)$, C is projectively equivalent to $ZX^{d-1} + F_d(Y,Z)$ and a generator for G_P is given by $\mathrm{diag}(\zeta_{d-1}, 1, 1)$. Take $A \in \mathrm{Aut}(C) \setminus G_P$. We have that A fixes P, otherwise $A(P)$ would be another inner Galois point distinct from P (cf. Proposition 1), which cannot happen. It follows that

$$A = \begin{pmatrix} 1 & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{pmatrix}$$

But a_{12} and a_{13} must vanish as well, for otherwise the equation of the "transformed" curve would contain monomials divisible by X^t, for $t < d-1$, which cannot occur since

A is an automorphism of C, *i.e.*, the equations of the "transformed" and of the "original" curve must be the same. Therefore, we may write:

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & \beta \\ 0 & \gamma & \delta \end{pmatrix}$$

Once A and $\mathrm{diag}(\zeta_{d-1}, 1, 1)$ commute, the result follows.

□

Corollary 2. Under the same conditions as in Proposition 3, if $\mathrm{Aut}(C)$ has order $2(d-1)$ (if the first condition of Proposition 3 is met) or $2d$ (in case the second condition is met), then $\mathrm{Aut}(C) \simeq C_{d-1} \times C_2$ and, in particular, it is abelian.

We may weaken the smoothness condition in Proposition 3, if we otherwise "strengthen" the group $\mathrm{Aut}(C)$: this would be replaced by the group $\mathrm{LAut}(C)$ consisting of those morphisms that can be extended to projective transformations. The Galois point would now have to be a unique extendable Galois point of multiplicity m and $d - m \not\equiv 0 \bmod p$. The conclusion would then be that the centralizer of G_P (in $\mathrm{LAut}(C)$) would be the whole of $\mathrm{LAut}(C)$.

CHAPTER

3

SMOOTH CURVES

In the present chapter we will give an overview, as chronologically accurate as possible, of the (main) results about Galois points for smooth curves that culminated in their utterly classification up to projective transformation. Throughout this chapter, curve is to be understood as non-singular of degree ≥ 4 (consequently strange curves are not taken into account).

The sections comprising the chapter correspond (mainly) to the possible values for the characteristic of the base field k, starting with zero characteristic. For curves over a field of positive characteristic, a special family of curves arising in even characteristic is considered separately.

The aforementioned classification was finished in (FUKASAWA, 2013), and was mostly due to the work of the following Japanese mathematicians: Hisao Yoshihara, Kei Miura, Masaaki Homma and Satoru Fukasawa. Apart from those special curves in characteristic 2, the principal ingredients for the classification are (CHANG, 1978), which guarantees that any automorphism of a smooth curve of degree ≥ 4 is linear, and a counting formula for the number of flexes a curve under such hypotheses can have, which can be found in (IITAKA, 1982, p. 294), in case $\operatorname{char} k = 0$, and in (STöHR; VOLOCH, 1986), for $\operatorname{char} k > 0$.

From now on, we denote by $\Delta(C)$ the set of inner Galois points for the curve C, and by $\delta(C)$ its cardinality. The same symbols with a $'$ will be used for outer Galois points. Since the curves under consideration in this chapter are all non-singular, the Galois group of any $P \in \Delta(C)$ has order $\deg C - 1$; similarly, if $P \in \Delta'(C)$, then G_P has order $\deg C$.

The following is a way to reword Lemma 1 and Lemma 2 and "mix" it with (STICHTENOTH, 2009, Theorem 3.7.1 and Corollary 3.7.2). It requires no proof to be given: simply recall that, once C is non-singular, G_P acts transitively on the sets

$(C \cap \ell_P) \setminus \{P\}$ (cf. the proof of Lemma 2), where ℓ_P is any line through P.

Lemma 5. Let P be a Galois point for a non-singular curve C. For a point $Q \in C$, denote by $G_P(Q) \leq G_P$ the stabilizer of Q with respect to the (natural) action of G_P on C, *i.e.*, $G_P(Q) = \{\sigma \in G_P \mid \sigma(Q) = Q\}$. Then $\#((C \cap \overline{PQ}) \setminus \{P\}) = [G_P : G_P(Q)]$ and $I_Q(C \cap \overline{PQ}) = |G_P(Q)|$.

3.1 Zero characteristic

For $\operatorname{char} k = 0$, the task of determining the possible values of $\delta(C)$ and $\delta'(C)$ as well as that of classifying the curves with a given prescription of the previous values was initiated in (MIURA; YOSHIHARA, 2000) and finished in the sequence (YOSHIHARA, 2001).

We are going to recover these results using Theorem 3; actually, some of them are already stated in Theorem 3. Our approach has minor differences to that of (MIURA; YOSHIHARA, 2000) and (YOSHIHARA, 2001); these differences are mostly (if not all) with respect to form rather than to the mathematical essence of the thing.

Inner points are treated at first.

Proposition 4. Let C be a degree d curve. If $\delta(C) \geq 2$, then $\delta(C) \geq d$.

Proof. Suppose $P, Q \in \Delta(C)$ with $P \neq Q$ and $P = (1:0:0)$. Take σ a generator for G_P as in Theorem 3 (item 1). We claim that $\sigma^s(Q) \neq Q$ for any $1 \leq s \leq d-2 = |G_P| - 1$. Suppose it is not so, and take s minimal with $\sigma^s(Q) = Q$; then the orbit of Q under the action of G_P consists of the s points $Q, \sigma(Q), \ldots, \sigma^{s-1}(Q)$, *i.e.*, $C \cap \overline{PQ} = \{P, Q, \sigma(Q), \ldots, \sigma^{s-1}(Q)\}$. The line $\overline{PQ}$ cannot be $T_P C$, for non-singular inner Galois points are total flexes (cf. Corollary 1). Therefore $I_P(C \cap \overline{PQ}) = 1$, and consequently $I_Q(C \cap \overline{PQ}) = (d-1)/s$ (cf. Lemma 1); but this cannot happen: Q, being also an inner Galois point, is also a total flex, so that $I_Q(C \cap \overline{PQ}) = 1$ or d, which is never obtained as $(d-1)/s$ for any $1 \leq s \leq d-2$. Therefore the orbit of Q is made up of $d-1$ (distinct) inner Galois points (cf. Proposition 1). Taking P into account, it follows that $\delta(C) \geq d$.

□

It may be worthy to stress out that the d inner Galois points considered in the preceding proof, *viz.* $\{P, \sigma(Q), \ldots, \sigma^{d-2}(Q), \sigma^{d-1}(Q) = Q\}$, are all *collinear*.

The next proposition makes use of the formula, which will be used to count flexes, that was mentioned in the beginning of the chapter. This formula, exactly as it is in (IITAKA, 1982, p .294, last line), reads

$$W = 3r + 6g - 6 - 2R - \alpha - \beta \tag{3.1}$$

Each of these letters represent values depending on the curve C; let us briefly explain their meaning. The integer $W = W(C)$ is the sum, over all non-singular points Q of C, of $I_Q(C \cap T_Q C) - 2$; regard that the sum is taken, effectively, only over the flexes of C. The quantities R, α and β are positive and depend upon the singularities of the curve C. Hence, we may rewrite (3.1) as

$$W(C) \leq 3r + 6g - 6 \tag{3.2}$$

The number r is just d, the degree of the curve, and g is its genus. Within our context, $g = (d-1)(d-2)/2$, and, after substitution and rearrangement, we may finally rewrite (3.2) in the "shape" we are going to use it:

$$W(C) = \sum_Q (I_Q(C \cap T_Q C) - 2) \leq 3d(d-2) \tag{3.3}$$

The $\leq$ in (3.3) is actually $=$ in view that for non-singular curves the quantities R, α and β vanish. However, the $\leq$ will be sufficient for our needs.

Proposition 5. If $\delta(C) \geq d$ then $d = 4 = \delta(C)$. Moreover C is projectively equivalent to $ZX^3 + Y^4 + Z^4 = 0$.

Proof. Take the equation of C given by Theorem 3 (without loss of generality, we may take $Z = 0$ to be the tangent line at $(1:0:0)$):

$$ZX^{d-1} + G_d(Y, Z) = 0$$

The intersection of C with the line $X = 0$ consists of d points, which correspond to the d roots of G_d; there are indeed d roots: if there was a repeated root, it would give rise to a singularity of C. Moreover, each of these points is a flex of order $d-1$, *i.e.*, their tangent lines intersect the curve at them with multiplicity $d-1$. Notice that these same tangent lines all pass through P.

For another inner Galois point $Q \neq (1:0:0)$, we may invoke Theorem 3 again, but this time for Q in place of P. Then, we again have that C is projectively equivalent to

$$ZX^{d-1} + \tilde{G}_d(Y, Z) = 0$$

from which we conclude that there will be other d flexes of C associated to Q, each of them with multiplicity $d-1$ as well. To sum up: for each inner Galois point P there corresponds d flexes $\{R_{P,1}, \ldots, R_{P,d}\}$, and each of which satisfies $I_{R_{P,i}}(C \cap T_{R_{P,i}} C) = d-1$.

We claim that to distinct inner Galois points P and Q there correspond disjoint sets of flexes. Indeed, if it was $R_{P,i} = R = R_{Q,j}$, then $P \in T_R C \cap C \ni Q$; once there is only one point in $T_R C \cap C \setminus \{R\}$, the only possibility is that $P = Q$, which is an impossibility. Hence, if there are $\delta(C)$ inner points for C, there will be at least $\delta(C)$ total flexes (each one

of the inner points) and at least $\delta(C)\cdot d$ flexes of order $d-1$. As we supposed $\delta(C)\geq d$, (3.3) gives us

$$\begin{aligned} d(d-2)+d^2(d-3)\leq &\delta(C)(d-2)+\delta(C)d(d-3)\leq W(C)\leq 3d(d-2)\rightsquigarrow \\ &\rightsquigarrow (d-2)+d(d-3)\leq 3(d-2) \end{aligned} \tag{3.4}$$

This inequality holds for $1\leq d\leq 4$. But $d\geq 4$, hence $d=4$, and as $d=4$ turns the above inequality into an equality, we see that $\delta(C)=4$ as well.

Now, it remains to show that C is projectively equivalent to $ZX^3+Y^4+Z^4=0$. To begin with, we point out that the four inner points are all collinear, as can be seen in the proof of Proposition 4. We can take $Y=0$ to be such line, without losing generality. Indeed, as $P=(1:0:0)$ is one of the inner points and as C has equation

$$ZX^3+G_4(Y,Z)=0$$

we see that the line ℓ containing the other inner points is not the line $T_PC:Z=0$; hence $\ell: aY+bZ=0$ for some $a\neq 0$. The projective transformation

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & a^{-1} & -a^{-1}b \\ 0 & 0 & 1 \end{pmatrix}$$

takes ℓ to the line with equation $Y=0$ and commutes with the generator $\mathrm{diag}(\zeta_3,1,1)$ of G_P, so that, after this transformation, the curve will still have equation

$$F(X,Y,Z)\overset{\text{def}}{=} ZX^3+\tilde{G}_4(Y,Z)=0$$

but this time all the 4 inner points will be contained in $Y=0$. Moreover, once Z does not divide $\tilde{G}_4(Y,Z)$, the coefficient of Y^4 in $\tilde{G}_4(Y,Z)$ does not vanish. Furthermore, if we substitute $Y=0$ in the equation for C, we get $ZX^3+eZ^4=0$. The roots of this quartic equation give all four inner Galois points, therefore it must be $e\neq 0$ as well (if not, the equation would give us only two points). We are going to write

$$\tilde{G}_4(Y,Z)=aY^4+bY^3Z+cY^2Z^2+dYZ^3+eZ^4 \tag{3.5}$$

By what we have just seen, it holds $ae\neq 0$.

To finish the proof, we will make use of an auxiliary-by-its-own-nature result: the one to be found in (YOSHIHARA, 2001, Lemma 11); within our setup, it says that a point $(1:\alpha:\beta)\in C$ is an inner Galois point if, and only if,

$$g_2^2=3g_1g_3 \qquad \text{where } F(1,y+\alpha,z+\beta)=\sum_{i=1}^{4} g_i(y,z)$$
$$\text{with } g_i(y,z) \text{ homogeneous of degree } i$$

The four inner points are $(1:0:0)$ and $(1:0:r\zeta_3^i)$, for $i=0,\ldots,2$, where $r^3=-1/e$. We now use (YOSHIHARA, 2001, Lemma 11) with $(1:0:r\zeta_3)$ in place of $(1:\alpha:\beta)$, and simplify a tiny bit the notation replacing R for $r\zeta_3$. For $F(1,y,z+R)=\sum_{i=1}^{4} g_i(y,z)$, the g_i's are given as follows (recall (3.5))

$$\begin{cases} g_4(y,z) &= ay^4+by^3z+cy^2z^2+dyz^3+ez^4 \\ g_3(y,z) &= bRy^3+2cRy^2z+3dRyz^2+4eRz^3 \\ g_2(y,z) &= cR^2y^2+3dR^2yz+6eR^2z^2 \\ g_1(y,z) &= -d/e\,y-3z \end{cases}$$

The equation $g_2^2=3g_1g_3$ will give five equations, one for each of the five monomials y^iz^{4-i}, $i=0,\ldots,4$, which are listed below (a common $-R$ was cancelled).

$$\begin{array}{lcc} \text{Coefficient of } y^4 & \rightsquigarrow & c^2/e=3db/e \\ \text{Coefficient of } y^3z & \rightsquigarrow & 6cd/e=3(2cd/e+3b) \\ \text{Coefficient of } y^2z^2 & \rightsquigarrow & (12ce+9d^2)/e=3(3d^2/e+6c) \\ \text{Coefficient of } yz^3 & \rightsquigarrow & 36de/e=3\cdot 13d \\ \text{Coefficient of } z^4 & \rightsquigarrow & 36e^2/e=36e \end{array}$$

From these, it readily follows that $d=c=b=0$. Hence $\tilde{G}_4(Y,Z)=aY^4+eZ^4$, with $ae\neq 0$. After rescaling, the curve is projectively equivalent to the one with equation

$$ZX^3+Y^4+Z^4=0$$

which finally concludes the proof.

□

Proposition 5 sets up the possible values for $\delta(C)$ when it is not zero: it can be 1 or 4 only. Moreover, it also tells that the curve attaining the most inner Galois points is unique up to projective equivalence. For the curves having exactly one inner Galois point, the characteristic equation given by item 1 of Theorem 3 cannot be "enhanced".

Now we consider outer Galois points.

Proposition 6. With C as before, there can be at most three outer Galois points, *i.e.*, $\delta'(C)\leq 3$.

Proof. Take again the equation given by Theorem 3; for an outer point, which we suppose, as always, to be $P=(1:0:0)$, it reads:

$$X^d+G_d(Y,Z)=0$$

The d points on the intersection of the curve with the line $X=0$ are, all of them, total flexes of the curve, and their tangent lines pass through P. We mention that this intersection

consists indeed of d points, for the polynomial G_d has distinct roots (otherwise the curve would be singular).

For another outer point $Q \neq P$, there will be yet another d total flexes. But, contrasting the behavior of inner points, to distinct outer Galois points there does not necessarily correspond disjoint sets of flexes. Nevertheless, there can be at most one common flex associated to any two distinct outer points, and this is because the tangent line at any common total flex will pass through both of the outer points.

Now take $\sigma \in G_P$ a generator for this group. Suppose that $\sigma(Q) \neq Q$. Recall that the projective transformation σ fixes all the points on the line $X = 0$ (cf. Remark 3); therefore, we may write $Q = (1 : y : z)$ and if it was $y = 0 = z$, it would be $Q = P$, which is not the case. Hence, the points $\sigma^k(Q) = (\zeta_d^k : y : z)$, for $k = 0, \ldots, d-1$, are all distinct and we have, up to now, $d+1$ outer points (cf. Proposition 1): the d points on the orbit of Q together with P. Moreover, they are all collinear, so that by a slightly different version of what was said in the preceding paragraph there can be at most one common point among all the flexes associated to all these outer points. Putting these information altogether in (3.3) results in

$$(d+1)(d-1)(d-2) + (d-2) \leq 3d(d-2) \tag{3.6}$$

This last inequality implies that $d \leq 3$, in contradiction to our initial assumption that $d \geq 4$. Therefore, it must be $\sigma(Q) = Q$. For an outer point R let us call ℓ_R the line whose points are all fixed by G_R (for instance, $\ell_P : X = 0$). The argument just given can be rephrased as: if $R \neq S$ are outer points, then $R \in \ell_S$ and $S \in \ell_R$ (notice that $\ell_S \neq \ell_R$).

Now it easily follows that there can be at most three outer points, for if there are two, say P and Q, as before, any other outer point should be in the intersection $\ell_P \cap \ell_Q$, which consists of a single point; and we are done.

□

Proposition 7. If $\delta'(C) \geq 2$ then C is projectively equivalent to the Fermat curve $X^d + Y^d + Z^d = 0$. Consequently $\delta'(C) = 3$.

Proof. Assume that $P = (1 : 0 : 0)$, C is given by

$$X^d + G_d(Y, Z) = 0$$

and keep in mind the other conclusions of Theorem 3. The other outer point Q will then lie on the line $X = 0$ (cf. the proof of Proposition 6). There is no loss in generality in supposing that $Q = (0 : 1 : 0)$: if it was not, we could take a projective transformation of the form

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix} \tag{3.7}$$

which commutes with the generator $\mathrm{diag}(\zeta_d, 1, 1)$ of G_P and takes C to a curve with equation

$$X^d + \tilde{G}_d(Y, Z) = 0$$

which has the same "type" as before.

If we look back at the proof of Lemma 3, we see that a generator τ for G_Q has the form

$$A_\tau = \begin{pmatrix} 1 & 0 & 0 \\ \alpha & \zeta_d & \beta \\ 0 & 0 & 1 \end{pmatrix}$$

for some α and β. But P must be fixed by G_Q, for the same reason why Q is fixed by G_P (cf. the proof of Proposition 6), and from this we conclude that $\alpha = 0$. We may, then, diagonalize A_τ without "messing up" our previous assumptions, *i.e.*, there is no loss in generality in assuming not only that $Q = (0 : 1 : 0)$ but also that G_Q is generated by $\mathrm{diag}(1, \zeta_d, 1)$. Indeed, there is a projectivity diagonalizing A_τ which fixes Q and has the same form as that in (3.7) (cf. the discussion at page 26).

Now, from the "point of view" of P, *i.e.*, using Theorem 3 for the Galois points P, the curve has equation

$$X^d + G_d(Y, Z) = 0$$

while from the point of view of Q the *same* curve (*i.e.*, there is no projective transformation involved) has equation

$$Y^d + H_d(X, Z) = 0$$

Therefore,

$$X^d + G_d(Y, Z) = \lambda(Y^d + H_d(X, Z)) \tag{3.8}$$

for some $\lambda \neq 0$. (3.8) now implies that the curve has equation

$$X^d + sY^d + tZ^d = 0$$

which is projectively equivalent to the Fermat curve. As any permutation of the variables is a linear automorphism of this curve, from Proposition 1 it follows that $(0 : 0 : 1)$ is another, and the only other (cf. Proposition 6), outer Galois point.

□

Again, Proposition 7 establishes the possible non-zero values for $\delta'(C)$: they can be either 1 or 3. Furthermore, for each $d \geq 4$ there is one and only one curve, up to projective equivalence, attaining 3 outer Galois points: the Fermat curve of degree d. Note that the Fermat curve of degree d also attains the maximum possible number, *viz.* $3d$, of total flexes among all degree d curves. Those curves having exactly one outer Galois point cannot be "more characterized" than as they are by Theorem 3.

3.2 Positive and mostly odd characteristic

In what follows we focus on the contents of (HOMMA, 2006), (FUKASAWA, 2007), (FUKASAWA, 2008) and (FUKASAWA, 2010). The results therein get very close to conclude the classification we have been speaking of so far, the only remaining case being that of curves in characteristic 2 attaining the second largest possible number of inner points (as well as two "sporadic" curves, also in characteristic 2, of degree $d = 4 \equiv 0 \bmod 2$, when outer points are under consideration; cf. (FUKASAWA, 2011, Theorem 3, (II)(ii) and (II)(iv))). An equivalent version of (3.3) for $\operatorname{char} k > 0$ must be used. In order for us to be able to interpret it, a new notion must be introduced; the details behind why this notion is well-defined may be encountered in (HOMMA, 1987).

Definition 6. For a curve C, the integer $q(C)$ such that $I_R(C \cap T_R C) \geq q(C)$ for all $R \in C$ is called the generic order of contact for it. If $q(C) > 2$, then it is a power of $p = \operatorname{char} k > 0$ and, in any case, $I_R(C \cap T_R C) > q(C)$ for finitely many points, by which the "generic" is explained. Obviously, $q(C) \leq \deg C$.

Remark 6. The curves such that $q(C) = d > 2$ are totally known and they are all strange curves (cf. (HOMMA, 1987, Theorem 3.4)). In particular, they are singular and not to worry about here. Concerning the notation, in (STöHR; VOLOCH, 1986), the $q(C)$ corresponds to the ϵ_2 order of the morphism $\hat{C} \to C \subset \mathbb{P}^2$ given by $(x : y : 1)$, where $\hat{C}$ is the non-singular model of C and the affine equation for C is $f(x, y) = 0$.

There exists a divisor (cf. (STöHR; VOLOCH, 1986) and also (FUKASAWA, 2007, Section 2)) $\mathcal{W}(C) = \sum_{P \in C} v_P(\mathcal{W}(C))P$ such that

- $\deg \mathcal{W}(C) = d((q(C)+1)d - 3q(C))$ and
- $I_P(C \cap T_P C) - q(C) \leq v_P(\mathcal{W}(C))$

From these, the equivalent form of (3.3) we were looking for is as stated below

$$\sum_{P \in C} (I_P(C \cap T_P C) - q(C)) \leq \deg \mathcal{W}(C) = d((q(C)+1)d - 3q(C)) \tag{3.9}$$

Notice that in the situations for which it holds $q(C) = 2$, $\operatorname{char} k = 0$ for instance, the right hand side of (3.9) turns into the right hand side of (3.3); however, it must be pointed out that the divisor $\mathcal{W}(C)$ is not necessarily given by $\sum_{P \in C}(I_P(C \cap T_P C) - 2)$. In fact, we have the following (cf. (FUKASAWA, 2008, Section 2), (FUKASAWA, 2007, Section 2) and (STöHR; VOLOCH, 1986, Theorem 1.5))

$$I_P(C \cap T_P C) - q(C) = v_P(\mathcal{W}(C)) \Leftrightarrow \binom{I_P(C \cap T_P C)}{q(C)} \not\equiv 0 \bmod p \tag{3.10}$$

3.2.1 The special case of the Hermitian curve

The first work on which the distribution of Galois points for curves over a field of positive characteristic were considered is (HOMMA, 2006). We denote by $\mathcal{H}_q$ the Hermitian curve of degree $q+1$, *i.e.*,

$$\mathcal{H}_q : X^{q+1} = Y^q Z + Y Z^q$$

for some power $q = p^e \geq 4$ of the characteristic p of the base field.

The Galois points for $\mathcal{H}_q$ are fully described in the following (cf. (HOMMA, 2006, Theorem 1))

Theorem 4. Any $\mathbb{F}_{q^2}$-rational point of $\mathbb{P}^2(k)$ is a Galois point for $\mathcal{H}_q$ and conversely.

The Hermitian curve $\mathcal{H}_q$ is well-known for being a maximal curve, *i.e.*, for reaching the maximum possible number of ($\mathbb{F}_{q^2}$-) rational points given by the Hasse-Weil bound. This number is q^3+1. Theorem 4 then implies that $\delta(\mathcal{H}_q) = q^3+1$. Since the projective plane $\mathbb{P}^2$ has q^4+q^2+1 $\mathbb{F}_{q^2}$-rational points, we conclude, again by Theorem 4 and the preceding, that $\delta'(\mathcal{H}_q) = q^4 - q^3 + q^2$. These observations show that, contrary to what happens for curves over a field of zero characteristic, the number of Galois points a smooth curve in positive characteristic can have can be as large as one desires, if only the degree is taken large enough. As we will see in the sequence, $\mathcal{H}_q$ together with another family of curves for $p = 2$ are the only "unbounded curves": any other smooth curve is such that $\delta(C)$ and $\delta'(C)$ are bounded.

There is yet another equivalent way to state Theorem 4 without mentioning the field on which the curve is defined; it, instead, uses purely geometric terms and is given below, for the sake of completeness (cf. (HOMMA, 2006, Theorem 2)).

Theorem 5. A point $P \in \mathcal{H}_q$ is an inner Galois point if, and only if, P is a total flex; and a point $Q \in \mathbb{P}^2 \setminus \mathcal{H}_q$ is an outer Galois point if, and only if, there exist two total flexes P_1 and $P_2 \in \mathcal{H}_q$ such that $Q = T_{P_1}C \cap T_{P_2}C$.

3.2.2 Inner points when $d \not\equiv 1 \bmod p$

When $d \not\equiv 1 \bmod p$, Proposition 4 still holds no matter what the characteristic of the field is: the proof does not even mention it. Also, the d points that are guaranteed to exist are collinear.

Now, when it comes to Proposition 5 it happens that it is still true for "any" p, but the proof differs only when $p = 2$. We wrote "any" because for $p = 2$ the curve with equation $ZX^3 + Y^4 + Z^4 = 0$ is singular: the polynomial $Y^4 + Z^4 = (Y+Z)^4$ has only one root (with $YZ \neq 0$), giving rise to the singular point $(0:1:1)$, which has multiplicity 3.

So the proper way to state the analogous of Proposition 5 for positive characteristic is as follows.

Proposition 8. If C is a non-singular curve of degree d in characteristic $p \geq 5$, such that $d \not\equiv 1 \bmod p$, then $\delta(C) \in \{0,1,4\}$. Moreover, $\delta(C) = 4$ only if $d = 4$, in which case C is projectively equivalent to the curve given by $ZX^3 + Y^4 + Z^4 = 0$. If $p = 2$ or 3, then $\delta(C) \in \{0,1\}$.

We did not mention anything about $p = 3$ before stating Proposition 8. But note that for $d = 4$, we have $d \equiv 1 \bmod 3$, even though the conclusion "$\delta(C) = 4$ implies $d = 4$" still holds for $p = 3$; hence, those double quotation marks in that "any" above are there to quote both $p = 2$ and 3. There is another observation to be made in what regards $p = 3$. For the proof of the last part of Proposition 5, (YOSHIHARA, 2001, Lemma 11) was invoked, and then the proof was concluded after some calculations. The fact is: (YOSHIHARA, 2001, Lemma 11), may it be coincidence or not, is valid exactly for all $p \neq 3$.

The proof of Proposition 8 for $p \geq 3$ is exactly the same as that for $\operatorname{char} k = 0$, Proposition 5. This is because a non-singular curve given by $ZX^{d-1} + G_d(Y,Z) = 0$, is in Theorem 3, still has generic order of contact equal to 2, allowing us to use (3.3) as in (3.4). That these curves have $q(C) = 2$ is a consequence of their dual map being separable[1], which can be seen by writing the equation locally as $x^{d-1} + G_d(y,1) = 0$ and showing that $\frac{d}{dx}\left(\frac{dy}{dx}\right) \neq 0$ in $k(C)$. The reader may consult (FUKASAWA, 2008, Section 2) and a similar computation that is done in the next section.

If $p = 2$, the dual map is no longer separable, but it can be shown that the generic order of contact is still 2. This is done by showing not that $\frac{d}{dx}\left(\frac{dy}{dx}\right) \neq 0$ but that $\mathcal{D}_y^{(2)}(x) \neq 0$, where $\mathcal{D}_y^{(l)}$ is the l-th Hasse derivative with respect to y, and using the fact that $q(C)$ is the smallest integer $l \geq 2$ such that $\mathcal{D}_y^{(l)}(x) \neq 0$ in $k(C)$ (cf. (FUKASAWA, 2007, Section 2) and (STöHR; VOLOCH, 1986, Theorem 1.1)) The details are given in (FUKASAWA, 2007, p. 135) (cf. also (HIRSCHFELD; KORCHMáROS; TORRES, 2013, Remark 1.37)).

3.2.3 *Outer points when* $d \not\equiv 0 \bmod p$

If we try to repeat the proof of Proposition 6 when the characteristic is positive, we must assume two conditions for the same sequence of implications to hold. First, we need that $d \not\equiv 0 \bmod p$, for C to be in item 1 of Theorem 3, and in second place, we need the generic order of contact to be 2, for (3.3) to be used as in (3.6). The former is assumed all through this (sub)section. Now, for the second condition to be valid, it is sufficient to

[1] Separability of the dual map implies finiteness of the number of flexes, and consequently that the generic order of contact is 2.

assume also that $d \not\equiv 1 \bmod p$ (which will imply that the dual map is separable), or that $d \equiv 1 \bmod p$ and the dual map of C is separable. Let us show, in the interest of being instructive, that $d \not\equiv 1 \bmod p$ really implies separability of the dual map.

The equation of C can be written as

$$X^d + G_d(Y,Z) = 0$$

where $G_d(Y,Z)$ does not have repeated roots (otherwise C would be singular). Without loss of generality, suppose the coefficient of Y^d in $G_d(Y,Z)$ is not zero; suppose also it is 1. The rational functions $x = X/Z$ and $y = Y/Z$ then satisfies

$$x^d + G_d(y,1) = 0 \tag{3.11}$$

We write

$$g(y) \stackrel{\text{def}}{=} G_d(y,1) = y^d + a_{d-1}y^{d-1} + \ldots + a_1 y + a_0$$

The dual map of C is separable if, and only if, $y'' \stackrel{\text{def}}{=} \frac{d}{dx}\left(\frac{dy}{dx}\right) \neq 0$ in $k(C)$. Differentiating (3.11), we obtain

$$dx^{d-1} + g'(y)y' = 0 \tag{3.12}$$

where $y' \stackrel{\text{def}}{=} \left(\frac{dy}{dx}\right)$ and g' is the usual derivative of the polynomial $G_d(T,1)$, in case there were any doubts about it. As $g'(y) \neq 0$, we can write

$$y' = -\frac{dx^{d-1}}{g'(y)}$$

Differentiating (3.12) now gives

$$d(d-1)x^{d-2} + g''(y)\cdot(y')^2 + g'(y)y'' = 0 \tag{3.13}$$

If $d \not\equiv 1 \bmod p$ (recall that $d \not\equiv 0 \bmod p$ also) but $y'' = 0$, then (3.13) would read

$$\begin{aligned} d(d-1)x^{d-2} = -g''(y)(y')^2 = -g''(y)\frac{d^2x^{2d-2}}{g'(y)^2} \rightsquigarrow \\ \rightsquigarrow\ dx^d g''(y) = -(d-1)g'(y)^2 \rightsquigarrow \\ \rightsquigarrow\ dg(y)g''(y) = (d-1)g'(y)^2 \end{aligned}$$

Notice we used (3.11): $x^d = -g(y)$. From this last equation, *viz.* $dg(y)g''(y) = (d-1)g'(y)^2$, it follows that $g(y)$ and $g'(y)$ have common zeroes. Actually, it follows that any zero of $g(y)$ is a zero of $g'(y)$. But this contradicts the separability of the polynomial $g(T) = G_d(T,1)$, which has to do with the smoothness of C. Hence, it cannot be $y'' = 0$; and we are done.

Thus, in these cases where the generic order of contact is 2, the proof of Proposition 6 still holds. Likewise, the proof of Proposition 7 also applies, but it should be

observed that if $d \equiv 1 \bmod p$, the dual map of the Fermat curve $X^d + Y^d + Z^d = 0$ is inseparable; therefore in case $d \equiv 1 \bmod p$ and C has separable dual map, we conclude that $\delta'(C) \in \{0,1\}$.

The remaining instances to consider are those for which $d \equiv 1 \bmod p$ and C has inseparable dual map. Putting aside the Hermitian curve, the conclusions stated in Proposition 6 and Proposition 7 are still true for these curves, and only the proof of Proposition 6 needs to be modified: that of Proposition 7 can be copied exactly as it is there. This modification includes using (3.9) as well as a couple of facts concerning the generic order of contact within this setup, namely: that $q(C) \mid d-1$ (cf. (HOMMA, 1989, Corollary 2.4)) and if $q(C) = d-1$ then C is projectively equivalent to the Hermitian curve (this follows easily from (HOMMA, 1989, Corollary 2.5)). Once we have put the Hermitian curve away from our current considerations, we then have that $2 < q(C) < d-1$, and since $q(C) \mid d-1$, we conclude that $d > 2q$. The analogous of (3.6) (the $d-2$ is to be replaced with a $d-q(C)$ and the right hand side of the inequality in (3.6) is to be replaced by the right hand side in (3.9)) is:

$$(d+1)(d-1)(d-q(C)) + (d-q(C)) \leq d((q(C)+1)d - 3q(C)) \tag{3.14}$$

It is left to the reader to check that (3.14) implies $d \leq 2q(C)$ (cf. also the proof of Proposition 11), contrary to the inequality derived a few lines above. The considerations made in this section were taken from (FUKASAWA, 2008) and (FUKASAWA, 2007), wherein any details we skipped are sure to be found.

A concise statement of what was done is given below.

Proposition 9. Let C be a non-singular curve of degree d in characteristic $p > 0$ such that $d \not\equiv 0 \bmod p$. If $d \not\equiv 1 \bmod p$, then $\delta'(C) \in \{0,1,3\}$ and $\delta'(C) = 3$ if, and only if, C is projectively equivalent to $X^d + Y^d + Z^d = 0$. If $d \equiv 1 \bmod p$ and the dual map of C is separable, then $\delta'(C) \in \{0,1\}$. If $d \equiv 1 \bmod p$, the dual map of C is inseparable and C is not projectively equivalent to the Hermitian curve, then $\delta'(C) \in \{0,1,3\}$ and $\delta'(C) = 3$ if, and only if, C is projectively equivalent to $X^d + Y^d + Z^d = 0$.

Notice that in the last case of Proposition 9, $d-1$ will not be a power of p, for otherwise $X^d + Y^d + Z^d = 0$ would be the Hermitian curve.

3.2.4 *Inner points when* $d \equiv 1 \bmod p$

When dealing with inner points on curves whose degree is $\equiv 1 \bmod p$, we must use item 2 of Theorem 3, rather than item 1 of the same theorem. In this case, the Galois group of a Galois point will no longer be cyclic, unless $d = p$ (it will not even be abelian in "most" cases; cf. item 5 of Remark 5). Still, we will be able to estimate the number of

inner Galois points in this case, and, except for $p = 2$, we will have that $\delta(C)$ is either 0 or 1.

The statement of this estimate is given below (cf. (FUKASAWA, 2010, Theorem 1)), and the proof will be done in a not-so-few number of intermediate steps.

Proposition 10. Let C be of degree d such that $d - 1 = p^e l$ for some $e \geq 1$ and l not divisible by p. Suppose also that C is not projectively equivalent to the Hermitian curve. Then the following holds:

1. If $p \geq 3$ or $l \geq 2$, then $\delta(C) \in \{0, 1\}$.
2. If $p = 2$ and $l = 1$, then $\delta(C) \in \{0, 1, d\}$.

The curves in item 2 of Proposition 10 for which $\delta(C) = d$ will be treated and thoroughly described later in this chapter.

Before beginning to prove Proposition 10, we bring back to memory a handful of facts concerning item 2 of Theorem 3, and also establish some notational conventions (cf. (FUKASAWA, 2010, Section 2)).

Given a smooth curve C of degree $d = p^e l + 1$ as before, we suppose throughout here that $P = (1 : 0 : 0)$ is an inner point for it and that its equation is

$$Z f(X, Y, Z)^l + G_d(Y, Z) = 0 \tag{3.15}$$

Remind that $f(X, Y, Z)$ is an additive polynomial of degree p^e with respect to the variable X, and its roots are all linear forms in Y and Z. In particular $X | f(X, Y, Z)$, *i.e.*, $f(0, Y, Z) = 0$. Moreover the polynomial $G_d(T, 1)$ is separable: if $t^\star$ was a repeated root, $(0 : t^\star : 1)$ would be a singular point. We also have $Z \nmid G_d(Y, Z)$, for otherwise (3.15) would be reducible (we do not lose generality in assuming that the $G_1(Y, Z)$ that appears in item 2 of Theorem 3 is Z; cf. the discussion in pages 49 and 26). The Galois group will be denoted by $G_P = C_p^e \rtimes C_l$, where $C_p^e \simeq \oplus^e \mathbb{Z}/p\mathbb{Z}$ and $C_l \simeq \mathbb{Z}/l\mathbb{Z}$, as in item 2 of Theorem 3. A generator for C_l is

$$\tau \stackrel{\text{def}}{=} \begin{pmatrix} \zeta_l & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and any element

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in C_p^e$$

will be denoted by (a,b). For any $\gamma \in G_P$ there are unique $i \in \{0,\dots,l-1\}$ and $(a,b) \in C_p^e$ such that

$$\gamma = (a,b)\cdot\tau^i = \begin{pmatrix} \zeta_l^i & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Back in the last chapter, we pointed out some geometrical aspects of the automorphisms of the plane associated to a Galois point for a curve; these are the contents of Remark 3 and they will play a significant role in what comes next. The reader is asked to take a look there. Any transformation $\gamma \in G_P$ will be either of type IV or of type V. These two types of transformations fix the Galois point P and all the points in a line, which we denote by ℓ_γ. More specifically, the reader may easily show that if $\gamma = (a,b)\tau^i \neq 1$ then

$$\ell_\gamma : (\zeta_l^i - 1)X + aY + bZ = 0 \tag{3.16}$$

Note that $P \in \ell_\gamma \Leftrightarrow \gamma \in C_p^e$, in accordance with any $\gamma \in C_p^e$ being of type V. Also, $\ell\gamma : X = 0$ for any $\gamma \in C_l$, and this line does not contain P, in accordance with any $\gamma \in C_l$ being of type IV. For $\gamma \neq 1$, if $R \in (C \cap \ell_\gamma) \setminus \{P\}$, then $T_R C = \overline{PR}$. Indeed, the condition $R \in \ell_\gamma$ implies that R if fixed by γ, and therefore that $1 \neq \gamma \in G_P(R)$; hence $I_R(C \cap \overline{PR}) = |G_P(R)| \geq 2$ (cf. Lemma 5), and it must be $\overline{PR} = T_R C$ by the smoothness of C.

Finally, the generic order of contact $q(C)$ will be denoted simply by q, and for $R \in C$ we will say that it is an $(r-q)$-flex if $I_R(C \cap T_R C) = r > q$.

The first step towards Proposition 10 is the following analogue of Proposition 4 (cf. (FUKASAWA, 2010, Lemma 1)).

Lemma 6. If $\delta(C) \geq 2$, then $\delta(C) \geq d$. Moreover, if we denote by $\mathcal{R}_P = \{Q_{P,1},\dots,Q_{P,s}\}$ the set of points Q for which $I_Q(C \cap \overline{PQ}) > 1$ (*i.e.*, the ramification points of π_P), then for any two inner Galois points P and P' there is a bijection $\psi : \mathcal{R}_P \to \mathcal{R}_{P'}$ preserving the ramification indices, *i.e.*, such that

$$I_{Q_{P,i}}(C \cap \overline{PQ_{P,i}}) = I_{\psi(Q_{P,i})}(C \cap \overline{P'\psi(Q_{P,i})}) \quad \forall\, i = 1,\dots,s$$

Proof. Let $P' \neq P$ be two distinct inner Galois points. The intersection of the line $\overline{PP'}$ with C consists of exactly d points. Indeed, if it was not we would have $I_{P'}(C \cap \overline{PP'}) > 1$, from which it follows that $\overline{PP'} = T_{P'}C$; but since P' is also an inner Galois point, it is a total flex (cf. Corollary 1): $T_{P'}C \cap C$ consists only of P'; and this is in contradiction with $P \in C \cap \overline{PP'}$ also. The first conclusion now follows from the fact that G_P acts transitively on $(C \cap \overline{PP'}) \setminus \{P\}$ together with Proposition 1.

For the remaining, take 3 distinct inner Galois points P, P' and P'' on the same line. This is possible because any line joining two distinct inner Galois points will

intersect the curve in exactly $d \geq 4$ points, as was just proved above. Now from the transitiveness of the action of $G_{P''}$ on $(C \cap \overline{PP'}) \setminus \{P''\}$, there exists $\psi \in G_{P''}$ such that $\psi(P) = P'$. This ψ is the bijection we sought.

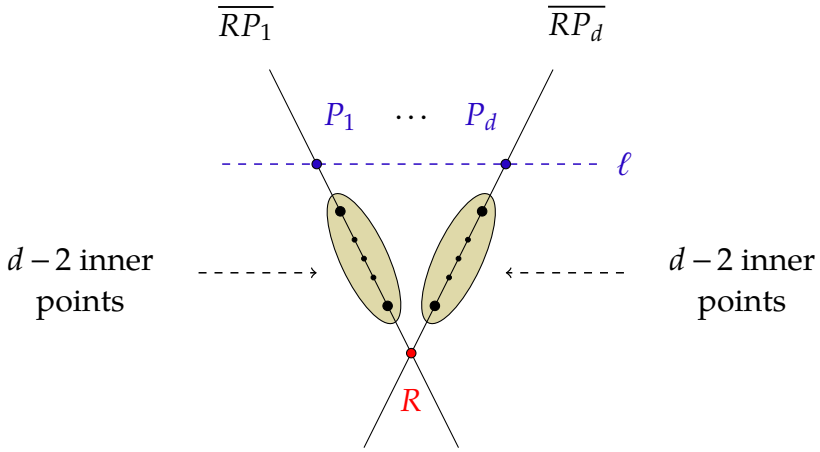
□

The next proposition has the same "spirit" of the discussion around (3.14), *i.e.*, they are mathematically quite similar (cf. (FUKASAWA, 2010, Proposition 1)).

Proposition 11. If $\delta(C) \geq d$ and C is not projectively equivalent to the Hermitian curve, then $\delta(C) = d$ and all these inner points are collinear.

Proof. Lemma 6 allows us to suppose that there are d inner points $P_1 \stackrel{\text{def}}{=} P, P_2, \ldots, P_d \in \delta(C)$ all contained on the same line ℓ. Note that $\{P_1, \ldots, P_d\} = C \cap \ell$, so that if $R \in \Delta(C) \setminus \{P_1, \ldots, P_d\}$ then R does not lie on ℓ. We suppose such a point R exists and will derive a contradiction using (3.9).

By Lemma 6 again, each line $\overline{RP_i}$ contains d inner Galois points, for $i = 1, \ldots, d$. Once R is the only point these lines share, we will then have that $\delta(C) \geq d(d-1)+1$, and recall that, by Corollary 1, they are all total flexes, *i.e.*, $(d-q)$-flexes.



Applying (3.9), we get

$$(d(d-1)+1)(d-q) \leq d((q+1)d-3q) \tag{3.17}$$

At the end of the previous section, we saw that $2 < q < d-1$ implies that $d > 2q$. Under the hypotheses of the present section, $q = 2$ can happen, so the inequality must now be written as $d \geq 2q$, as the reader may check. We now show that from (3.17) it follows that $d < 2q$, giving the contradiction we wanted and, thus, finishing the proof. First, let us rewrite (3.17) as

$$h(d) \stackrel{\text{def}}{=} d^3 - (2q+2)d^2 + (4q+1)d - q \leq 0 \tag{3.18}$$

where h is to be seen as a function $h : \mathbb{R}_{\geq 4} \to \mathbb{R}$ in the variable d. We have that $h'(d) > 0$ for all $d > q + \frac{1}{2}$. In particular h is (strictly) increasing for all $d \geq 2q$, and since $h(2q) = q > 0$ we see that in order for (3.18) to be true it is necessary that $d < 2q$, and we are done.

□

From now on, we will denote the d inner Galois points that a curve under the conditions of Proposition 11 has by $P \stackrel{\text{def}}{=} P_1, \ldots, P_d$, and the line joining all them by ℓ_{Gal}. The next result shows that $\delta(C) = d$ cannot happen if $l \geq 3$ (cf. (FUKASAWA, 2010, Proposition 2)).

Proposition 12. If $l \geq 3$, then $\delta(C) \leq 1$.

Proof. Suppose $\delta(C) \geq 2$. Then by Lemma 6 and Proposition 11 we have that $\delta(C) = d$ (notice that $l \geq 2$ implies that C cannot be a Hermitian curve). We do not yet suppose $l \geq 3$ for what comes next, just $l \geq 2$. It will be emphatically stated when the assumption $l \geq 3$ should be done. As $l \geq 2$, the cyclic subgroup C_l of G_P is not trivial, and hence the line ℓ_τ exists (recall it is given by $X = 0$). We claim that there exists a point $R_0 \in C \cap \ell_\tau$ such that it is fixed by C_l and by no other $\sigma \in G_P \setminus C_l$. Indeed, all points of ℓ_τ are fixed by C_l, by the mere definition of this line. Note that $C \cap \ell_\tau$ consists of d distinct points: they correspond exactly to the roots of $G_d(T, 1) = 0$ (cf. (3.15)), which has d distinct roots. If $R \in C \cap \ell_\tau$ if fixed by some $\gamma = (a, b)\tau^i \notin C_l$, then it is clearly also fixed by $(a, b) \in C_p^e$, from which it follows that $R \in \ell_{(a,b)}$ too. Note that the line ℓ_τ is different from any of the lines $\ell_{(a,b)}$: $P \notin \ell_\tau$ while $P \in \ell_{(a,b)}$. From all that has been said, we can conclude that there can be as many points $R \in C \cap \ell_\tau$ that are also fixed by some $\gamma \in G_P \setminus C_l$ as there are elements $(a, b) \in C_p^e$, but no more. Once there are p^e elements in C_p^e and d points in $C \cap \ell_\tau$, from the last assertion there are *at least* $d - p^e$ points on $C \cap \ell_\tau$ that are fixed only by C_l. But

$$d - 1 = p^e l \rightsquigarrow d - p^e = p^e(l - 1) + 1 \geq 1$$

and therefore there is at least one element in $C \cap \ell_\tau$ fixed by C_l only (actually, there will be at least $p^e + 1$ such points, for it holds that $l \geq 2$). The claim is thus proved.

Recall also that for any $R \in C \cap \ell_\tau$ we have $\overline{PR} = T_R C$. For the point R_0 as above, it then holds that

$$I_{R_0}(C \cap \overline{PR_0}) = I_{R_0}(C \cap T_{R_0} C) = |G_P(R_0)| = |C_l| = l \tag{3.19}$$

(3.19) implies that $l \geq q$. Now we must assume that $l \geq 3$. In this case (3.19) implies the stronger inequality $l > q$: if $q = 2$, then clearly $l \geq 3 \Rightarrow l > q$, and if $q > 2$, q is a power of p while l is not divisible by it, and we get $l > q$ again (note also that if $l = 2$, then it must be $q = 2$).

Take any $R \in C \cap \ell_\tau$ and suppose $|G_P(R)| = p^a \cdot l$ for some $a \geq 0$. By Lemma 5 it follows that the intersection of $C \setminus \{P\}$ with the line $\overline{PR} = T_R C$ consists of p^{e-a} points, and all of them are $(p^a l - q)$-flexes. Since $p^{e-a}(p^a l - q) \geq p^e(l-q)$, these points will contribute with at least $p^e(l-q)$ to the degree of the divisor $\mathcal{W}(C)$, as in (3.9). Let $\mathcal{F}_P \stackrel{\text{def}}{=} \{(C \cap \overline{PR}) \setminus \{P\} \mid R \in C \cap \ell_\tau\}$. It should be clear that if $P \neq P'$ are distinct inner Galois points, then $\mathcal{F}_P \cap \mathcal{F}_{P'} = \emptyset$, otherwise, for $Q \in \mathcal{F}_P \cap \mathcal{F}_{P'}$, we would have

$$\overline{PQ} = \overline{P'Q} \rightsquigarrow \overline{PQ} = T_Q C = \overline{PP'} = \ell_{\text{Gal}}$$

But ℓ_{Gal} intersects C in exactly d points, while $T_Q C$, being a tangent line to C, intersects C in fewer than d points.

Recall that for each point $R \in C \cap \ell_\tau$, the points $C \cap \overline{PR} \setminus \{P\}$ will give a contribution of at least $p^e(l-q)$ to the degree of $\mathcal{W}(C)$. Since there are d points in $C \cap \ell_\tau$ we conclude that the contribution, to the same quantity, of all points in $\mathcal{F}_P$ will be at least $dp^e(l-q)$ (note that if $R \neq R'$ are both in $C \cap \ell_\tau$, then $(C \cap \overline{PR}) \cap (C \cap \overline{PR'}) = \{P\}$ only). Taking into account the contribution coming from the inner point P itself, which is a total flex (cf. Corollary 1), we get a total contribution of at least $(d-q) + dp^e(l-q)$ associated with $\mathcal{F}_P$ and P. But as we saw in the previous paragraph, $\mathcal{F}_P \cap \mathcal{F}_{P'} = \emptyset$, and once there are d inner Galois points, (3.9) finally gives

$$d((d-q) + dp^e(l-q)) \leq d((q+1)d - 3q)$$

which we rewrite as

$$d(p^e(l-q) - q) + 2q \leq 0 \tag{3.20}$$

By the inequality $l > q$, we have $p^e(l-q) \geq p^e$. We also have that $l | (p^e - 1)$ (cf. item 2 of Theorem 3), from which we obtain $p^e > p^e - 1 \geq l > q$. Combining $p^e(l-q) \geq p^e$ with $p^e > q$ results in $p^e(l-q) - q > 0$. But then $d(p^e(l-q) - q) + 2q$ is a (strictly) positive integer, contrary to (3.20). And the proof is finally finished.

□

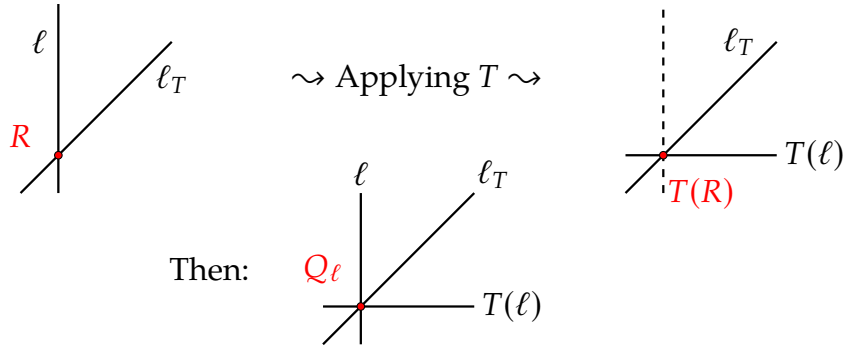
The lemma below, albeit being trivial, will prove to be of great value in making the proof of Proposition 13 less intricate.

Lemma 7. Let $T \neq \text{id}$ be a projective transformation of $\mathbb{P}^2$ which fixes all points of a line ℓ_T. Let $\ell \neq \ell_T$ be any line not fixed by T, *i.e.*, $T(\ell) \neq \ell$. Then

$$Q_\ell \stackrel{\text{def}}{=} \ell \cap T(\ell) \in \ell_T$$

and, in particular, Q_ℓ is fixed by T, *i.e.*, $T(Q_\ell) = Q_\ell$.

Proof. Take $R = \ell \cap \ell_T$. Then $T(R) = R$, since $R \in \ell_T$. But $T(R) \in T(\ell)$, since $R \in \ell$. Therefore $T(R) = R \in T(\ell) \cap \ell_T$; and with $R \in \ell$ and $R \in T(\ell)$, we conclude that $R \in \ell \cap T(\ell) = Q_\ell$. The following may help visualize the situation.



□

The next proposition corresponds to (FUKASAWA, 2010, Proposition 3) and it will be used to complete Proposition 10 for the cases $p > 2$ and $l = 1$.

Proposition 13. Suppose $\delta(C) = d$ and also that there exists $(a, b) \in C_p^e \setminus \{\mathrm{id}\} \subset G_P \setminus \{\mathrm{id}\}$ such that $\ell_{(a,b)} \neq T_P C$. Then there exist at least $d-2$ tangent lines T to C such that

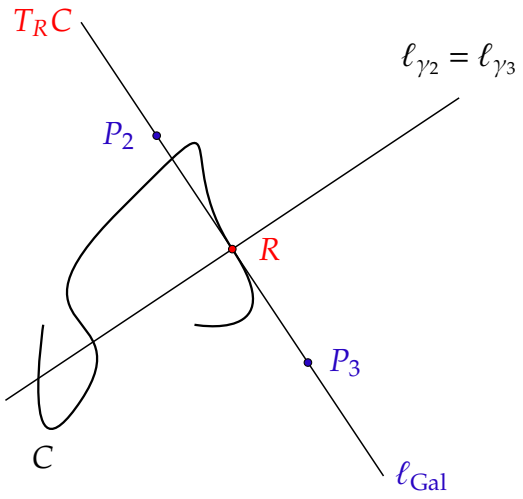
1. each T pass through P_d and
2. $I_Q(C \cap T)$ is divisible by p for any $Q \in (C \cap T) \setminus \{P_d\}$.

In particular, these imply that $l = 1$ and $p = 2$.

Remark 7. As will become clear in the proof, and as is expected, Proposition 13 holds no matter what inner point $P_i \neq P$ we take in place of P_d. However, this will be of no importance for what comes.

Proof. Let $(a, b) \in G_P \setminus \{\mathrm{id}\}$ be as above. Remind that, once $(a, b) \in C_p^e$, we have that $P \in \ell_{(a,b)}$ and also that the line $\ell_{(a,b)}$ is a tangent line to C such that the intersection multiplicity $I_Q(C \cap \ell_{(a,b)})$ is divisible by p for any $Q \in (C \cap \ell_{(a,b)}) \setminus \{P\}$ (cf. (3.16) and the discussion following it). Take $\gamma_2 \in G_{P_2}$ and $\gamma_3 \in G_{P_3}$ such that $\gamma_2(P) = P_d = \gamma_3(P)$; this is possible because $\delta(C) = d \geq 4$ and because G_{P_i} acts transitively on $\Delta(C) \setminus \{P_i\}$. Items 1 and 2 will be proven if we show that $\gamma_2(\ell_{(a,b)}) \neq \gamma_3(\ell_{(a,b)})$. Indeed, by showing that $\gamma_2(\ell_{(a,b)}) \neq \gamma_3(\ell_{(a,b)})$ it follows, by repetition of argument, that the $d-2$ lines $\gamma_i(\ell_{(a,b)})$ are all distinct, where $\gamma_i \in G_{P_i}$, $i = 2, \ldots, d-1$, takes P to P_d. It is clear that item 1 and item 2 will hold: all γ_i are projective transformations: they take tangent lines to tangent lines and leave invariant all intersection multiplicities. Hence, we go on to show that $\gamma_2(\ell_{(a,b)}) \neq \gamma_3(\ell_{(a,b)})$.

The first thing to notice is: $\ell_{\gamma_2} \neq \ell_{\gamma_3}$. Suppose not, and take any $R \in C \cap \ell_{\gamma_2} = C \cap \ell_{\gamma_3}$. From $R \in C \cap \ell_{\gamma_2}$ we have that $P_2 \in T_R C$, and from $C \cap \ell_{\gamma_3}$, that $P_3 \in T_R C$. But then $T_R C = \overline{P_2 P_3} = \ell_{\mathrm{Gal}}$, which is a contradiction, for ℓ_{Gal} is not a tangent line to C: it intersects the curve exactly in the d inner points (cf. below).

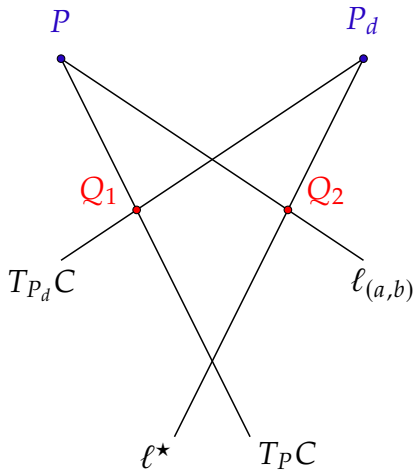


T_RC is tangent to C

WHEREAS

ℓ_{Gal} is not

Recall that inner Galois points are total flexes, so that $T_PC \neq T_{P_d}C$ and thus the point $Q_1 \overset{\text{def}}{=} T_PC \cap T_{P_d}C$ is well-defined. Since $\gamma_2(T_PC) = T_{P_d}C$, Lemma 7 implies that $Q_1 \in \ell_{\gamma_2}$, and also that $Q_1 \in \ell_{\gamma_3}$, because $\gamma_3(T_PC) = T_{P_d}C$ as well; hence $Q_1 = T_PC \cap T_{P_d}C = \ell_{\gamma_2} \cap \ell_{\gamma_3}$. Suppose, for us to derive a contradiction, that it was $\gamma_2(\ell_{(a,b)}) = \gamma_3(\ell_{(a,b)})$, and denote this line by $\ell^\star$. Let $Q_2 = \ell_{(a,b)} \cap \ell^\star$. Using Lemma 7 again (notice that $\ell_{(a,b)}$ and $\gamma_2(\ell_{(a,b)})$ are distinct lines: the former pass through P and not through P_d while the latter pass through P_d and not through P), we conclude that $Q_2 = \ell_{\gamma_2} \cap \ell_{\gamma_3}$. Since $Q_2 \in \ell_{(a,b)}$ and $\ell_{(a,b)} \neq T_PC$, by our initial hypothesis, it follows that $Q_2 \notin T_PC$ (note: $\ell_{(a,b)} \cap T_PC = \{P\}$). But $Q_1 = \ell_{\gamma_2} \cap \ell_{\gamma_3}$ too, and $Q_1 \in T_PC$. The points Q_1 and Q_2 are, therefore, distinct: $Q_1 \in T_PC$ while $Q_2 \notin T_PC$; on the other hand, and simultaneously, they are equal, once $Q_1 = \ell_{\gamma_2} \cap \ell_{\gamma_3} = Q_2$, and $\ell_{\gamma_2} \neq \ell_{\gamma_3}$ (cf. below).



This contradiction finishes, therefore, item 1 and item 2; now we proceed to show that $p = 2$ and $l = 1$. The $d-2$ lines we just proved to exist are, all of them, of the form $\ell_{(s,t)}$ for some $\mathrm{id} \neq (s,t) \in C_p^e \leq G_{P_d}$. In fact, each of these $d-2$ lines is given by $\gamma_i(\ell_{(a,b)})$ for some $\gamma_i \in G_{P_i}$, as was just proved in the lines above; once $\ell_{(a,b)}$ is the line associated to $(a,b) \in C_p^e \leq G_P$, the reader can easily check that $\gamma_i(\ell_{(a,b)})$ is the line

associated to $\gamma_i(a,b)\gamma_i^{-1} \in C_p^e \leq G_{P_d}$. And from the fact that these $d-2$ lines are all distinct, we conclude that there are at least $d-2$ elements in $C_p^e \setminus \{1\}$, hence

$$d-1 = |G_{P_d}| \geq |C_p^e| \geq d-1$$

Therefore $G_{P_d} \simeq C_p^e$, from which it follows that $l = 1$. With this new information in mind, it now follows that those $d-2$ lines are exactly all of the lines ℓ_σ, for $\sigma \in G_{P_d} \setminus \{\mathrm{id}\}$. Moreover, there are no more tangent lines to C passing through P_d apart from those just cited: any tangent line to C passing through P_d would necessarily be of the form ℓ_γ for some $\gamma \in G_{P_d}$. Hence, where it is written "there exist **at least** $d-2$ tangent lines T to C such that..." we must now read "there exist **exactly** $d-2$ tangent lines T to C such that...". In particular, $\ell_\sigma \neq \ell_{\sigma'}$ for $\sigma \neq \sigma'$. Take $\sigma \in G_{P_d}$ and suppose $\sigma^2 \neq \mathrm{id}$. It is then clear that $\ell_\sigma = \ell_{\sigma^2}$: if $P \in \ell_\sigma$ then $\sigma^2(P) = \sigma(\sigma(P)) = \sigma(P) = P$, and hence all points in ℓ_σ are also fixed by σ^2; therefore we have $\ell_\sigma \subset \ell_{\sigma^2}$, and the equality clearly follows. But $\sigma \neq \sigma^2$ (otherwise $\sigma = \mathrm{id}$), so that the lines ℓ_σ and ℓ_{σ^2} should be distinct, as observed earlier. This contradiction leads us to conclude that $\sigma^2 = \mathrm{id}$ for all $\sigma \in G_{P_d}$. Therefore the exponent of G_{P_d}, which is p, is exactly 2. The proof is thus finished.

□

We are now going to show item 1 of Proposition 10 for $p \geq 3$ and $l = 1$ (cf. (FUKASAWA, 2010, p. 14)). We note that, in such cases, the group G_P reduces to C_p^e, and (3.15) to

$$Zf(X,Y,Z) + G_d(Y,Z) = 0 \tag{3.21}$$

Also within this situation, and under the assumption $\delta(C) = d$, Proposition 13 implies that $\ell_{(a,b)} = T_P C$ for any $(a,b) \in G_P \simeq C_p^e$. But $T_P C$ is given by $Z = 0$ (cf. (3.21)). So in order for $\ell_{(a,b)} : aY + bZ = 0$ to be $Z = 0$ the "first coordinates" of all elements G_P must vanish, *i.e.*, we must have $a = 0$ for all $(a,b) \in G_P$. Looking back at the proof of item 2 of Theorem 3, we have that the polynomial $f(X,Y,Z)$ is given by

$$f(X,Y,Z) = \prod_{(a,b)\in C_p^e} (X - aY - bZ) \tag{3.22}$$

We just saw that, under the present hypotheses, $a = 0$ for all $(a,b) \in C_p^e$; hence (3.22) becomes

$$f(X,Z) = \prod_{(0,b)\in C_p^e} (X - bZ) \tag{3.23}$$

which does not depend on Y. We now claim that the tangent lines at all of the d inner Galois points are concurrent. To see this, take $Q \stackrel{\text{def}}{=} T_P C \cap T_{P_2} C$. Since, by Proposition 13, $\ell_{(a,b)} = T_P C$ for all $(a,b) \in G_P$ (the following does not make use of $a = 0$), we have, from the definition of $\ell_{(a,b)}$, that $(a,b)(Q) = Q$. But once G_P acts transitively on the set $C \cap \ell_{\mathrm{Gal}} = \{P_1, \ldots, P_d\}$, we have that

$$Q = (a,b)(Q) = (a,b)(T_P C \cap T_{P_2} C) = (a,b)(T_P C) \cap (a,b)(T_{P_2} C) = T_P C \cap T_{P_i} C$$

where $(a,b)(P_2) = P_i$. Thus, $Q = T_{P_i}C \cap T_{P_j}C$ for any $i \neq j$, *i.e.*, the lines $T_{P_i}C$, $i = 1,\ldots,d$, are concurrent, which is what was claimed. As $T_PC : Z = 0$, and as Q is not one of the inner Galois points, it follows that Q is given by $Q = (x^\star : 1 : 0)$ for some $x^\star \in k$. We may suppose, with no loss of generality, that $x^\star = 0$. Indeed, take the projective transformation

$$T_{x^\star} \stackrel{\text{def}}{=} \begin{pmatrix} 1 & -x^\star & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

which corresponds, in our notation, to $(-x^\star, 0)$; its inverse is, therefore, $(x^\star, 0)$. This transformation $T_{x^\star}$ takes Q to $(0:1:0)$, and it fixes $P = (1:0:0)$; it also leaves G_P unchanged: $(-x^\star,0)\circ(a,b)\circ(x^\star,0) = (a,b)$. Finally, it takes C to the curve given by the following equation

$$\begin{aligned} Zf(X + x^\star Y, Y, Z) + G_d(Y,Z) = Zf(X,Y,Z) + G_d(Y,Z) + f(x^\star Y, Y, Z) = \\ = Zf(X,Y,Z) + \tilde{G}_d(Y,Z) = 0 \end{aligned}$$

which is an equation of the same type of (3.21). Notice that in the equation above we used the "additiveness" of $f(X,Y,Z)$ with respect to the variable X. Summing up the preceding considerations, we have that C is given by (cf. (3.23))

$$Zf(X,Z) + G_d(Y,Z) = 0 \tag{3.24}$$

with $Z \nmid G_d(Y,Z)$, *i.e.*, the coefficient of Y^d in $G_d(Y,Z)$ does not vanish, and $Q = (0:1:0)$ is the common point of the tangent lines to all of the d inner Galois points. Consider now the projection $\pi_Q : C \to \ell_Y$ from Q to $(Q \not\ni)\ell_Y : Y = 0$. Notice that $Q \notin C$: any line $T_{P_i}C$ intersects C only at P_i. From $Q \notin C$, we see that π_Q has degree d which is $\not\equiv 0 \bmod p$. Notice also that each inner Galois point P_i is totally ramified with respect to π_Q: the smoothness of C guarantees that its ramification index is exactly $I_{P_i}(C \cap \overline{P_iQ}) = I_{P_i}(C \cap T_{P_i}C) = d$. Once the ramification indices associated to the inner Galois points are equal to d, which is $\not\equiv 0 \bmod p$, and once $\delta(C) = d$, the different divisor of π_Q, $\mathrm{Diff}(\pi_Q)$, will have degree at least $d(d-1)$ (cf. (STICHTENOTH, 2009, Theorem 3.5.1 and Definition 3.4.3)). Applying Hurwitz's genus formula (cf. (STICHTENOTH, 2009, Theorem 3.4.13)) for π_Q gives (remind that the genus of C is $(d-1)(d-2)/2$: it is a degree d non-singular curve)

$$2 \cdot \frac{(d-1)(d-2)}{2} - 2 = d(2\cdot 0 - 2) + \deg \mathrm{Diff}(\pi_Q) \rightsquigarrow \deg \mathrm{Diff}(\pi_Q) = d(d-1)$$

Hence, the only ramified points with respect to π_Q are the inner Galois points, and they are all *totally* ramified. Now, the ramified points of C with respect to π_Q are exactly the points of C whose tangent lines pass through Q. Any line through Q is given by $t_zX - t_xZ = 0$ for some t_z and $t_x \in k$ (not both of them vanishing), and its points are thus $(t_x : T : t_z)$ and $(0:1:0)$, for $T \in k$ a parameter. Let us exclude, for the moment,

the point P from the discussion: it is the only point of C in the line $Z = 0$; as we will only consider lines through Q different from $Z = 0$, we have that $t_z \neq 0$, and we can describe the points of the line $\ell_{t_x} : t_z X - t_x Z = 0$ that are contained in the affine chart $Z = 1$ by $(\tilde{t}_x : T : 1)$, for $T \in k$. We will denote $\tilde{t}_x = t_x/t_z$ by t_x only. Let $g(T) \stackrel{\text{def}}{=} G_d(T, 1)$. Substituting the preceding parametrization on (3.24) gives

$$f(t_x, 1) + g(T) = 0 \tag{3.25}$$

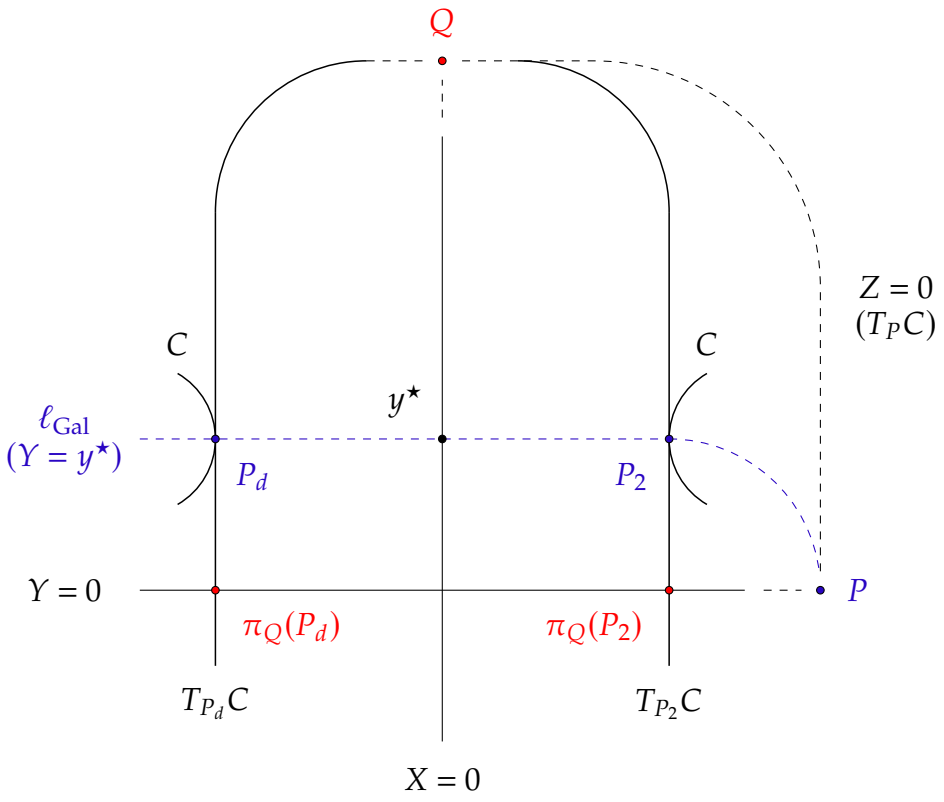
which is a degree d polynomial on T. Its roots give the (y coordinates of the) points on $C \cap \ell_{t_x}$; any repeated root corresponds to a point R for which ℓ_{t_x} is tangent to C at it, and the multiplicity of the root (as root of the polynomial (3.25)) corresponds exactly to the intersection multiplicity $I_R(C \cap \ell_{t_x})$. This implies that if ℓ_{t_x} is the tangent line to a total flex of C, (3.25) will admit only one root $T = y_{t_x}$. As it turns out, this happens to be the case for the points $P_2, \ldots, P_d$. For the point P_i, (3.25) will therefore read

$$f(t_{x_i}, 1) + g(T) = c_i \cdot (T - y_i)^d \tag{3.26}$$

where we write y_i instead of $y_{t_{x_i}}$. Taking the (formal) derivative, with respect to T, of both sides of (3.26), we get (recall that $d \equiv 1 \bmod p$)

$$g'(T) = c_i \cdot (T - y_i)^{d-1} \quad \forall\, i = 2, \ldots, d \tag{3.27}$$

The left hand side of (3.27) does not depend on i. From this we conclude that $y_i = y^\star$ and $c_i = c^\star$ for all $i = 2, \ldots, d$. The following must be pointed out: the fact that $y_i = y^\star$ for all $i = 2, \ldots, d$ tells us that the Y coordinates of the inner Galois points contained in the affine chart $Z = 1$ are all the same, namely $y^\star$; this should already had been clear: ℓ_{Gal}, being a line through P distinct from $Z = 0$, is given by $\alpha Y - \beta Z = 0$, for some $\alpha \neq 0$. Consequently, the line ℓ_{Gal} is given by $Y - y^\star Z = 0$.



Hence we may rewrite (3.26) as

$$g(T) - c^\star \cdot (T - y^\star)^d = f(t_{x_i}, 1) \tag{3.28}$$

Again, the left hand side of (3.28) does not depend on i, so we must have $f(t_{x_i}, 1) = c_0$ for all $i = 2, \ldots, d$, and we may finally write

$$g(T) = c^\star \cdot (T - y^\star)^d + c_0 \rightsquigarrow G_d(Y, Z) = c^\star (Y - y^\star Z)^d + c_0 Z^d$$

The following projective transformation

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & y^\star \\ 0 & 0 & 1 \end{pmatrix}$$

does not affect at all our previous assumptions. In fact, it leaves $Zf(X, Z)$ unchanged, and it also leaves G_P unchanged:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & y^\star \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -y^\star \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

But it takes $G_d(Y, Z)$ to $c^\star Y^d + c_0 Z^d$. After another projective change of the Y coordinate only, we may assume that C has equation

$$Zf(X, Z) + Y^d + c_0 Z^d = 0 \tag{3.29}$$

One last projective transformation, this time given by (cf. a similar discussion in page 63)

$$\begin{pmatrix} 1 & 0 & -s_0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where s_0 is such that $f(s_0,1) = -c_0$, and we may finally assume that C is given by (cf. (3.29))

$$Zf(X+s_0Z,Z)+Y^d+c_0Z^d = Zf(X,Z)+Y^d+Z^d(f(s_0,1)+c_0) = Zf(X,Z)+Y^d = 0 \quad (3.30)$$

Note that, since $\Delta(C) = C \cap \ell_{\text{Gal}}$ and $\ell_{\text{Gal}} : Y = 0$, all the inner Galois points are given by the roots of $Zf(X,Z) = 0$, *i.e.*, they are $(1:0:0)$ and $(b:0:1)$ for every $(0,b) \in G_P$. For $b = 0$, which corresponds to the identity element of G_P, this means that $P' \stackrel{\text{def}}{=} (0:0:1)$ is one of the inner Galois points that are distinct from P; recall that the tangent line at any inner Galois point pass through Q, so that we have that $T_{P'}C$ is given by $X = 0$. We will consider now the projection $\pi_{P'}$ from P'. If we remind that the lines $\ell_{(0,b)}$ for $(0,b) \in G_P$ are all equal to the line T_PC, and that any ramified point with respect to π_P should lie in one of those lines, we conclude that the only ramified place with respect to π_P is P itself and it is totally ramified, because $T_PC \cap C = \{P\}$ only. Lemma 6 then implies that P' is the only ramified point with respect to $\pi_{P'}$. In complete analogy with what was done in the case of π_Q (cf. page 63), we have that any ramified point with respect to $\pi_{P'}$ lying in the affine chart $X = 1$ will be associated to a repeated root of

$$Tf(1,T)+t_y^d = 0 \quad (3.31)$$

The converse is also true. But if (3.31) has any repeated root r, then r is also a root of the derivative of the polynomial (considered as a polynomial in the variable T) in the left hand side of (3.31). Now, observe that this derivative is independent of the parameter t_y: it is just the derivative of the polynomial $h(T) \stackrel{\text{def}}{=} Tf(1,T)$. Suppose that $h'(T)$ has roots, *i.e.*, that $h'(T)$ is not a non-zero constant. Take r to be such a root. It is, then, clearly possible to find $t_y \in k$ such that r is also a root of (3.31): it suffices to take it such that $-t_y^d = h(r)$. Therefore, it holds that the ramified points under consideration (*i.e.*, those in the affine chart $X = 1$) are all given by the roots of $h'(T)$, and conversely. However, as we have already seen, the only ramified point with respect to $\pi_{P'}$ is P' itself, and it is not contained in affine chart $X = 1$. From this, we conclude that $h'(T)$ has no roots at all: it is a non-zero constant. Let us take a closer look at this polynomial $h(T) = Tf(1,T)$. The polynomial $f(X,Z)$, being an additive polynomial in the variable X of degree $d-1 = p^e$, and homogeneous when both variables are considered, may be written as (cf. (GOSS, 1998, Proposition 1.1.5 and Theorem 1.2.1))

$$f(X,Z) = X^{p^e} + a_{e-1}X^{p^e}Z^{p^e-p^{e-1}} + \ldots + a_1X^pZ^{p^e-p} + a_0XZ^{p^e-1} \quad (3.32)$$

from which we may write (recall that $h(T) = Tf(1,T)$)

$$h'(T) = a_1 T^{p^e - p} + \ldots + a_{e-1} T^{p^e - p^{e-1}} + 1$$

So in order for $h'(T)$ to be a non-zero constant, we must have $a_1 = \ldots = a_{e-1} = 0$. Recall that $f(X,Z)$ is separable, a condition equivalent to $a_0 \neq 0$ (cf. (3.32)). Summing all up, we have that C is given by the following equation (cf. (3.30))

$$ZX^{p^e} + a_0 Z^{p^e} X + Y^{p^e+1} = 0, \quad \text{for some } a_0 \neq 0$$

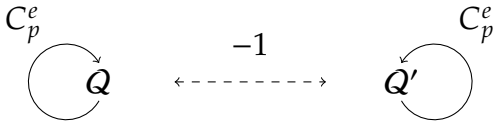
whose projective equivalence to the Hermitian curve is left to the reader to check. What we just showed is: for $p \geq 3$ and $l = 1$, if $\delta(C) \geq 2$ then C is projectively equivalent to the Hermitian curve. This, together with Lemma 6 allows us to state (cf. (FUKASAWA, 2010, Proposition 4))

Proposition 14. Suppose $p \geq 3$ and $l = 1$. If C is not projectively equivalent to the Hermitian curve then $\delta(C) \leq 1$.

It now remains, for the proof of Proposition 10 to be completed, to consider the case $l = 2$ (cf. (FUKASAWA, 2010, p. 14)). The first thing to notice is that if $l = 2$ then p cannot be 2; thus, the curves considered in what comes have degree $2p^e + 1$ for $p \geq 3$ and $e \geq 1$. Suppose $\delta(C) = d$; Proposition 13 again implies that $\ell_{(a,b)} = T_P C$ for all $(a,b) \in C_p^e \leq G_P$, with $(a,b) \neq (0,0)$. Therefore, as happened with the case $l = 1$ (cf. (3.23)), we again have that the first coordinates of the elements $(a,b) \in C_p^e$ must vanish, so that $f(X,Y,Z)$ does not depend on Y; (3.15) can then be written as

$$Zf(X,Z)^2 + G_d(Y,Z) = 0 \tag{3.33}$$

In analogy with what we did previously in the case $l = 1$, let us consider the set $\{T_P C \cap T_{P_i} C \mid 2 \leq i \leq d\}$. There are two cosets of C_p^e in $G_P \simeq C_p^e \rtimes C_2$; we denote $C_2 = \{1, -1\}$ and, therefore, these two cosets just mentioned by $\pm C_p^e$. Let us consider the orbit of P_2 by the action of G_P. The action of G_P in the set $\Delta(C) \setminus \{P\}$ is transitive, hence the orbit of P_2 by the elements in the coset C_p^e will consist of $|G_P|/2 = (d-1)/2 = p^e$ elements, which we denote by $\mathcal{Q} \stackrel{\text{def}}{=} \{Q_1 \stackrel{\text{def}}{=} P_2, \ldots, Q_{p^e}\}$. The other p^e elements, those in the orbit of P_2 under the action of $-C_p^e$, will be denoted by $\mathcal{Q}' \stackrel{\text{def}}{=} \{Q'_1, \ldots, Q'_{p^e}\}$ in such a way that $Q'_k = (-1)(Q_k)$ for all $k = 2, \ldots, p^e$, where the symbol -1 just used is to be understood as being the non-identity element of C_2. The important thing to notice here is this: any two elements in $\mathcal{Q}$ are taken into one another by an element in C_p^e, and the same holds for $\mathcal{Q}'$.



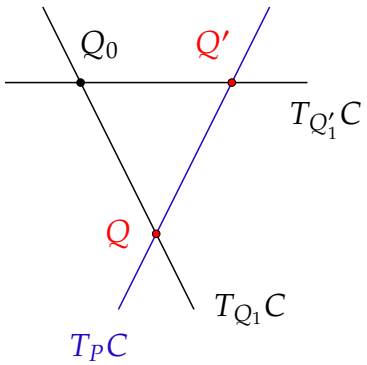
Since any $(a,b) \in C_p^e$ fixes all the points in the line $\ell_{(a,b)} = T_P C$, we have that

$$T_P C \cap T_{Q_i} C = (a,b)(T_P C \cap T_{Q_i} C) = T_P C \cap T_{Q_j} C$$

and also that

$$T_P C \cap T_{Q'_i} C = (a,b)(T_P C \cap T_{Q'_i} C) = T_P C \cap T_{Q'_j} C$$

With all this in hand, it is now clear that the set $\{T_P C \cap T_{P_i} C \mid 2 \leq i \leq d\}$ can consist of at most 2 points: one associated with the inner points in $\boldsymbol{Q}$, which we denote by Q, and another associated with those in $\boldsymbol{Q}'$, which we denote by Q'. Suppose $Q \neq Q'$; and note that, by what we defined just now, $Q = T_P C \cap T_{Q_1} C$ and $Q' = T_P C \cap T_{Q'_1} C$. Let $Q_0 \overset{\text{def}}{=} T_{Q_1} C \cap T_{Q'_1} C$, and note that $Q_0 \notin T_P C$ (otherwise $Q = Q'$). Consider the group $C_p^e \leq G_{Q_1}$. For any $\sigma \neq \mathrm{id}$ in such group, $\ell_\sigma = T_{Q_1} C$, by Proposition 13; in particular σ fixes Q_0. The point $Q_\sigma \overset{\text{def}}{=} \sigma(Q'_1)$ is an inner Galois point different from Q_1 and from Q'_1, because the G_{Q_1} acts transitively on $\Delta(C) \setminus \{Q_1\}$. By Lemma 7 we have that $Q_0 \in T_{Q_\sigma} C$; in particular $Q_\sigma \neq P$: if not, it would be $Q_0 \in T_P C$, which is not the case, as was just seen a few lines above. Thus, either $Q = T_P C \cap T_{Q_\sigma} C$ or $Q' = T_P C \cap T_{Q_\sigma} C$, but in both scenarios we get a contradiction; let us see why. If $Q = T_P C \cap T_{Q_\sigma} C$, then $T_{Q_\sigma} C = \overline{Q_0 Q} = T_{Q_1} C$, which implies $Q_\sigma = Q_1$ (because inner points are total flexes); but $Q_\sigma = \sigma(Q'_1)$ (recall $\sigma \in G_{Q_1}$) cannot be Q_1, unless it was $Q'_1 = Q_1$, which is not. If $Q' = T_P C \cap T_{Q_\sigma} C$, then in the same way we would conclude that $Q_\sigma = Q'_1$, which, again, is not since $\sigma \neq \mathrm{id}$ and the action of G_{Q_1} in $\Delta(C) \setminus \{Q_1\}$ is transitive.



Hence, $Q = Q'$, *i.e.*, the tangent lines to all inner Galois points are concurrent, like they were in the case of $l = 1$. Considering the projection π_Q from Q like we did in the case of $l = 1$ (cf. page 63), we are led to conclude that C is projectively equivalent to the curve given by (cf. (3.29) and (3.33))

$$Z f(X,Z)^2 + Y^d + c Z^d = 0 \tag{3.34}$$

where, again, we may write $f(X,Z)$ like in (3.32):

$$f(X,Z) = X^{p^e} + a_{e-1} X^{p^e} Z^{p^e - p^{e-1}} + \ldots + a_1 X^p Z^{p^e - p} + a_0 X Z^{p^e - 1} \tag{3.35}$$

with $a_0 \neq 0$, since $f(X,Z)$ is separable. The considerations to be done in the sequence make up the contents of (FUKASAWA, 2010, Proposition 5). In the affine chart $X = 1$, the point $P = (1:0:0)$ is the origin, and we may write the local equation of C in this chart as (where $z = Z/X$ and $y = Y/X$)

$$\phi(z) \stackrel{\text{def}}{=} z f(1,z)^2 + cz^d = -y^d \tag{3.36}$$

Once $Z = 0$ is the tangent line to C at P, the function z will not be a uniformizing parameter for C at P; we take the function y to be such parameter, and we write v_P for the (discrete) valuation, the order function of the local ring at P; hence $v_P(y) = 1$. As $Z = 0$ is the tangent line to C at P and as $I_P(C \cap T_P C) = d$, we have that $v_P(z) = d$. This equality could also be derived from (3.36). Indeed, we have that

$$v_P(z f(1,z)^2 + cz^d) = v_P(z) + v_P(f(1,z)^2 + cz^{d-1}) = v_P(z) \tag{3.37}$$

where we used $v_P(f(1,z)^2 + cz^{d-1}) = 0$, which holds since P is not a zero of the function $f(1,z)^2 + cz^{d-1}$: $f(1,0) = 1 \neq 0$. Therefore, (3.37) together with (3.36) gives

$$v_P(z) = v_P(-y^d) = d \cdot v_P(-y) = d \tag{3.38}$$

Let z' and z'' be the derivatives dz/dy and d^2z/dy^2, respectively. The usual derivatives of $\phi(z)$ and $f(1,z)$, as polynomials in z, will be denoted in the same way. Taking the derivative d/dy on both sides of (3.36) we get (it will be shown that $\phi' \neq 0$)

$$\phi' \cdot z' = -y^{d-1} \;\rightsquigarrow\; z' = -y^{d-1}/\phi' \tag{3.39}$$

And doing the same with (3.39) gives (recall that $d - 1 \equiv 0 \bmod p$)

$$\phi'' \cdot (z')^2 + \phi' z'' = 0 \tag{3.40}$$

Using (3.39) in the above (3.40), we have that

$$z'' = -\frac{\phi'' y^{2(d-1)}}{(\phi')^3} \tag{3.41}$$

Let us consider now the functions $\phi'(z)$ and $\phi''(z)$. Recalling (3.36), we have that

$$\phi'(z) = f^2 + 2 \cdot z \cdot f \cdot f' + cz^{d-1} \tag{3.42}$$

From this we see that the function $\phi'(z)$ does not vanish at P (because $f(1,0) \neq 0$), thus $v_P(\phi'(z)) = 0$; in particular $\phi'(z) \neq 0$ (cf. (3.39) and (3.40) where we divided by ϕ'). Deriving (3.42) once again, we obtain

$$\phi'' = 4f \cdot f' + 2z((f')^2 + f \cdot f'') = 2f \cdot (2f' + z f'') + 2z(f')^2 \tag{3.43}$$

And we are now led to consider the functions $(f(1,z))'$ and $(f(1,z))''$. By (3.35), we have that

$$f(1,z)' = -a_0 z^{p^e-2} \quad \text{and therefore} \quad f(1,z)'' = 2a_0 z^{p^e-3} \tag{3.44}$$

From (3.44), it follows that $2f' + zf'' = 0$; we can then rewrite (3.43) as

$$\phi'' = 2z(f')^2 = 2a_0^2 z^{2p^e-3} \tag{3.45}$$

Finally, plugging (3.45) into (3.41) gives

$$z'' = \frac{-2a_0^2 z^{2p^e-3} y^{4p^e}}{\phi'^3} \tag{3.46}$$

(3.46) tells that $z'' \neq 0$, hence the dual map of C is separable and, in particular, the generic order of contact for C is 2 (cf. Definition 6 as well as the footnote in page 52). Therefore the right hand side of (3.9) reduces to $3d(d-2)$ (cf. the discussion at the beginning of section 3.2). The d inner Galois points are total flexes, and thus $I_{P_i}(C \cap T_{P_i}C) - q(C) = d-2$ for each one of them; then, if we use (3.9) the way we were using it before, we will get

$$d(d-2) \leq 3d(d-2) \tag{3.47}$$

which is not useful at all. What happens is that

$$\binom{I_{P_i}(C \cap T_{P_i}C)}{q(C)} = \binom{d}{2} = \frac{(2p^e+1)(2p^e)}{2} \equiv 0 \bmod p$$

and therefore, by (3.10) and the fact that $I_R(C \cap T_R C) - q(C) \leq v_R(\mathcal{W}(C))$ for any $R \in C$, we conclude that $I_{P_i}(C \cap T_{P_i}C) < v_{P_i}(\mathcal{W}(C))$, so that the left hand side of (3.47) can, and will, be sharpened. The divisor $\mathcal{W}(C)$ is explicitly given by (cf. (FUKASAWA, 2008, Section 2), (FUKASAWA, 2007, Section 2) and references therein)

$$\mathcal{W}(C) = 3D + \operatorname{div}(z'') + 3\operatorname{div}(dy) \tag{3.48}$$

where D is the divisor corresponding to $C \cap \ell_\infty$, where ℓ_∞ is the line at infinity with respect to the affine chart $X = 1$, *i.e.*, $\ell_\infty : X = 0$. Once $P \notin \ell_\infty$, we have that $v_P(3D) = 0$. Also $v_P(\operatorname{div}(dy)) = 0$, since y is a uniformizing parameter at P. Hence, from (3.48), we have that

$$v_P(\mathcal{W}(C)) = v_P(\operatorname{div}(z'')) = v_P(z'') \tag{3.49}$$

Now, using (3.46) and (3.38) we can write, for the quantity appearing in (3.49),

$$v_P(\mathcal{W}(C)) = 4p^e + (2p^e - 3)(2p^e + 1) = 4p^{2e} - 3 \tag{3.50}$$

(3.50) holds also for the other inner Galois points: G_{P_i}, which consists entirely of projective transformations, acts transitively on the set $\Delta(C) \setminus \{P_i\}$ and $v_P(\mathcal{W}(C)) = v_{T(P)}(\mathcal{W}(T(C))$, for any projective transformation T. Therefore, from the preceding and from (3.50), there

will be a contribution of $d(4p^{2e}-3)$ to the degree of $\mathcal{W}(C)$, which is $3d(d-2)$, and thus (3.9) allows us to finally write (recall that $d = 2p^e+1$)

$$d(4p^{2e}-3) \leq 3d(d-2) \;\rightsquigarrow\; 4p^e \leq 6$$

which does not hold for any pair (p,e) with $p \geq 3$ and $e \geq 1$. This last contradiction finishes the proof of Proposition 10.

3.3 Even characteristic

We now investigate those non-singular curves, whose existence is possible only if $p = 2$, for which $d = \deg C = \delta(C)$ (cf. item 2 of Proposition 10). The results contained in this section are essentially the same as those in (FUKASAWA, 2013) and in (FUKASAWA, 2014), but the approach given here is our own and may, therefore, differ with the one given there in minor aspects.

Recall that the degree of any such curve is a unit more than a power of two, *i.e.*, $d = 2^n+1$. Our aim is to completely classify such curves. More specifically, we will give explicit equations, for any $n \geq 2$, of all non-singular plane curves of degree 2^n+1 with exactly 2^n+1 inner Galois points, up to projective transformation.

Recall Lemma 6 and Proposition 11: for a degree d curve in this setup to have d inner Galois points, it is necessary (and also sufficient) that it has 2 of them and that it is not projectively equivalent to the Hermitian curve.

So suppose C is a non-singular plane curve of degree $d = 2^n+1 = q+1$ (from now on, we will write q and 2^n interchangeably), with $n \geq 2$, over an algebraically closed field k of characteristic 2 that has 2 inner Galois points. We keep the notation we used throughout subsection 3.2.4 (cf. what comes after Proposition 10). Under these circumstances, $G_P \simeq C_2^n$ and each $\sigma \in G_P$ is its own inverse. Recall also (3.15): $P = (1:0:0)$ is one of the inner points, its tangent line has equation $Z = 0$ and C has equation

$$Z \cdot \left(\prod_{(\alpha,\beta)\in G_P} (X + \alpha Y + \beta Z) \right) + G_d(Y,Z) = 0 \tag{3.51}$$

Let $Q \neq P$ be another inner Galois point. Once $Q \notin T_P C$, we may write $Q = (x:y:1)$. Consider the following projective transformation

$$T_1 \overset{\text{def}}{=} \begin{pmatrix} 1 & 0 & -x \\ 0 & 1 & -y \\ 0 & 0 & 1 \end{pmatrix}; \quad \text{note that} \quad T_1^{-1} = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$$

We have that T_1

- takes Q to $(0:0:1)$,
- fixes $P = (1:0:0)$,
- fixes all the points in the line $T_P C : Z = 0$ and
- takes $(\alpha, \beta) \in G_P$ to $T_1 \circ (\alpha, \beta) \circ T_1^{-1} = (\alpha, \alpha y + \beta)$.

Therefore, after applying T_1, we may suppose the same we supposed before and, additionally, that $(0:0:1)$ is another inner Galois point. Note that the type of equation C satisfies will not change, only the roots of the additive polynomial appearing in (3.51) will do. Indeed, the equation for $T_1(C)$ will be something like

$$Z \cdot \left(\prod_{(\tilde{\alpha}, \tilde{\beta}) \in \tilde{G}_P} (X + \tilde{\alpha} Y + \tilde{\beta} Z) \right) + \tilde{G}_d(Y, Z) = 0 \tag{3.52}$$

where, as before, $\tilde{G}_P = T_1 G_P T_1^{-1}$: the matrices of the elements G_P are of the same type of those of $\tilde{G}_P$, *i.e.*, they are given by a matrix like the one below

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

for some a and $b \in k$. We will then write only G_P for the Galois group associated to P.

Now that we have $(1:0:0)$ and $(0:0:1)$ as inner points, we know that the line joining them, *viz.* ℓ_{Gal}, is given by $Y = 0$; by Proposition 11, $\Delta(C) = C \cap \ell_{\text{Gal}}$. In particular, $T_Q C : X + bY = 0$ for some $b \in k$. We can go one step further and also apply the projective transformation below

$$T_2 \stackrel{\text{def}}{=} \begin{pmatrix} 1 & -b & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

This transformation T_2

- fixes Q and P,
- does not fix all the points in the line $T_P C : Z = 0$, but leaves this line unchanged,
- takes $T_Q C : X + bY = 0$ to $X = 0$ and
- leaves G_P unchanged after conjugation.

After all these considerations, we may finally suppose that C has equation like (3.51), and that two of the inner Galois points are $(1:0:0)$ and $(0:0:1)$, with tangent lines

given by $Z = 0$ and $X = 0$, respectively. The additive polynomial in (3.51) will be denoted by what we have been denoting it hitherto, by $f(X, Y, Z)$.

From the fact that $Q = (0 : 0 : 1)$ is also an inner Galois point with respect to C with tangent line given by $X = 0$, and recalling that inner Galois points are total flexes (cf. Corollary 1), we conclude that

$$Z f(0, Y, Z) + G_d(Y, Z) = 0$$

must have $(X : Y : Z) = (0 : 0 : 1)$ as its unique root. Noting that $f(0, Y, Z) = 0$, once $X | f(X, Y, Z)$, this leads us to conclude that (afterwards a rescaling transformation)

$$G_d(Y, Z) = Y^d$$

We put this altogether in the following

Lemma 8. Let C be a non-singular plane curve of degree $2^n + 1 = q + 1$, for $n \geq 2$, defined over a field k of characteristic 2 with (at least) 2 inner Galois points. Then C is projectively equivalent to the curve given by

$$Z \prod_{(\alpha,\beta)\in G_P} (X + \alpha Y + \beta Z) + Y^{q+1} = 0$$

where the pairs (α, β) constitute an elementary abelian group of order q and exponent 2.

Lemma 8 represents the first step towards the classification we have spoken about: it will be of great importance in subsection 3.3.4.

3.3.1 An example

The following is an example of a degree $5 = 2^2 + 1$ non-singular curve, defined over $\mathbb{F}_4$, which is not projectively equivalent to the Hermitian curve and which attains the maximum possible number of inner Galois points that a curve in such conditions can attain, *viz.* 5. Its affine equation is (cf. (FUKASAWA, 2010, pp. 10, 15)):

$$C : \; g(x, y) \stackrel{\text{def}}{=} x(x + ay + 1)(x + y + a)(x + a^2 y + a^2) + y^5 = 0 \tag{3.53}$$

Here, $a \in \mathbb{F}_4$ is a primitive element for the extension $\mathbb{F}_4/\mathbb{F}_2$, *i.e.*, a is a root of the polynomial $T^2 + T + 1 \in \mathbb{F}_2[T]$. We claimed that C is non-singular; to see this, let us take the "projective" equation for C:

$$G(X, Y, Z) \stackrel{\text{def}}{=} X^4 Z + aX^2 Y Z^2 + XY^3 Z + XZ^4 + Y^5 = 0 \tag{3.54}$$

The derivatives of $G(X, Y, Z)$ are as follows

$$\begin{aligned} G_X(X, Y, Z) &= Z(Y^3 + Z^3) \\ G_Y(X, Y, Z) &= aX^2 Z^2 + XZY^2 + Y^4 \\ G_Z(X, Y, Z) &= X(Y^3 + X^3) \end{aligned}$$

From the above expressions, together with (3.54), we see that there are no singular points lying on the lines $X = 0$ or $Z = 0$. At this point it is worth noting that the projective transformation corresponding to the permutation of X and Z is an automorphism of C. In other words, $G(X,Y,Z) = G(Z,Y,X)$. So, without loss of generality, we may search for singular points lying in the affine chart $Z = 1$. From $G_X(x,y,1) = 0$ it follows that $y^3 = 1$, therefore we can have $y = 1$, a or a^2. Now, from $y^3 = 1$ and $G_Z(x,y,1) = 0$ it also follows that $x^3 = 1$, *i.e.*, $x = 1$, a or a^2, so we have 9 possibilities for the pair (x,y) of a singular point. Let us see which of these 9 possible pairs vanishes the other derivative, G_Y.

(x,y)	$G_Y(x,y,1)$
$(1,1)$	a
$(1,a)$	a^2
$(1,a^2)$	a^2
$(a,1)$	a
(a,a)	a
(a,a^2)	1
$(a^2,1)$	1
(a^2,a)	a^2
(a^2,a^2)	1

Since the derivative G_Y does not vanish for any "candidate" for singular point, C is indeed smooth.

The reader may easily check that the polynomial (cf. (3.53))

$$f(X,Y,Z) \stackrel{\text{def}}{=} X(X+aY+Z)(X+Y+aZ)(X+a^2Y+a^2Z) \tag{3.55}$$

is additive with respect to the variable X: its roots $\{0, aY+Z, Y+az, a^2Y+a^2Z\}$ are closed under addition (we also remind the reader that $a+1 = a^2$). It is now quite clear from (3.55) that $P = (1:0:0)$ is an inner Galois point for C: the conditions of item 2 of Theorem 3 are met (the condition $l \mid p^e - 1$ is trivially satisfied whenever $l = 1$). From now on, and until the next chapter, when we say Galois point we always mean inner Galois point.

As was formerly observed, $G(X,Y,Z)$ is invariant after swapping X and Z (*i.e.*, $G(X,Y,Z) = G(Z,Y,X)$), whereupon we deduce that $P' = (0:0:1)$ is another Galois point, for any permutation of the variables is a projective transformation (cf. also Proposition 1). It follows from Lemma 6 that there are at least $d = 5$ Galois points for C. These 5 points we know for sure to be Galois all lie in the line $Y = 0$ (cf. Proposition 11) and correspond, apart from P, to one linear factor of $G(X,0,1) = f(X,0,1)$ each.

X	$\rightsquigarrow$	$(0:0:1)$
$X+a$	$\rightsquigarrow$	$(a:0:1)$
$X+1$	$\rightsquigarrow$	$(1:0:1)$
$X+a^2$	$\rightsquigarrow$	$(a^2:0:1)$

We thus see that these 5 Galois points are exactly the five $\mathbb{F}_4$-rational points of the line $Y=0$. According to Proposition 11, to show that C has **exactly** 5 Galois points, it suffices to show that C is not projectively equivalent to the Hermitian curve. This is done by showing that the generic order of contact for C is exactly 2. From this, and also from the fact that $q(C)$ is invariant under projective transformations, we can conclude that C is not projectively equivalent to the Hermitian curve because the generic order of contact for the Hermitian curve $\mathcal{H}_q$ (whose degree is $q+1$) is $q \geq 4$.

There are two ways to visualize that 2 is the generic order of contact for C, and we show both of them. First of all, Definition 6 applied to our setting, namely of a degree 5 curve in characteristic 2, says that either $q(C)=2$ or $q(C)=4$, the last integer being the only power of 2 strictly between 2 and 5.

Take the line $\ell_{(a^2,a^2)}: Y+Z=0$. Any point R in $\ell_{(a^2,a^2)} \cap C$, with $R \neq P$, is such that $T_R C = \ell_{(a^2,a^2)}$, and we also have that $P \in \ell_{(a^2,a^2)}$ (cf. subsection 3.2.4, after Proposition 10). It then follows that for all points in $\ell_{(a^2,a^2)} \cap C$ the intersection multiplicity of their tangent line (which is the same for all, namely $\ell_{(a^2,a^2)}$) with C (at them) is the same number. If we show that the set $\ell_{(a^2,a^2)} \cap C$ consists of three points, P, R_1 and R_2, Bézout's theorem will imply that $I_{R_i}(T_{R_i}C \cap C) = 2$, and we will be done. Without loss of generality, we will look for the points of $\ell_{(a^2,a^2)} \cap C$ lying in the affine chart $Z=1$ (once the only point of C lying in the line $Z=0$ is P). Making $Y=Z=1$ in the polynomial G we obtain

$$(X(X+a^2)+1)^2$$

But the above polynomial has 2 distinct roots (in a degree 2 extension field of $\mathbb{F}_4$, *i.e.*, in $\mathbb{F}_{16}$). And we are done.

Next we consider the another mentioned way of showing that the generic order of contact for C is 2. The lines ℓ_σ for $\sigma \in G_P$ are explicitly given by the following equations

$$\ell_{(a,1)}: aY+Z=0, \quad \ell_{(1,a)}: Y+aZ=0 \quad \text{and} \quad \ell_{(a^2,a^2)}: Y+Z=0$$

Recall that all these lines contain P, so that the tangent line $T_R C$ is equal to ℓ_{σ_i} for any point $R \in \ell_{\sigma_i} \cap C$ with $R \neq P$.

The crucial feature about these lines, in the sense that it is the sufficient condition for C not being projectively equivalent to the Hermitian curve, is that they are pairwise distinct. Actually, it is sufficient just 2 of them to be distinct for us to reach the same conclusion; this will become clear after the following arguments. We suppose C is

projectively equivalent to the Hermitian curve, so that $q(C) = 4$. Take $R \in \ell_{(a,1)} \cap C$ different from P (such a point exists once none of the ℓ_{σ_i} is $Z = 0$, the tangent line to C at P). Then, as was mentioned above, $T_R C = \ell_{(a,1)}$. Once $q(C) = 4$, we have $I_R(\ell_{(a,1)} \cap C) \geq 4$. By Bézout's theorem, it follows that $I_R(\ell_{(a,1)} \cap C) = 4$, because C has degree 5 and $I_P(\ell_{(a,1)} \cap C) = 1$. But then the stabilizer of R in G_P has order at least 4, and hence is all of G_P. If R is fixed by all of G_P, then it is also fixed by, say, $(1, a)$ and we have that either $R \in \ell_{(1,a)}$ or $R \notin \ell_{(1,a)}$. If we show that $R \in \ell_{(1,a)}$, then we will be done since R, $P \in \ell_{(a,1)} \cap \ell_{(1,a)}$ with $R \neq P$ implies that $\ell_{(a,1)} = \ell_{(1,a)}$, a contradiction. So we must show that $R \in \ell_{(1,a)}$. Suppose not. Then $(1, a)$ fixes all the points in the line $\ell_{(1,a)}$ and also the point R, which is not in that line (the point R is fixed because its stabilizer is all of G_P). According to (MITCHELL, 1911, p. 212) (cf. also Remark 3), $(1, a)$ is, then, a transformation of type IV, and therefore it can be written, in suitable coordinates, as

$$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

In particular, $(1, a)$ would be diagonalizable. But one can easily verify that none of the matrices representing the σ_i's is diagonalizable (no transformation of type V is diagonalizable whatsoever). Hence, it must be $R \in \ell_{(1,a)}$, with which we finish.

Are there any other non-singular curves of degree 5 defined over $\mathbb{F}_4$ with exactly 5 Galois points? Remind that the first row of the matrix representation of each element in G_P corresponds to one linear factor in the factorization of $f(X, Y, Z)$: if $(\sigma_{11}\ \sigma_{12}\ \sigma_{13})$ is the first row of $\sigma \in G_P$, then $f(X, Y, Z)$ has the linear factor $\sigma_{11}X + \sigma_{12}Y + \sigma_{12}Z$. If we start with an order 4 subgroup S of $PGL(3, 4)$ whose matrices are of the form

$$M_\sigma = \begin{pmatrix} 1 & \sigma_{12} & \sigma_{13} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

we can then construct the polynomial $f_S(X, Y, Z) = Z \prod_{\sigma \in S}(X + \sigma_{12}Y + \sigma_{13}Z)$, and then consider the curve

$$C_S : f_S(X, Y, Z) + Y^5 = 0$$

which is easily seen to have the Galois point $P = (1 : 0 : 0)$, by virtue of Theorem 3 (item 2). The question that arises is: will this curve C_S be non-singular and have exactly 5 Galois points? If we take, for example, the subgroup

$$\left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & a^2 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & a^2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & a & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

the corresponding curve will be given by the following equation

$$ZX(X + a^2Y + Z)(X + Y + a^2Z)(X + aY + aZ) + Y^5 = 0$$

which looks pretty much like the curve we considered in this section (cf. (3.53)), the only difference being the choice of primitive element for the extension $\mathbb{F}_4/\mathbb{F}_2$. It is then obvious that this curve is also non-singular and have exactly 5 Galois points, because all arguments above hold for any choice of primitive element for $\mathbb{F}_4/\mathbb{F}_2$. Later on, we will see that the original curve and this one are not projectively equivalent (cf. Proposition 16). Next, we will generalize this construction.

3.3.2 Generalizing the previous example to "arbitrary" degree

We are now going to consider curves of degree 2^n+1. The arbitrariness of the degree comes from the arbitrariness of $n \geq 2$. An example where $n = 2$ was considered in the previous section and the idea here is to generalize it, *i.e.*, we want to construct a non-singular curve of degree 2^n+1 (over $\mathbb{F}_{2^n}$) with exactly 2^n+1 inner Galois points. We do this by "reverse engineering" the example considered previously, just as was discussed at the end of the last section.

We are interested in subgroups of $PGL(3,q)$ whose matrices are of the following form (it will later be clear that there is no loss of generality in considering only matrices of this form, instead of those in the bigger group $PGL(3,k)$; cf. Theorem 6)

$$(\alpha,\beta) = \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{3.56}$$

Let us denote the subgroup of $PGL(3,q)$ of all matrices of the above form by R_1. We can define an $\mathbb{F}_2$ vector space structure in R_1 (cf. the proof of item 2 of Theorem 3): we sum two matrices by multiplying them in the usual way and we multiply $M \in R_1$ by a scalar $v \in \mathbb{F}_2$ simply by multiplying it "v times":

$$(\alpha,\beta)\oplus(\alpha',\beta') \stackrel{\text{def}}{=} \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & \alpha' & \beta' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha+\alpha' & \beta+\beta' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (\alpha+\alpha',\beta+\beta')$$

and

$$v \odot (\alpha,\beta) \stackrel{\text{def}}{=} \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^v = \begin{pmatrix} 1 & v\alpha & v\beta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (v\alpha, v\beta)$$

Hence, the multiplicative structure of R_1 (in $PGL(3,2^n)$) has, in fact, an additive structure (the additiveness coming from the linear space structure just defined) and we can write, once the order of R_1 is $q^2 = 2^{2n}$, $R_1 \simeq \oplus_{i=1}^{2^n}\mathbb{F}_2$. We then see that R_1 is an elementary abelian group.

Let $G \leq R_1$ be a subgroup of order q. Once R_1 has order q^2, the existence of such a subgroup is guaranteed. We can construct a degree $q+1$ curve over $\mathbb{F}_q$ using the given subgroup G by letting its equation be

$$g_G(X,Y,Z) \stackrel{\text{def}}{=} Z \prod_{(\alpha,\beta)\in G} (X+\alpha Y+\beta Z) + Y^{q+1} = 0 \tag{3.57}$$

The curve given by equation (3.57) will be denoted by C_G, and $f_G(X,Y,Z)$ will denote the polynomial $Z\prod_{(\alpha,\beta)\in G}(X+\alpha Y+\beta Z)$, so that $g_G(X,Y,Z) = f_G(X,Y,Z)+Y^{q+1}$.

The curves constructed in this way, *i.e.*, those given by (3.57), **always** have $P=(1:0:0)$ as a Galois point: they satisfy the conditions of Theorem 3 (item 2). Moreover, the subgroup G is exactly the Galois group G_P, and we will write only G in place of G_P.

Notice that Theorem 3 (item 2) also guarantees that P is a non-singular point of C_G. If $(\alpha,0)\in G$ for some $\alpha\neq 0$, then the polynomial f_G has the linear factor $(X+\alpha Y)$. But then, it is not difficult to check that $(0:0:1)$ is a singular point of C_G. Now, if there is some $\beta\in\mathbb{F}_q$ such that (α,β) and (α',β) are in G, with $\alpha\neq\alpha'$, then $(\alpha+\alpha',0)$ would also be in G , from which we also conclude that the curve is singular for such G. So in order for G to give rise to a non-singular curve, it is necessary (although not necessarily sufficient) that the projection onto the second coordinate gives all of $\mathbb{F}_q$, *i.e.*, it is necessary for the map

$$\rho_G : \begin{cases} G & \to & \mathbb{F}_q \\ (\alpha,\beta) & \mapsto & \beta \end{cases} \tag{3.58}$$

to be surjective (or, equivalently, injective, once the domain and codomain are finite of the same cardinality). We are not interested in curves that are projectively equivalent to the Hermitian curve, so we exclude $G_{\mathcal{H}_q} \stackrel{\text{def}}{=} \{(0,\alpha) \mid \alpha\in\mathbb{F}_q\}$ from the discussion. From now on, we will only consider groups which satisfy this condition: the map ρ_G as in (3.58) is surjective, *i.e.*, the second coordinate "covers" all of $\mathbb{F}_q$.

We have already seen that for every order q subgroup of R_1, the corresponding curve has $P=(1:0:0)$ as inner Galois point. In order to guarantee the existence of another Galois point (and, hence, of at least 2^n+1 of them) it is sufficient to show that the projective transformation

$$\psi \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

corresponding to the permutation of the variables X and Z, is an automorphism of the curve C_G, for then $\psi(1:0:0) = (0:0:1)$ would also be a Galois point. But ψ will be an automorphism of C_G if, and only if, $f_G(X,Y,Z) = f_G(Z,Y,X)$ (notice that $\psi^{-1}=\psi$). If this happens, then there will be at least 2^n+1 inner Galois points, all of them lying in the

line $Y = 0$, which is the line joining $(1:0:0)$ and $(0:0:1)$. Note also that they will be all the $q+1$ $\mathbb{F}_q$-rational points of $Y = 0$, thanks to our choice of G.

Let us now see what kind of restriction has to be imposed on the group G in order for $f_G(X,Y,Z) = f_G(Z,Y,X)$ to hold. From (3.57), we have that

$$f_G(Z,Y,X) = X \prod_{(\alpha,\beta)\in G} (Z + \alpha Y + \beta X) = XZ\left(\prod_{\beta\neq 0} \beta\right) \prod_{(\alpha,\beta)\neq(0,0)} (X + \alpha\beta^{-1}Y + \beta^{-1}Z) \quad (3.59)$$

Now, once the elements appearing as second coordinate (the β's) "cover" all of $\mathbb{F}_q$ (cf. page 78), we have that $\prod_{\beta\neq 0}\beta = 1$. So, by (3.59), the equality $f_G(X,Y,Z) = f_G(Z,Y,X)$ turns into the following

$$\prod_{(\alpha,\beta)\neq(0,0)} (X + \alpha Y + \beta Z) = \prod_{(\alpha,\beta)\neq(0,0)} (X + \alpha\beta^{-1}Y + \beta^{-1}Z) \quad (3.60)$$

With (3.60), we see that $f_G(X,Y,Z) = f_G(Z,Y,X)$ is equivalent to

$$(\alpha,\beta) \in G \setminus \{(0,0)\} \Leftrightarrow (\alpha\beta^{-1}, \beta^{-1}) \in G \setminus \{(0,0)\} \quad (3.61)$$

The condition stated in (3.61) will be called simply by *change condition*.

With all we did so far in mind, it is quite natural to search for groups G whose elements are given by $G_{\theta,\lambda} \stackrel{\text{def}}{=} \{(\lambda g, \theta(g)) \mid g \in \mathbb{F}_q\}$, where $\theta : \mathbb{F}_q \to \mathbb{F}_q$ is a **field** automorphism of $\mathbb{F}_q$ and $\lambda \in \mathbb{F}_q^\times$ (we do not consider $\lambda = 0$: $G_{\theta,0} = G_{\mathcal{H}_q}$) is a fixed element: the set $G_{\theta,\lambda}$ certainly has q elements, and the fact that θ is an automorphism of $\mathbb{F}_q$ implies that $G_{\theta,\lambda}$ has indeed a group structure (cf. the considerations made after (3.56)) and also that $\rho_{G_{\theta,\lambda}}$ is surjective (cf. (3.58)). Once $\rho_{G_{\theta,\lambda}}$ is surjective, $C_{G_{\theta,\lambda}}$ may be non-singular. Now the change condition for $G_{\theta,\lambda}$ reads (here we use the fact that θ is a field automorphism)

$$g \cdot \theta(g^{-1}) = g^{-1} \ \ \forall\, g \in \mathbb{F}_q^\times \ \rightsquigarrow \ \ \theta(g) = g^2 \ \ \forall\, g \in \mathbb{F}_q$$

i.e., for the change condition to hold for $G_{\theta,\lambda}$, θ must be the Frobenius automorphism that generates the Galois group of the extension $\mathbb{F}_q/\mathbb{F}_2$. The converse is easily seen to be true too. Once θ will be fixed from now on, we denote $G_{\theta,\lambda}$ by G_λ only.

So for every $\lambda \in \mathbb{F}_q^\times$, the subgroup $G_\lambda \stackrel{\text{def}}{=} \{(\lambda\alpha, \alpha^2) \mid \alpha \in \mathbb{F}_q\}$ satisfies the change condition and is such that the projection onto the second coordinate gives us all of $\mathbb{F}_q$. Let us call by C_λ the curve C_{G_λ}, and by f_λ and g_λ the corresponding polynomials. We claim that $f_\lambda(x,y,1) \in k(y)[x]$ is given by

$$x^{2^n} + \sum_{i=1}^{n-1} (\lambda y)^{2^n - 2^{n-i+1}+1} x^{2^{n-i}} + (y^{2^n-1}+1)x \quad (3.62)$$

Indeed, it suffices to show that the roots of the above polynomial (in the variable x) are $\lambda\alpha y+\alpha^2$ for every $\alpha\in\mathbb{F}_q$, once $f_\lambda(x,y,1)$ was "constructed" in such a way that those are exactly its roots. If we evaluate the sum in the middle of (3.62) at $x=\lambda\alpha y+\alpha^2$ we get

$$\sum_{i=1}^{n-1}(\lambda y)^{2^n-2^{n-i}+1}\alpha^{2^{n-i}}+(\lambda y)^{2^n-2^{n-i+1}+1}\alpha^{2^{n-i+1}}= \\ \sum_{i=1}^{n-1}(\lambda y)^{2^n-2^{n-i}+1}\alpha^{2^{n-i}}+\sum_{i=1}^{n-1}(\lambda y)^{2^n-2^{n-i+1}+1}\alpha^{2^{n-i+1}} \tag{3.63}$$

Noting that $n-i+1=n-(i-1)$, we can rewrite (3.63) as (after changing $i-1$ to j)

$$\sum_{i=1}^{n-1}(\lambda y)^{2^n-2^{n-i}+1}\alpha^{2^{n-i}}+\sum_{j=0}^{n-2}(\lambda y)^{2^n-2^{n-j}+1}\alpha^{2^{n-j}} \tag{3.64}$$

Now for each k between 1 and $n-2$, the term $(\lambda y)^{2^n-2^{n-k}+1}\alpha^{2^{n-k}}$ appears in both of the sums in (3.64), so that they cancel out (once we are in characteristic 2). It thus remains the term corresponding to $n-1$ in the sum indexed by i plus the term corresponding to 0 in the sum indexed by j, which gives

$$\alpha^2 y^{2^n-1}+\lambda\alpha y$$

So, evaluating $x=\lambda\alpha y+\alpha^2$ in (3.62) gives

$$\lambda\alpha y^{2^n}+\alpha^2+\alpha^2 y^{2^n-1}+\lambda\alpha y+(y^{2^n-1}+1)(\lambda\alpha y+\alpha^2)=0$$

and proves the claim.

The curve C_λ is thus given by the following equation (in the affine chart $Z=1$)

$$C_\lambda: y^{2^n+1}+x^{2^n}+\sum_{i=1}^{n-1}(\lambda y)^{2^n-2^{n-i+1}+1}x^{2^{n-i}}+(y^{2^n-1}+1)x=0 \tag{3.65}$$

Changing variables ($y\mapsto y/\lambda$), (3.65) gets the much nicer aspect (recall: $\lambda\in\mathbb{F}_{2^n}$)

$$C_\lambda: \lambda^{-2}y^{2^n+1}+x^{2^n}+\sum_{i=1}^{n-1}y^{2^n-2^{n-i+1}+1}x^{2^{n-i}}+(y^{2^n-1}+1)x=0 \tag{3.66}$$

We now claim the following: C_λ is non-singular if, and only, if $\lambda\neq 1$. We already saw that there does not exist singular point in the line $Z=0$: the only point of the curve contained in this line is the Galois point P, and it is smooth. So we restrict our search for singular points in the affine chart $Z=1$. On the one hand, the derivative of the polynomial in (3.66) with respect to x gives

$$y^{2^n-1}+1$$

which vanishes if, and only if, $y \in \mathbb{F}_q^\times$ (remind that $+1 = -1$ in characteristic 2). On the other hand, the derivative of (3.66) with respect to y gives

$$\lambda^{-2} y^{2^n} + \sum_{i=1}^{n-1} y^{2^n - 2^{n-i+1}} x^{2^{n-i}} + y^{2^n - 2} x \tag{3.67}$$

Suppose $(x : y : 1)$ is a singular point of C_λ. Then (3.67) vanishes, as well as (3.66). Multiplying the above expression by $y \in \mathbb{F}_q^\times$, we get the following expression, which is still 0:

$$\lambda^{-2} y^{2^n+1} + \sum_{i=1}^{n-1} y^{2^n - 2^{n-i+1}+1} x^{2^{n-i}} + y^{2^n - 1} x \tag{3.68}$$

Substituting (3.66) in the above (3.68), we get

$$x^{2^n} + x$$

and this last expression vanishes if, and only if, $x \in \mathbb{F}_q$. So if $(x : y : 1)$ is a singular point of C_λ, then it is an $\mathbb{F}_q$-rational point. Moreover, y is non-zero. Still under the assumption that $(x : y : 1)$ is a singular point, we can rewrite equation (3.68) as

$$\lambda^{-2} y^2 + \sum_{i=1}^{n-1} y^{2 - 2^{n-i+1}} x^{2^{n-i}} + x = 0 \tag{3.69}$$

Dividing both sides of (3.69) by y^2 we get

$$\lambda^{-2} + \sum_{i=1}^{n-1} (xy^{-2})^{2^{n-i}} + xy^{-2} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(xy^{-2}) + \lambda^{-2} = 0 \tag{3.70}$$

But $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(xy^{-2}) \in \mathbb{F}_2$, and once $\lambda \neq 0$, we conclude that for $(x : y : 1)$ to be a singular point of C_λ it is necessary and sufficient that $\lambda = 1$. Note that the condition $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(xy^{-2}) + 1 = 0$ implies that x is also non-zero. By the reasoning we made above, we can also conclude that, for $\lambda = 1$, every point $(x : y : 1) \in \mathbb{P}^2(\mathbb{F}_q)$ satisfying $(x, y) \in \mathbb{F}_q^\times \times \mathbb{F}_q^\times$ and $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(xy^{-2}) = 1$ is a singular point of C_1. The trace map $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is $\mathbb{F}_2$-linear and surjective, once the extension $\mathbb{F}_{2^n}/\mathbb{F}_2$ is separable. The rank-nullity theorem then gives

$$\dim \mathrm{Ker}(\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}) = n - 1$$

Now let $\{\sigma_1, \ldots, \sigma_n\}$ be a basis for $\mathbb{F}_{2^n}$ as $\mathbb{F}_2$-vector space such that $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\sigma_1) = 1$ and $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\sigma_i) = 0$ for $i \geq 2$. Writing $s = \sum_{i=1}^n \nu_i \sigma_i \in \mathbb{F}_{2^n}$, we have that

$$\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(s) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\sum_{i=1}^n \nu_i \sigma_i\right) = \sum_{i=1}^n \nu_i \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\sigma_i) = \nu_1$$

With this, we see that $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(s) = 1$ if, and only if, $\nu_1 = 1$. Hence, there are 2^{n-1} elements in $\mathbb{F}_{2^n}$ with trace 1, one for each list $(\nu_2, \ldots, \nu_n) \in \mathbb{F}_2^{n-1}$. In this way, if we fix $x \in \mathbb{F}_{2^n}^\times$, there

will be 2^{n-1} different values for $y \in \mathbb{F}_{2^n}^{\times}$ such that $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(xy^{-2}) = 1$. Thus, there are $(2^n-1)2^{n-1}$ distinct singular points for C_1. But then, it is a matter of simple calculations to check that its genus is zero. In particular its automorphism group is isomorphic to $PGL(2,k)$.

For $\lambda \neq 1$, we now show that no C_λ is projectively equivalent to the Hermitian curve $\mathcal{H}_q$. The argument given below is similar to the second one we used to show the same for the curve of the previous section, *i.e.*, we show that the generic order of contact for C_λ is 2 because the lines $\ell_{(\lambda\alpha,\alpha^2)}$ are pairwise distinct (cf. page 75). We know that for each $\alpha \neq 0$, all points on the line $\ell_{(\lambda\alpha,\alpha^2)} : \lambda y + \alpha z = 0$ are fixed by the automorphism corresponding to $(\lambda\alpha, \alpha^2)$; also: $\ell_{(\lambda\alpha,\alpha^2)}$ contains P and is the tangent line to C_λ at every $R \in \ell_{(\lambda\alpha,\alpha^2)} \cap C$, with $R \neq P$. Note that $\ell_{(\lambda\alpha,\alpha^2)} \neq \ell_{(\lambda\beta,\beta^2)}$ for $\alpha \neq \beta$. If C_λ was to be projectively equivalent to the Hermitian curve $\mathcal{H}_q$, whose generic order of contact is q, then for $R \in \ell_{(\lambda\alpha,\alpha^2)} \cap C$, with $R \neq P$, we would have $I_R(T_R C \cap C) = q$ (such a point R exists, because no line $\ell_{(\lambda\alpha,\alpha^2)}$ is $T_P C : Z = 0$). But then, the stabilizer of R in G_P would have order at least q, and hence would be all of G_P, since G_P has order q; in particular, R would be fixed by $(\lambda\beta, \beta)$, with $\beta \neq \alpha$. But then, as in the case of the previous section, $R \in \ell_{(\lambda\beta,\beta^2)}$ as well, from which it follows that $\ell_{(\lambda\alpha,\alpha^2)} = \overline{PR} = \ell_{(\lambda\beta,\beta^2)}$, a contradiction.

We summarize all we did in the following

Proposition 15. Let $n \geq 2$ and $q = 2^n$. Then, for every $\lambda \in \mathbb{F}_q^{\times}$, with $\lambda \neq 1$, the curve with affine equation

$$C_\lambda : \lambda^{-2} y^{2^n+1} + x^{2^n} + \sum_{i=1}^{n-1} y^{2^n - 2^{n-i+1}+1} x^{2^{n-i}} + (y^{2^n-1}+1)x = 0$$

is a degree $q+1$ non-singular curve with exactly $q+1$ inner Galois points, namely, all $\mathbb{F}_q$-rational points of the line $Y = 0$. For $\lambda = 1$, the curve C_1 is rational.

We finish this section with an observation. The curve C_1, being rational, can be parametrized as $(t^{q+1} : t^q + t : 1)$ for $t \in k$ (cf. (FUKASAWA, 2013, Remark 3)).

3.3.3 The group of automorphisms and the Hasse-Witt invariant of C_λ

We now turn our attention to the group of automorphisms of the family of curves C_λ, which Proposition 15 treats of. First of all, any automorphism of C_λ, for $\lambda \neq 1$, is linear, because C_λ is non-singular of degree ≥ 4 for any $\lambda \in \mathbb{F}_q^{\times}$ (cf. (CHANG, 1978)). Moreover, any automorphism $\phi \in \mathrm{Aut}(C_\lambda)$ must give a permutation of the set of Galois points. Once all $q+1 \geq 2$ Galois points lie on the line $Y = 0$, this means that ϕ fixes the line $Y = 0$. Moreover, the Galois points are exactly all the $q+1$ $\mathbb{F}_q$-rational points of the

line $Y = 0$. So ϕ is represented by a matrix M_ϕ in $PGL(3,k)$ of the following form

$$M_\phi = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & 1 & 0 \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

The second row of M_ϕ is precisely $(0\,1\,0)$ for this is the necessary and sufficient condition for ϕ to fix the line $Y = 0$. Recall that C_λ is given by the following equation

$$f_\lambda(X,Y,Z) + Y^{q+1} = 0$$

Once ϕ^{-1} is an automorphism of C_λ it must leave the above equation unchanged, so that we must have

$$f_\lambda(X,Y,Z) = f_\lambda(a_{11}X + a_{12}Y + a_{13}Z, Y, a_{31}X + a_{32}Y + a_{33}Z) \tag{3.71}$$

The following table shows the coefficients of each variable, X, Y and Z, for each linear factor of $f_\lambda(X,Y,Z)$; the first line corresponds to the linear factor Z, the second line to the linear factor X and the third line corresponds to the linear factors $X + \lambda\alpha Y + \alpha^2 Z$, for each $\alpha \in \mathbb{F}_q^\times$.

Coeffs. of X	Coeffs. of Y	Coeffs. of Z
0	0	1
1	0	0
1	$\lambda\alpha$	α^2

The next table shows how each of the lines of the above one transforms after ϕ^{-1}, *i.e.*, after $X \mapsto a_{11}X + a_{12}Y + a_{13}Z$, $Y \mapsto Y$ and $Z \mapsto a_{31}X + a_{32}Y + a_{33}Z$. In other words, the following table is the same as the above one, but for the polynomial $f_\lambda(\phi(X,Y,Z))$.

Coeffs. of x	Coeffs. of y	Coeffs. of z
a_{31}	a_{32}	a_{33}
a_{11}	a_{12}	a_{13}
$a_{11} + \alpha^2 a_{31}$	$a_{12} + \lambda\alpha + \alpha^2 a_{32}$	$a_{13} + \alpha^2 a_{33}$

It is clear that in order for (3.71) to hold, the lines of the second table must be a permutation of the lines of the first one (and possibly multiplied by some suitable constants). We now go on to show that ϕ must be defined over $\mathbb{F}_q$, *i.e.*, that $M_\phi \in PGL(3,q)$.

Suppose that, for some $\alpha \neq \beta \in \mathbb{F}_q$, we had

$$(a_{11} + \alpha^2 a_{31})X + (a_{12} + \lambda\alpha + a_{32}\alpha^2)Y + (a_{13} + \alpha^2 a_{33})Z = rX \tag{3.72}$$

and

$$(a_{11}+\beta^2 a_{31})X+(a_{12}+\lambda\beta+a_{32}\beta^2)Y+(a_{13}+\beta^2 a_{33})Z=sZ \tag{3.73}$$

where r and $s\in k^\times$, *i.e.*, ϕ takes the line $X+\lambda\alpha Y+\alpha^2 Z=0$ to the line $X=0$ and the line $X+\lambda\beta Y+\beta^2 Z=0$ to the line $Z=0$. We will call any such ϕ an *automorphism of type one*. Note that our assumptions do not contemplate the case where $a_{31}X+a_{32}Y+a_{33}Z=rX$ (ϕ takes the line $Z=0$ to the line $X=0$) or $a_{31}X+a_{32}Y+a_{33}Z=sZ$ (ϕ fixes the line $Z=0$). These cases will be considered later on. The above equations (3.72) and (3.73) may be rewritten, respectively, as

$$\begin{cases} a_{11}+\alpha^2 a_{31} &= r\\ a_{12}+\lambda\alpha+\alpha^2 a_{32} &= 0\\ a_{13}+\alpha^2 a_{33} &= 0 \end{cases}$$

and

$$\begin{cases} a_{11}+\beta^2 a_{31} &= 0\\ a_{12}+\lambda\beta+\beta^2 a_{32} &= 0\\ a_{13}+\beta^2 a_{33} &= s \end{cases}$$

which give, for their turn, the following

$$\begin{cases} a_{11} &= \beta^2 r/(\alpha+\beta)^2\\ a_{12} &= \lambda\alpha\beta/(\alpha+\beta)\\ a_{13} &= \alpha^2 s/(\alpha+\beta)^2\\ a_{31} &= r/(\alpha+\beta)^2\\ a_{32} &= \lambda/(\alpha+\beta)\\ a_{33} &= s/(\alpha+\beta)^2 \end{cases} \tag{3.74}$$

We then have, using the data listed in (3.74), that

$$\begin{aligned} &f_\lambda(a_{11}X+a_{12}Y+a_{13}Z,Y,a_{31}X+a_{32}Y+a_{33}Z)=\\ &rX\cdot sZ\cdot\prod_{\gamma\neq\alpha,\beta}\left(\left[\frac{r(\beta+\gamma)^2}{(\alpha+\beta)^2}\right]X+\left[\frac{\lambda(\alpha+\gamma)(\beta+\gamma)}{(\alpha+\beta)}\right]Y+\left[\frac{s(\alpha+\gamma)^2}{(\alpha+\beta)^2}\right]Z\right)\cdot\ell_\infty\\ &r^{q-1}sXZ\cdot\left(\prod_{\gamma\neq\alpha,\beta}\frac{(\beta+\gamma)^2}{(\alpha+\beta)^2}\right)\cdot\prod_{\gamma\neq\alpha,\beta}\left(X+\left[\frac{\lambda(\alpha+\beta)(\alpha+\gamma)}{r(\beta+\gamma)}\right]Y+\left[\frac{s(\alpha+\gamma)^2}{r(\beta+\gamma)^2}\right]Z\right)\cdot\ell_\infty \end{aligned} \tag{3.75}$$

The factor ℓ_∞ in the above expressions is

$$\ell_\infty\overset{\text{def}}{=}\frac{r}{(\alpha+\beta)^2}X+\frac{\lambda}{(\alpha+\beta)}Y+\frac{s}{(\alpha+\beta)^2}Z$$

which comes from the factor Z in $f_\lambda(X,Y,Z)$. The product $\prod_{\gamma\neq\alpha,\beta}\frac{(\beta+\gamma)^2}{(\alpha+\beta)^2}$ is simply $\prod_{\delta\in\mathbb{F}_q^\times\setminus\{1\}}\delta$, which is 1. Substituting these into (3.75), we are then left with

$$\begin{aligned} &f_\lambda(a_{11}X+a_{12}Y+a_{13}Z,Y,a_{31}X+a_{32}Y+a_{33}Z)=\\ &\frac{r^q s}{(\alpha+\beta)^2}XZ\cdot\prod_{\gamma\neq\alpha,\beta}\left(X+\left[\frac{\lambda(\alpha+\beta)(\alpha+\gamma)}{r(\beta+\gamma)}\right]Y+\left[\frac{s(\alpha+\gamma)^2}{r(\beta+\gamma)^2}\right]Z\right)\cdot\left(X+\frac{\lambda(\alpha+\beta)}{r}Y+\frac{s}{r}Z\right) \end{aligned}$$

So, in order for (3.71) to hold, we must have

$$\frac{r^q s}{(\alpha+\beta)^2} = 1 \tag{3.76}$$

and

$$\frac{(\alpha+\beta)^2(\alpha+\gamma)^2}{r^2(\beta+\gamma)^2} = \frac{s(\alpha+\gamma)^2}{r(\beta+\gamma)^2} \Rightarrow rs = (\alpha+\beta)^2 \tag{3.77}$$

Finally, (3.76) and (3.77) leads us to conclude that $r^{q-1} = 1$, *i.e.*, $r \in \mathbb{F}_q^\times$ and, consequently, that $(\alpha+\beta)^2/r = s \in \mathbb{F}_q^\times$ also. And this shows that the automorphism (of type one) ϕ is in $PGL(3,q)$. The analysis of the other two kinds of automorphisms, namely those that satisfy

1. $a_{31}X + a_{32}Y + a_{33}Z = rX$ and $(a_{11}+\alpha^2 a_{31})X + (a_{12}+\lambda\alpha+\alpha^2 a_{32})Y + (a_{13}+\alpha^2 a_{33})Z = sZ$, which will be called *automorphisms of type two*, and

2. $a_{31}X + a_{32}Y + a_{33}Z = sZ$ and $(a_{11}+\alpha^2 a_{31})X + (a_{12}+\lambda\alpha+\alpha^2 a_{32})Y + (a_{13}+\alpha^2 a_{33})Z = rX$, which will be called *automorphisms of type three*,

for some $\alpha \in \mathbb{F}_q$ and $r, s \in k^\times$, are completely analogous to the previous one and lead us to conclude also that r and $s \in \mathbb{F}_q^\times$ and $r = s^{-1}$. So we have shown that any automorphism of C_λ, for any $\lambda \in \mathbb{F}_q^\times$ is defined over $\mathbb{F}_q$.

Let us explicitly write the matrices associated with the automorphisms of C_λ of each type. We will denote the set of automorphisms of type one by $T_{\lambda,1}$, and analogously for the other types. Thus, we have

$$T_{\lambda,1} = \left\{ \begin{pmatrix} \frac{\beta^2 r}{(\alpha+\beta)^2} & \frac{\lambda\alpha\beta}{(\alpha+\beta)} & \frac{\alpha^2}{r} \\ 0 & 1 & 0 \\ \frac{r}{(\alpha+\beta)^2} & \frac{\lambda}{(\alpha+\beta)} & \frac{1}{r} \end{pmatrix} \mid r \in \mathbb{F}_q^\times, \alpha \neq \beta \in \mathbb{F}_q \right\}$$

$$T_{\lambda,2} = \left\{ \begin{pmatrix} \alpha^2 r & \lambda\alpha & \frac{1}{r} \\ 0 & 1 & 0 \\ r & 0 & 0 \end{pmatrix} \mid r \in \mathbb{F}_q^\times, \alpha \in \mathbb{F}_q \right\}$$

$$T_{\lambda,3} = \left\{ \begin{pmatrix} r & \lambda\alpha & \frac{\alpha^2}{r} \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{r} \end{pmatrix} \mid r \in \mathbb{F}_q^\times, \alpha \in \mathbb{F}_q \right\}$$

Note that the matrices of $T_{\lambda,3}$ can be decomposed, for $r \neq 1$ as

$$\begin{pmatrix} r & \lambda\alpha & \alpha^2 r^{-1} \\ 0 & 1 & 0 \\ 0 & 0 & r^{-1} \end{pmatrix} = \begin{pmatrix} r & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & r^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & \lambda\alpha r^{-1} & (\alpha r^{-1})^2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{3.78}$$

The rightmost matrices in (3.78) are exactly those that make up the Galois group at the Galois point $P = (1:0:0)$. The matrices in the middle of (3.78) all have order $q-1$, as $r \in \mathbb{F}_q^\times$, and they fix the Galois points $P = (1:0:0)$ and $Q = (0:0:1)$ and permute the other $q-1$ Galois points cyclically. We will denote the set constituted by them as C_{q-1}. Note that the set $T_{\lambda,3}$ is the only one amongst the $T_{\lambda,i}$ which is a subgroup.

Our analysis shows that any automorphism of C_λ is either an automorphism of type one, two or three. The converse, which states that any automorphism of type one, two or three is an automorphism of C_λ, is clearly true. Notice that the automorphisms of type one, two and three are pairwise distinct: no automorphism of type one is of type two or three, none of type two is of type one or three and none of type three is of type one or two. Any automorphism of type two or three is determined by $r \in \mathbb{F}_q^\times$ and $\alpha \in \mathbb{F}_q$, so there are $(q-1)q$ automorphisms of type two and $(q-1)q$ of type three. For those of type one, they are determined by $r \in \mathbb{F}_q^\times$ and $\alpha, \beta \in \mathbb{F}_q$, with $\alpha \neq \beta$. So there are $(q-1)q(q-1)$ automorphisms of type one. Therefore, the full group of automorphisms of C_λ has cardinality $(q-1)q + (q-1)q + q(q-1)(q-1) = (q+1)q(q-1)$. Remind that any automorphism of C_λ fixes the line $Y = 0$. The projective transformations in $PGL(3,q)$ that fix a line form a subgroup of $PGL(3,q)$ isomorphic to $PGL(2,q)$ (the group of automorphisms of a projective line that are defined over $\mathbb{F}_q$). Noting that the cardinality of $PGL(2,q)$ is $(q+1)q(q-1)$, we can conclude that the full automorphism group of C_λ is isomorphic to $PGL(2,q)$, "realized" as the group of automorphisms of the line $Y = 0$ acting on the set of its $\mathbb{F}_q$-rational points, and whose structure is well known. We are now in a position to prove the following (cf. (FUKASAWA, 2013, Lemma 7))

Proposition 16. If λ and $\lambda' \in \mathbb{F}_q^\times$ with $\lambda \neq \lambda'$, then C_λ is not projectively equivalent to $C_{\lambda'}$.

Proof. Suppose there was a projective transformation ψ taking C_λ to $C_{\lambda'}$. Then, as ψ preserves Galois points, and as the Galois points of both C_λ and $C_{\lambda'}$ are the $\mathbb{F}_q$-rational points of the line $Y = 0$, we see that ψ should permute these points. The equation of C_λ may be written, after a projective transformation that does not affect the positions of the inner Galois points at all, as (cf. (3.57), (3.66) and also Proposition 15)

$$Z \prod_{\alpha \in \mathbb{F}_q} (X + \alpha Y + \alpha^2 Z) + \lambda^{-2} Y^{q+1} = 0 \tag{3.79}$$

From (3.79) above, it is readily seen that the tangent line to the inner point $P_\alpha = (\alpha^2 : 0 : 1)$ is $X + \alpha Y + \alpha^2 Z = 0$, which does not depend on λ (the tangent line to $P = P_1 = (1:0:0)$ is still given by $Z = 0$). Indeed, the line $X + \alpha Y + \alpha^2 Z = 0$ intersects C_λ only at P_α, henceforth it must be its tangent line. In other words: for any λ, the Galois points for C_λ as well as their tangent lines are the same geometric objects in $\mathbb{P}^2$. Therefore, the projective transformation ψ also permutes these lines. Let $R \stackrel{\text{def}}{=} (1:0:1)$. Suppose

$\psi(P_1) = P_i$ for some $i \neq 1$. Take $j \in \{1,\dots,d\} \setminus \{1,i\}$ and $\sigma \in G_{P_j}(C_{\lambda'})$, where $G_{P_j}(C_{\lambda'})$ denotes the group associated to the Galois point P_j with respect to the curve $C_{\lambda'}$, such that $\sigma(P_i) = P_1$ (such σ exists for the action of $G_{P_j}(C_{\lambda'})$ in $\Delta(C_{\lambda'}) \setminus \{P_j\}$ is transitive). Consider the projective transformation $\sigma \circ \psi$. It is also a projective transformation taking C_λ to $C_{\lambda'}$ since σ is an automorphism of $C_{\lambda'}$; however, this new transformation fixes the point P_1 since $\sigma \circ \psi(P_1) = \sigma(P_i) = P_1$. Thus, the existence of $\psi : C_\lambda \to C_{\lambda'}$ implies the existence of $\psi_1 : C_\lambda \to C_{\lambda'}$ fixing $P_1 = P$. Suppose now that $\psi_1(Q) = P_l$ for some P_l distinct from Q (and from P, obviously). It then exists $\eta \in G_P(C_{\lambda'})$ such that $\eta(P_l) = Q$, again because $G_P(C_{\lambda'})$ acts transitively on the set $\Delta(C_{\lambda'})$, from which both P_l and Q are elements. Taking ψ_2 to be $\eta \circ \psi_1$, we once more conclude that the existence of $\psi : C_\lambda \to C_{\lambda'}$ implies the existence of $\psi_2 : C_\lambda \to C_{\lambda'}$ fixing **both** P and Q. Finally, we suppose $\psi_2(R) = P_s$, with $P_s \neq R, P$ and Q. To repeat what we did in the preceding lines, we need an automorphism γ of $C_{\lambda'}$ fixing both P and Q and taking P_s to R. This γ we seek is to be found in the group C_{q-1} (cf.the paragraph immediately following (3.78)). Thus, considering $\psi_3 \overset{\text{def}}{=} \gamma \circ \psi_2$, we can finally conclude that the existence of $\psi : C_\lambda \to C_{\lambda'}$ implies the existence of $\psi_3 : C_\lambda \to C_{\lambda'}$ fixing the three points P, Q and R. By what we saw some lines above, ψ_3 also fixes the tangent lines $T_P C$, $T_Q C$ and $T_R C$, from which it follows that the points $A \overset{\text{def}}{=} (0:1:0) = T_P C \cap T_Q C$ and $B = (1:1:0) = T_P C \cap T_R C$ are also fixed by ψ_3. Let $M_{\psi_3} \in PGL(3,k)$ be a matrix representing ψ_3. From the fact that ψ_3 fixes P, Q and A, it follows that

$$M_{\psi_3} = \begin{pmatrix} s_1 & 0 & 0 \\ 0 & s_2 & 0 \\ 0 & 0 & s_3 \end{pmatrix}$$

for some $s_i \in k^\times$. From the fact that ψ_3 fixes B, it follows that $s_1 = s_2$, and, finally, from it fixing R it follows that $s_1 = s_3$. Therefore $\psi_3 = \mathrm{id}$ and, consequently, the existence of $\psi : C_\lambda \to C_{\lambda'}$ implies that $C_\lambda = C_{\lambda'}$. But then, from (3.79) it follows that $\lambda = \lambda'$; and the proof is finished.

□

We now compute the Hasse-Witt invariant, also known as p-rank, of C_λ; we will denote the Hasse-Witt invariant of a curve C by $\gamma(C)$. To this end, we will make use of the Deuring-Shafarevich formula (cf. (HIRSCHFELD; KORCHMáROS; TORRES, 2013, Theorem 11.62) and also (NAKAJIMA, 1987, Equation 2.2)), which can be thought of as being to the p-rank the same that the Hurwitz genus formula is to the genus. In order to use such formula, we need to identify which points of C_λ are ramified with respect to the map π_P; the ramification index of $R \in C_\lambda$ will be denoted, as usual, by e_R. The point P itself is totally ramified, so that we have $e_P = \deg \pi_P = d - 1 = q$. It is also known that the line $\ell_{(\lambda\beta,\beta^2)} : \lambda Y + \beta Z = 0$ is the tangent line to C_λ at any $R \in C_\lambda \cap \ell_{(\lambda\beta,\beta^2)}$, where

$R \neq P$, hence any of these points is ramified with respect to π_P, and its ramification index equals the order of contact $I_R(C_\lambda \cap \ell_{(\lambda\beta,\beta^2)})$ (cf. Lemma 5). The ramification index is also equal to $q/|o(R)|$, where $o(R)$ denotes the orbit of R by the action of G_P, *i.e.*, $o(R) = (C_\lambda \cap \overline{PR}) \setminus \{P\}$. Thus, to compute the ramification index, we can compute the size of the orbits, which is equivalent to us computing the number of distinct solutions, in x, of $g_\lambda(x, \beta/\lambda, 1) = 0$ for a fixed $\beta \in \mathbb{F}_q^\times$ (just take a parametrization for the line $\ell_{(\lambda\beta,\beta^2)}$ and substitute it in the equation of C_λ, which is, by definition, $g_\lambda = 0$). The equation $g(x, \beta/\lambda, 1) = 0$ gives us

$$x \cdot \prod_{\alpha \neq 0} (x + \alpha(\alpha + \beta)) + \beta^2/\lambda^2 = 0 \tag{3.80}$$

Consider the map

$$T_\beta : \begin{cases} \mathbb{F}_q & \to & \mathbb{F}_q \\ \alpha & \mapsto & \alpha(\alpha + \beta) \end{cases}$$

T_β is easily seen to be $\mathbb{F}_2$-linear (remind the Freshman's dream), whose kernel, which consists of $\{0, \beta\}$ only, has dimension 1. The rank-nullity theorem then gives $n - 1$ for the dimension of its image, so that $\#\mathrm{Im}(\psi) = q/2$. From this it follows that the number of distinct solutions, in x, of (3.80) is $q/2$; therefore, the ramification index for any of the points in $C_\lambda \cap \ell_{(\lambda\alpha,\alpha^2)}$ is exactly 2. Recall that, for $\alpha \neq \beta$, it holds that $\ell_{(\lambda\alpha,\alpha^2)} \cap \ell_{(\lambda\beta,\beta^2)} = \{P\}$, from which it follows that the sets $C \cap \ell_{(\lambda\alpha,\alpha^2)} \setminus \{P\}$ and $C \cap \ell_{(\lambda\beta,\beta^2)} \setminus \{P\}$ are disjoint. The Deuring-Shafarevich formula then gives

$$\gamma(C_\lambda) - 1 = |G_P| \cdot (\gamma(\mathbb{P}^1) - 1) + \sum_{R \in C_\lambda} (e_R - 1) \tag{3.81}$$

Replacing $|G_P| = q$, $\gamma(\mathbb{P}^1) = 0$ and

$$\sum_{R \in C_\lambda} (e_R - 1) \geq (q-1) + \sum_{\alpha \in \mathbb{F}_q^\times} \sum_{i=1}^{q/2} (2-1) = (q-1) + \frac{q(q-1)}{2} \tag{3.82}$$

in (3.81) we obtain

$$\gamma_{C_\lambda} \geq \frac{q(q-1)}{2} \tag{3.83}$$

But the genus $g(C_\lambda)$ of C_λ is exactly $q(q-1)/2$, once C_λ is non-singular, and it is known that for any curve C it holds that $0 \leq \gamma(C_\lambda) \leq g(C_\lambda)$. This and (3.83) lead us to conclude that $\gamma(C_\lambda) = g(C_\lambda)$, *i.e.*, the curves C_λ are all ordinary (cf. (HIRSCHFELD; KORCHMáROS; TORRES, 2013, Definition 11.87)). This also implies that the inequality in (3.82) is actually an equality, therefore the set of ramified points with respect to the map π_P is precisely the set of points $C_\lambda \cap \ell_{(\lambda\alpha,\alpha^2)}$ for every $\alpha \in \mathbb{F}_q^\times$.

Below, we state all that was done in this section.

Proposition 17. For the curves C_λ as in Proposition 15, it holds that $\mathrm{Aut}(C_\lambda) \simeq PGL(2,q)$ and $\gamma(C_\lambda) = q(q-1)/2 = g(C_\lambda)$.

It is worth noting, *en passant*, that the size of the automorphisms group of C_λ grows like $g(C)^{3/2}$; henceforth, the Hurwitz bound $\mathrm{Aut}(C) \leq 84(g(C)-1)$ does not hold for no one of the C_λ (provided that $q \geq 64$). However their "ordinariness" implies that it holds $\mathrm{Aut}(C_\lambda) \leq 84g(C)(g(C)-1)$ (cf. (HIRSCHFELD; KORCHMáROS; TORRES, 2013, Theorem 11.88) and also (NAKAJIMA, 1987)).

3.3.4 Complete classification of "2-Galois maximal" curves

What we call by "2-Galois maximal" curves are the curves in item 2 of Proposition 10 for which $\delta(C) = d$. In subsection 3.3.2, we exhibited a family of curves of degree $q+1$, for every $q = 2^n \geq 4$, in which each curve of the family is 2-Galois maximal (cf. Proposition 15). Our objective now is to show that any 2-Galois maximal curve is projectively equivalent to a curve "almost like" one in that family. More precisely, it will be shown that for any 2-Galois maximal curve C of degree $q+1$, C is projectively equivalent to C_λ, not for some $\lambda \in \mathbb{F}_q^\times \setminus \{1\}$, but rather for some $\lambda \in k^\times$ such that λ is not a $(q+1)$-th root of 1.

So let C be a 2-Galois maximal curve. Lemma 8 states that C is projectively equivalent to the curve given by

$$Z \prod_{(\alpha,\beta)\in G_P} (X + \alpha Y + \beta Z) + Y^{q+1} = 0 \tag{3.84}$$

where the group G_P is elementary abelian of order q and exponent 2, and where two of the inner Galois points are $P = (1:0:0)$ and $P_0 = (0:0:1)$. The set $\Delta(C) \setminus \{P\}$ is given by the points $P_\beta = (\beta:0:1)$ for each β such that (α,β) is in G_P: these are precisely the points in the intersection $C \cap \overline{PP_0}$ that are contained in the affine chart $Z = 1$ (recall that, by Proposition 11, all inner Galois points are collinear). From this, we can see that all β's are pairwise distinct: if not, there would not be exactly q Galois points apart from P (cf. the discussion at page 78). We will denote P_0 by Q.

Let $\beta \neq 0$. The Galois group at P_β, G_{P_β}, acts transitively on the set $\Delta(C) \setminus \{P_\beta\}$. In particular, once $\beta \neq 0$, there will be an automorphism $\phi_\beta \in G_{P_\beta}$ (which is also an automorphism of C) such that $\phi_\beta(P) = Q$. But since all automorphisms of G_{P_β} have order two (because the groups G_{P_β} have exponent two) we also have that $P = \phi_\beta^{-1}(Q) = \phi_\beta(Q)$. So if we have the knowledge of ϕ_β, we can obtain valuable informations about the α's and β's (the ones appearing in the matrices corresponding to G_P) once we must have

$$Z \prod_{(\alpha,\beta)\in G_P} (X + \alpha Y + \beta Z) + Y^{q+1} = \phi_\beta\left(Z \prod_{(\alpha,\beta)\in G_P} (X + \alpha Y + \beta Z) + Y^{q+1} \right) \tag{3.85}$$

Before we begin our search for the automorphisms ϕ_β, let us point out a few other things. Looking carefully at what we did in section 3.3 (before stating Lemma 8), we see that we can change the roles of $P = (1:0:0)$ and $Q = (0:0:1)$ and conclude that C is also given by the following equation

$$X \prod_{(\mu,\nu)\in G_Q} (Z + \mu Y + \nu X) + Y^{q+1} = 0 \tag{3.86}$$

where, again, the group G_Q is elementary abelian of order q and exponent 2. But then, as (3.84) and (3.86) are two equations for the same curve C, we are led to conclude that

$$Z \prod_{(\alpha,\beta)\in G_P} (X + \alpha Y + \beta Z) + Y^{q+1} = c \cdot \left(X \prod_{(\mu,\nu)\in G_Q} (Z + \mu Y + \nu X) + Y^{q+1} \right) \tag{3.87}$$

for some $c \in k^\times$. Comparing the coefficients of the monomial Y^{q+1} on both sides of (3.87), we see that it must be $c = 1$. Finally, (3.87) leads to the following

$$\prod_{(\alpha,\beta)\neq(0,0)} (X + \alpha Y + \beta Z) = \left(\prod_{\nu\neq 0} \nu \right) \prod_{(\mu,\nu)\neq(0,0)} (X + \mu\nu^{-1} Y + \nu^{-1} Z)$$

Thus, $\prod_{\nu\neq 0} \nu$ must equal 1, and the sets

$$G_P \quad \text{and} \quad \{(\mu\nu^{-1}, \nu^{-1}) \mid (\mu,\nu) \in G_Q \setminus \{(0,0)\}\} \cup \{(0,0)\} \tag{3.88}$$

must be the same group. Swapping X and Z in the preceding considerations, we can also conclude that $\prod_{\beta\neq 0} \beta$ must equal 1 and that the sets

$$G_Q \quad \text{and} \quad \{(\alpha\beta^{-1}, \beta^{-1}) \mid (\alpha,\beta) \in G_Q \setminus \{(0,0)\}\} \cup \{(0,0)\} \tag{3.89}$$

must be the same group as well. If we knew the involution $X \mapsto Z$, $Y \mapsto Y$ and $Z \mapsto X$ was an automorphism of C, the previous conditions related to (3.88) and (3.89) would be exactly the change condition of subsection 3.3.2 (cf. (3.61)).

Now we find the automorphisms ϕ_β, for $\beta \neq 0$. From (3.84), it is easy to see that the tangent line at $P_\beta = (\beta:0:1)$ is given by $T_{P_\beta}C : X + \alpha Y + \beta Z = 0$. Indeed, the line $\ell_\beta : X + \alpha Y + \beta Z = 0$ contains P_β and is such that $C \cap \ell_\beta = \{P_\beta\}$, so that it must be $\ell_\beta = T_{P_\beta}C$. The Galois group G_{P_β} is known to satisfy the following

1. it fixes the line $Y = 0$ (the line passing through all Galois points);
2. it fixes the point P_β;
3. it fixes the tangent line $T_{P_\beta}C : X + \alpha Y + \beta Z = 0$;
4. every one of its elements has order two;

We also know, once C is non-singular of degree ≥ 4, that all its automorphisms are given by projective transformations. Let, then, $\phi \in G_{P_\beta}$ be such that its matrix representation in $PGL(3,k)$ is

$$\phi = \begin{pmatrix} \phi_{11} & \phi_{12} & \phi_{13} \\ \phi_{21} & \phi_{22} & \phi_{23} \\ \phi_{31} & \phi_{32} & \phi_{33} \end{pmatrix}$$

From item 1 above, we conclude that $\phi_{21} = 0 = \phi_{23}$: the line $\phi_{21}X + \phi_{22}Y + \phi_{23}Z = 0$ has to be the line $Y = 0$. Now item 2 tells us that

$$\begin{pmatrix} \phi_{11} & \phi_{12} & \phi_{13} \\ 0 & \phi_{22} & 0 \\ \phi_{31} & \phi_{32} & \phi_{33} \end{pmatrix} \begin{pmatrix} \beta \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \phi_{11}\beta + \phi_{13} \\ 0 \\ \phi_{31}\beta + \phi_{33} \end{pmatrix} \quad \text{must be equal to} \quad \begin{pmatrix} \lambda\beta \\ 0 \\ \lambda \end{pmatrix}$$

for some $\lambda \neq 0$. Hence, $\phi_{13} = \beta(\phi_{11} + \lambda)$ and $\phi_{31} = \beta^{-1}(\phi_{33} + \lambda)$. Using now item 3, we obtain that the linear form

$$\phi(X + \alpha Y + \beta Z) = (\phi_{11} + \phi_{33} + \lambda)X + (\phi_{12} + \alpha\phi_{22} + \beta\phi_{32})Y + \beta(\phi_{11} + \phi_{33} + \lambda)Z$$

has to be the linear form $sX + s\alpha Y + s\beta Z$, for some $s \neq 0$; this implies that $s = \phi_{11} + \phi_{33} + \lambda \neq 0$ and

$$\phi_{12} + \alpha\phi_{22} + \beta\phi_{32} = \alpha(\phi_{11} + \phi_{33} + \lambda) \tag{3.90}$$

Finally, from item 4 we infer that the matrix

$$\phi^2 = \begin{pmatrix} \phi_{11} & \phi_{12} & \beta(\phi_{11} + \lambda) \\ 0 & \phi_{22} & 0 \\ \beta^{-1}(\phi_{33} + \lambda) & \phi_{32} & \phi_{33} \end{pmatrix} \begin{pmatrix} \phi_{11} & \phi_{12} & \beta(\phi_{11} + \lambda) \\ 0 & \phi_{22} & 0 \\ \beta^{-1}(\phi_{33} + \lambda) & \phi_{32} & \phi_{33} \end{pmatrix} =$$

$$\begin{pmatrix} \phi_{11}^2 + (\phi_{11} + \lambda)(\phi_{33} + \lambda) & \phi_{12}(\phi_{11} + \phi_{22}) + \beta\phi_{32}(\phi_{11} + \lambda) & \beta(\phi_{11} + \lambda)(\phi_{11} + \phi_{33}) \\ 0 & \phi_{22}^2 & 0 \\ \beta^{-1}(\phi_{33} + \lambda)(\phi_{11} + \phi_{33}) & \phi_{32}(\phi_{22} + \phi_{33}) + \beta^{-1}\phi_{12}(\phi_{33} + \lambda) & \phi_{33}^2 + (\phi_{11} + \lambda)(\phi_{33} + \lambda) \end{pmatrix}$$

must be equal to some non-zero multiple of the identity matrix, say $\omega \cdot \mathrm{Id}$. Comparing the elements in the diagonal, we obtain

$$\phi_{11}^2 + (\phi_{11} + \lambda)(\phi_{33} + \lambda) = \phi_{33}^2 + (\phi_{11} + \lambda)(\phi_{33} + \lambda) \rightsquigarrow \phi_{11}^2 = \phi_{33}^2 \rightsquigarrow \phi_{11} = \phi_{33}$$

and then,

$$\phi_{22}^2 = \phi_{11}^2 + (\phi_{11} + \lambda)(\phi_{33} + \lambda) = \lambda^2 \rightsquigarrow \phi_{22} = \lambda$$

Substituting $\phi_{11} = \phi_{33}$ and $\phi_{22} = \lambda$ in (3.90), we obtain $\phi_{12} = \beta\phi_{32}$. Therefore we have $\phi^2 = \lambda^2\mathrm{Id}$. Since all matrices under consideration are in $PGL(3,k)$, we may take λ to be 1, and if we denote $\phi_{11} = a$ and $\phi_{32} = b$ for some $a, b \in k$, we can finally infer that G_{P_β} consists of automorphisms whose matrix representation have the following form

$$\langle a, b \rangle \stackrel{\text{def}}{=} \begin{pmatrix} a & \beta b & \beta(a+1) \\ 0 & 1 & 0 \\ \beta^{-1}(a+1) & b & a \end{pmatrix}$$

Notice that these matrices are closed under taking products: $\langle a,b\rangle \cdot \langle a',b'\rangle = \langle a+a'+1, b+b'\rangle$ and that $\langle 1,0\rangle = \mathrm{Id}$. We note also that

$$(\gamma : 0 : 1) \overset{\langle a,b\rangle}{\mapsto} (a(\beta+\gamma)+\beta : 0 : \gamma\beta^{-1}(a+1)+a) \tag{3.91}$$

i.e., the image of the Galois point P_γ by $\langle a,b\rangle$ does not depend on the second coordinate of the pair (a,b). Once G_{P_β}, whose order is q, must act transitively on the set $\Delta(C)\setminus\{P_\beta\}$, which has cardinality q, we conclude that all numbers appearing as first coordinates of $\langle a,b\rangle$ **must be distinct**.

From (3.91) we see that the automorphism in G_{P_β} that takes P to Q and Q to P corresponds to $\langle 0,b\rangle$, for some appropriate b. But this same automorphism must also swap the tangent lines $T_PC : Z = 0$ and $T_QC : X = 0$. But $\langle 0,b\rangle$ takes the line $Z = 0$ to the line $\beta^{-1}X + bY = 0$, and so in order for $\langle 0,b\rangle$ to take T_PC to T_QC, we must have $b = 0$ as well.

Summing up, the automorphism ϕ_β we were searching for is given by the following matrix.

$$\phi_\beta = \begin{pmatrix} 0 & 0 & \beta \\ 0 & 1 & 0 \\ \beta^{-1} & 0 & 0 \end{pmatrix}$$

For every $\beta \neq 0$ the equation of the curve must be invariant by the above automorphism, which maps $X \mapsto \beta Z$, $Y \mapsto Y$ and $Z \mapsto \beta^{-1}X$. Substituting this into (3.85) we get:

$$\begin{aligned} \prod_{(\alpha,\gamma)\neq(0,0)} (x+\alpha y+\gamma z) = \prod_{(\alpha,\gamma)\neq(0,0)} (\beta^{-1}\gamma x+\alpha y+\beta z) \\ (\beta^{-1})^{q-1}\left(\prod_{\gamma\neq 0}\gamma\right) \prod_{(\alpha,\gamma)\neq(0,0)} (x+\alpha\beta\gamma^{-1}y+\beta^2\gamma^{-1}z) \end{aligned} \tag{3.92}$$

As we saw earlier, $\prod_{\gamma\neq 0}\gamma = 1$, so we conclude that $(\beta^{-1})^{q-1} = 1$, which implies, for its turn, that $\beta \in \mathbb{F}_q^\times$. Consequently, the inner Galois points are precisely the $\mathbb{F}_q$-rational points of the line $Y = 0$. From (3.92) it also follows that

$$(\alpha,\gamma) \in G_P \setminus \{(0,0)\} \iff (\alpha\beta\gamma^{-1}, \beta^2\gamma^{-1}) \in G_P \setminus \{(0,0)\} \ \ \forall \beta \in \mathbb{F}_q^\times \tag{3.93}$$

The condition in (3.93) is somehow a strengthened version of the previous change condition (cf. (3.61)): for $\beta = 1$, (3.93) is precisely the change condition (3.61), which is equivalent to say that the involution $X \mapsto Z$, $Y \mapsto Y$ and $Z \mapsto X$ is an automorphism of C. Now that we know that the elements appearing as second coordinates of the automorphisms $(\alpha,\gamma) \in G_P$ span all of $\mathbb{F}_q$, we can take γ to be 1 and vary $\beta \in \mathbb{F}_q$ in (3.93) to conclude that the group is given exactly by $\{(\alpha\beta, \beta^2) \mid \beta \in \mathbb{F}_q\}$. We must have $\alpha \neq 0$, otherwise we would get the Hermitian curve. The curve C we thus obtained, and which we will denote by C_α is just like the curves C_λ we studied in subsection 3.3.2: the only

difference is that it does not necessarily hold that $\alpha \in \mathbb{F}_q$. The expression given back then by (3.62) still holds for the more general $\lambda \in k^\times$. (3.66) in the current context reads:

$$C_\alpha : (\alpha^{-1})^{2^n+1} y^{2^n+1} + x^{2^n} + \sum_{i=1}^{n-1} y^{2^n-2^{n-i+1}+1} x^{2^{n-i}} + (y^{2^n-1}+1)x = 0 \tag{3.94}$$

Repeating the analysis of singularity conditions we did for C_λ (the one following (3.66)), but now using (3.94) instead (the only difference will come from λ^{-2} being replaced by $(\alpha^{-1})^{q+1}$), we obtain that in order for C_α to be non-singular it is necessary and sufficient that $(\alpha^{-1})^{q+1} \neq 1$ (cf. (3.70)). In other words: α cannot be a $(q+1)$-th root of 1. Let us denote the group of $(q+1)$-th roots of 1 by μ_{q+1}. Proposition 17 still holds under the present conditions, the only difference is the following: once $\alpha \in \mathbb{F}_q$ is not necessarily true, the automorphisms of C_α will not necessarily be defined over $\mathbb{F}_q$; nonetheless, these automorphisms will be given exactly by the sets $T_{\alpha,1}$, $T_{\alpha,2}$ and $T_{\alpha,3}$ as in page 85. Also, Proposition 16 still holds for α and $\alpha' \in k \setminus \mu_{q+1}$ with $\alpha \neq \alpha'$. Their proofs need no modification. Finally, the argument, given before the statement of Proposition 15, used to show that C_λ is not projectively equivalent to the Hermitian curve can also be used to show the same for C_α.

All this being said, we can state the complete classification of 2-Galois maximal curves as below.

Theorem 6. Let C be a 2-Galois maximal curve of degree $q+1$. Then C is projectively equivalent to the curve given by

$$C_\alpha : Z \prod_{s \in \mathbb{F}_q} (X + \alpha s Y + s^2 Z) + Y^{q+1} = 0$$

for some $\alpha \in k^\times$ that is not a $(q+1)$-th root of 1. The converse also holds. Moreover, we have that $\mathrm{Aut}(C_\alpha) \simeq PGL(2,q)$ and also that C_α is an ordinary curve, *i.e.*, its 2-rank equals its genus (which equals $q(q-1)/2$).

CHAPTER

4

EXTENDABLE POINTS FOR SINGULAR CURVES

In this last chapter we are going to consider extendable Galois points for singular curves. Its contents are, in the author's best knowledge, novel, *i.e.*, nowhere to be found in the literature at the time this thesis was submitted. The condition of the point being extendable is essential for us to make use of Theorem 3, which not only characterizes the equation of the curve but also gives the structure of the corresponding Galois group.

Throughout the chapter, we will say only Galois point instead of extendable Galois point. As we will consider only outer points and non-singular inner points, we maintain the notation used in Chapter 3 and denote the set of inner non-singular and outer (extendable!) Galois points of C by $\Delta(C)$ and $\Delta'(C)$, and their cardinalities by $\delta(C)$ and $\delta'(C)$, respectively.

For the case of outer points, which is to be studied the most, we will be able to determine the set $\Delta'(C)$ when $\deg C \not\equiv 0 \bmod p$ (cf. Theorem 7) and when $\deg C$ is a power of p (with $p \neq 2$; cf. Theorem 8). For inner non-singular points with $\deg C \not\equiv 1 \bmod p$, we will show that $\delta(C) \leq 1$ (cf. Theorem 9).

4.1 Outer points when $d \not\equiv 0 \bmod p$

As the title of this section says, we will consider outer Galois points for curves of degree $d \not\equiv 0 \bmod p$, and, as usual, $d \geq 4$. Let C be such a curve and P such a point; we invoke Theorem 3 (item 1) to assume that C is given by the following equation

$$X^d + G_d(Y, Z) = 0 \tag{4.1}$$

and also that $P = (1 : 0 : 0)$. Contrary to what happened entirely throughout Chapter 3, the polynomial G_d can now have multiple roots. Actually, it **must** have multiple roots in order for C to be singular. Indeed, considering the derivative of $X^d + G_d(Y, Z)$ with respect to X, we see that any singular point of C must be contained in the line $X = 0$.

Making $X = 0$ in (4.1), it follows that any singular point $(0 : y : z)$ must be a root of G_d, *i.e.*, $G_d(y, z) = 0$. But the derivatives of $X^d + G_d(Y, Z)$ with respect to Y and Z are simply the derivatives of the polynomial G_d, with respect to the same variables. Summing up, we conclude that any singular point $S = (x : y : z)$ of the curve given by (4.1) must satisfy

- $x = 0$,
- $G_d(y, z) = 0$ and
- $G_{d,Y}(y, z) = 0$ and $G_{d,Z}(y, z) = 0$.

Therefore, S will give rise to a repeated root of G_d. The converse obviously holds true.

We write $G_d(Y, Z)$ as a product of linear factors:

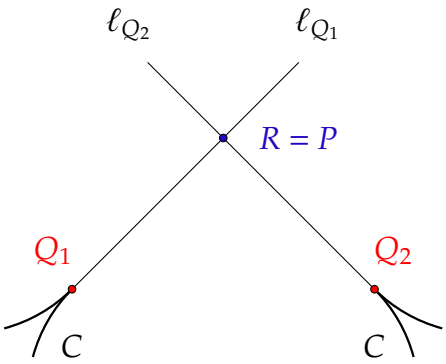
$$G_d(Y, Z) = \ell_{Q_1}^{n_1} \cdot \ldots \cdot \ell_{Q_s}^{n_s} \tag{4.2}$$

In the above, $\ell_{Q_i} \stackrel{\text{def}}{=} z_i Y - y_i Z$ and $Q_i \stackrel{\text{def}}{=} (0 : y_i : z_i)$, $i = 1, \ldots, s$, are the roots of $G_d(Y, Z)$. We will also denote by ℓ_{Q_i} the line given by $\ell_{Q_i} = 0$, since there is no way this can cause confusion. Note that all lines ℓ_{Q_i} pass through the point $P = (1 : 0 : 0)$, and each one of them, say ℓ_{Q_j}, intercepts C at Q_j with multiplicity $I_{Q_j}(C \cap \ell_{Q_j})$ exactly d. The point Q_i will be a singular point of C if, and only if, the n_i that appears in (4.2) is ≥ 2. Moreover, if Q_i is such a singular point, then it has only one tangent line: ℓ_{Q_i} itself. By our initial assumption, that which tells C is singular, there is at least one such point, which we set to be Q_1.

Suppose that C has another singular point, Q_2, and also that C has another outer Galois point R. For a suitable projective transformation, we may suppose that $R = (1 : 0 : 0)$ and that C has equation

$$X^d + \tilde{G}_d(Y, Z) = 0$$

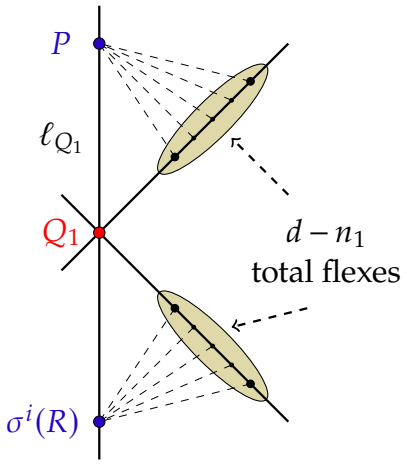
Once projective transformations take singular points to singular points, the same considerations we made in the last paragraph are true for R in place of P. Consequently, the tangent line (which we saw to be unique) at each singular point pass through R too. As there are two distinct singular points, Q_1 and Q_2, whose tangent lines intersect the curve only at them, their tangent lines are also distinct, and therefore $R = \ell_{Q_1} \cap \ell_{Q_2} = P$.



The considerations we just made are summarized in the following.

Lemma 9. If C has at least two singular points, then it has at most one outer Galois point, *i.e.*, $\delta'(C) \leq 1$.

From now on, let us assume that Q_1 is the only singular point of C. Looking back at (4.2), we see that it cannot be $n_1 = d$: otherwise $G_d(Y,Z) = \ell_{Q_1}^d$, from which it follows that C would be reducible: $X^d + \ell_{Q_1}^d = \prod_{i=0}^{d-1}(X - \zeta_d^i \mu \ell_{Q_1})$, where ζ_d is a primitive d-th root of 1 and $\mu^d = -1$. Therefore the multiplicity of Q_1 satisfies $2 \leq n_1 \leq d-1$. The other points $Q_2, \ldots, Q_{d-n_1}$ are total flexes of C. As was observed before Lemma 9, any other extendable outer point $R \neq P$ for C must lie on the line ℓ_{Q_1}, and not on the line $X = 0$ since ℓ_{Q_1} intersects $X = 0$ only at Q_1. In other words: the coordinates of R must be $(\alpha : y^\star : z^\star)$, for some $\alpha \neq 0$. Hence, for $\sigma = \mathrm{diag}(\zeta_d, 1, 1)$ a generator of G_P (cf. Theorem 3), we have that $\sigma(R) = (\zeta_d \alpha : y^\star : z^\star), \sigma^2(R), \ldots, \sigma^{d-1}(R)$ are $d-1$ distinct outer Galois points for C, so that C has at least $d+1$ outer points: $P \cup \{\sigma^i(R) \mid i = 0, \ldots, d-1\}$ (cf. Proposition 1 and the proof of Proposition 6). All these points lie in the line ℓ_{Q_1}, *i.e.*, they are collinear. Recall that the multiplicity of Q_1 is n_1. For each of these $d+1$ extendable outer points, there are $d - n_1$ total flexes, and they are all distinct. Indeed, if there was a total flex Q associated to the extendable outer points P_i and P_j, as $T_Q C$ contains both P_i and P_j, we see that $T_Q C = \overline{P_i P_j} = \ell_{Q_1}$. But $\ell_{Q_1} \cap C = \{Q_1\}$, the only singular point of C. This way, we see that C has at least $(d+1)(d-n_1)$ total flexes.



Let us make the following additional hypothesis on the degree of the curve: $d-1 \not\equiv 0 \bmod p$ (in particular $p \neq 2$, once we already assumed $d \not\equiv 0 \bmod p$).

4.1.1 $d \not\equiv 1 \bmod p$

We will show that the dual map of C is separable; from this it will follow that the generic order of contact $q(C)$ (cf. Definition 6) for C is 2, and therefore we will be able to count the total flexes of C using (3.3), in the same way we did back in Chapter 3.

Remark 8. Actually, since we are dealing with singular curves, the most accurate form of (3.3) and (3.9) that must be used is the following (cf. (FUKASAWA, 2007, Section 2) and (STöHR; VOLOCH, 1986, p. 6))

$$\sum_P I_P(C \cap T_P C) - q(C) \leq 3d + (q(C)+1)(2g(C)-2)$$

where $g(C)$ denotes the genus of C and the sum in the left hand side is taken over the non-singular points of C. If we replace $g(C) \leq (d-1)(d-2)/2$, we recover and (3.9); moreover, if $q(C) = 2$ we recover (3.3).

What we are now going to do is similar to what we did in the beginning of subsection 3.2.3 (cf. also the end of subsection 3.2.2). First of all, we may suppose that $Q_1 = (0:1:0)$ and $Q_2 = (0:0:1)$, and still maintain generality: for this it suffices to take a suitable projective transformation. Under this assumption, we have that C has no singular point in the affine chart $Z \neq 0$. Henceforth, the polynomial $g(T) \stackrel{\text{def}}{=} G_d(T,1)$ has no repeated roots (otherwise there would be a singular point with $Z \neq 0$; cf. the beginning of this section). We may then write (4.1) locally as

$$x^d + g(y) = 0 \tag{4.3}$$

From (4.3) it follows that

$$dx^{d-1} + g'(y)y' = 0 \tag{4.4}$$

Since Q_2 is non-singular and $T_{Q_2}C = \overline{PQ_2} : Y = 0$, we have that x is a uniformizing parameter at Q_2. In particular, x, and consequently x^{d-1} too, is not zero. Since $d \not\equiv 0 \bmod p$, we have that $dx^{d-1} \neq 0$, and from (4.4) it follows that $g'(y)y' \neq 0$, and, subsequently, that $g'(y) = 0$. (4.4) then allows us to write

$$y' = -\frac{dx^{d-1}}{g'(y)} \tag{4.5}$$

Differentiating one last time, we get from (4.4) (remind that we assumed $d-1 \not\equiv 0 \bmod p$):

$$d(d-1)x^{d-2} + g''(y)(y')^2 + g'(y)y'' = 0 \tag{4.6}$$

If it was $y'' = 0$, then we would obtain from (4.6) and (4.5) (and also the equation of C, (4.1))

$$(d-1)x^{d-2} = -\frac{dg''(y)x^{2d-2}}{(g'(y))^2} \rightsquigarrow (d-1)g'(y)^2 = g''(y)\cdot g(y) \tag{4.7}$$

But (4.7) is telling that any root of $g(T)$ is also a root of $g'(T)$, or, in other words, that $g(T)$ has repeated roots, a contradiction to what was formerly observed. Thus, $y'' \neq 0$, which implies that the dual map of C is separable, which for its turn implies that $q(C) = 2$.

Using the fact that C has at least $(d+1)(d-n_1)$ total flexes, (3.3) gives

$$(d+1)(d-n_1)(d-2) \leq 3d(d-2) \quad \rightsquigarrow \quad (d+1)(d-n_1) \leq 3d \tag{4.8}$$

Since $2 \leq n_2 \leq d-1$, in order for (4.8) to hold, it must be $n_1 = d-1$ or $n_1 = d-2$. We will show that in both cases we get a contradiction with the number of total flexes that the curves in either case can have, therefore concluding that C cannot have more than one outer Galois point.

We begin with $n_1 = d-1$. In this case $s = 2$ and there is no loss in generality in assuming that $Q_1 = (0:0:1)$ (this is a bit different from what we supposed a few lines above), so that $\ell_{Q_1} = Y$, and that $Q_2 = (0:1:0)$, so that $\ell_{Q_2} = Z$; in other words: we may suppose, without losing generality, that C has equation $X^d + Y^{d-1}Z = 0$. Our analysis shows that there are at least $(d+1)(d-(d-1)) = d+1 \geq 5$ total flexes. We will show that, actually, the curve $X^d + Y^{d-1}Z = 0$ has only one total flex, namely Q_2. Indeed, the point Q_2 is a total flex and lies in the line $Z = 0$, which is its tangent line; hence, if there are any other flexes, they must lie on the affine chart $Z \neq 0$. We will denote by $f(x,y)$ the dehomogenization of $X^d + Y^{d-1}Z$, *i.e.*, $f(x,y) \stackrel{\text{def}}{=} x^d + y^{d-1}$. The equation for the Hessian curve of C in the affine chart $Z \neq 0$ reads:

$$(d-1)f_x(f_{xy}f_y - f_{yy}f_x) - (d-1)f_y(f_{xx}f_y - f_{yx}f_x) + df(f_{xx}f_{yy} - f_{xy}f_{yx}) = 0 \tag{4.9}$$

Once $f(x,y) = x^d + y^{d-1}$, the mixed derivatives, $f_{xy} = f_{yx}$, vanish. If we are looking for flexes (and/or singular points) for the curve C, we can also make $f = 0$ in (4.9). After doing so we are left with

$$f_{xx}f_y^2 + f_{yy}f_x^2 = 0 \quad \text{and} \quad f = 0$$

We list the derivatives we are going to use below.

- $f_x = dx^{d-1} \quad \rightsquigarrow \quad f_x^2 = d^2x^{2d-2}$
- $f_{xx} = d(d-1)x^{d-2}$
- $f_y = (d-1)y^{d-2} \quad \rightsquigarrow \quad f_y^2 = (d-1)^2y^{2d-4}$
- $f_{yy} = (d-1)(d-2)y^{d-3}$

Substituting these into $f_{xx}f_y^2 + f_{yy}f_x^2 = 0$ we get

$$d(d-1)^3x^{d-2}y^{2d-4} + d^2(d-1)(d-2)x^{2d-2}y^{d-3} = 0 \tag{4.10}$$

The two summands above share the factor $x^{d-2}y^{d-3}$, and hence we can rewrite (4.10) (we also cancel out the common constant $d(d-1)$, which is, never too much to recall, $\not\equiv 0 \bmod p$)

$$x^{d-2}y^{d-3}((d-1)^2y^{d-1} + d(d-2)x^d) = 0 \tag{4.11}$$

Plugging $x = 0$ (resp. $y = 0$), (4.11) is satisfied; then, in order for $f = x^d + y^{d-1}$ to also vanish, we must have $y = 0$ (resp. $x = 0$). This gives us the point $Q_1 = (0:0:1)$, which is the only singular for C, and does not come into play, for we are accounting only flexes. The only other possibility is, thus, $(d-1)^2y^{d-1} + d(d-2)x^d = 0$ and $f = 0$, with $xy \neq 0$. But $(d-1)^2 = d(d-2)+1$, so that the factor inside parentheses in (4.11) is

$$d(d-2)(x^d + y^{d-1}) + y^{d-1} = d(d-2)f + y^{d-1} = y^{d-1} \neq 0$$

which shows that C has no other flex than Q_2. Next, we treat the case $n_1 = d-2$. The treatment is similar to the preceding one, only the computations are insignificantly more complicated.

Now we have $s = 3$ and, as above, there is no loss in generality in supposing that $Q_1 = (0:0:1)$, $Q_2 = (0:1:0)$. We write $Q_3 \stackrel{\text{def}}{=} (0:-\beta:\alpha)$, with $\alpha\beta \neq 0$. The curve C has, therefore, the following equation: $X^d + Y^{d-2}Z(\alpha Y + \beta Z) = 0$; also, since $n_2 = d-2$, C has at least $(d+1)(d-(d-2)) = 2d+2 \geq 10 > 2$ total flexes. Let us count the number of flexes of C in the affine chart $Y \neq 0$, for the line $Y = 0$ intersects C only at the singular point Q_1. We will show that C has $2d+2$ flexes but only 2 total flexes: Q_2 and Q_3. The equation of C in the affine chart $Y \neq 0$ is

$$x^d + z(\alpha + \beta z) = x^d + \beta z^2 + \alpha z = 0 \tag{4.12}$$

We now apply, to (4.12), the projective transformation given by the following matrix

$$T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{\alpha}{2\sqrt{\beta}} & \sqrt{\beta} \\ 0 & 1 & 0 \end{pmatrix}; \quad \text{note that} \quad T^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & \frac{1}{\sqrt{\beta}} & -\frac{\alpha}{2\beta} \end{pmatrix}$$

to then get the (projectively equivalent) curve C' given by the following (affine) equation

$$f(x,y) \stackrel{\text{def}}{=} x^d + y^2 - \frac{\alpha^2}{4\beta} = 0 \tag{4.13}$$

The points Q_i are taken to the following

$$\begin{aligned} T(Q_1) &= (0:1:0) \\ T(Q_2) &= (0:\alpha/2\sqrt{\beta}:1) \\ T(Q_3) &= (0:-\alpha/2\sqrt{\beta}:1) \end{aligned}$$

Recall that $T(Q_1)$ is the only singular point of C'. Note also that, for $\ell_X : X = 0$ and $U_Z : Z \neq 0$ we have $C' \cap \ell_X \cap U_Z = \{T(Q_2), T(Q_3)\}$, so that any other (*i.e.*, other than $T(Q_2)$ or $T(Q_3)$) flex $(x_0 : y_0 : 1)$ for C' will satisfy $x_0 \neq 0$. Indeed, the $f_{xx} f_y^2 + f_{yy} f_x^2 = 0$ equation for C' reads (cf. (4.13))

$$2dx^{d-2}(dx^d + 2(d-1)y^2) = 0 \tag{4.14}$$

The solutions to equations (4.13) and (4.14) corresponding to $x = 0$ give the points $T(Q_2)$ and $T(Q_3)$. There are no solutions with $y = 0$ and $x \neq 0$, and there are $2d$ solutions with $xy \neq 0$. Take one of these latter solutions, say $P_0 \stackrel{\text{def}}{=} (x_0 : y_0 : 1)$ with $x_0 y_0 \neq 0$. The tangent line to C' at P_0 is given by

$$dx_0^{d-1}(x - x_0) + 2y_0(y - y_0) = 0$$

and is parametrized as

$$\begin{cases} x = 2y_o t + x_0 \\ y = -dx_0^{d-1} t + y_0 \end{cases} \qquad t \in k \tag{4.15}$$

Substituting the parametrization (4.15) into (4.13) we obtain

$$Q_{P_0}(t) \stackrel{\text{def}}{=} (2y_0 t + x_0)^d + (-dx_0^{d-1} t + y_0)^2 - \frac{\alpha^2}{4\beta} = 0$$

The highest power of t dividing $Q_{P_0}(t)$ is exactly the order of contact $I_{P_0}(C' \cap T_{P_0} C')$. It then suffices to show that this order of contact is less than d in order to show that P_0 is not a total flex. The constant term of $Q_{P_0}(t)$ is $x_0^d + y_0^2 - \alpha^2/4\beta$, which vanishes because $P_0 \in C'$. The coefficient multiplying the monomial t is:

$$\binom{d}{d-1} 2y_0 x_0^{d-1} - 2dx_0^{d-1} y_0$$

which, again, vanishes, meaning simply that $P_0 \in T_{P_0} C'$. For the coefficient multiplying the monomial t^2, it is given by:

$$\binom{d}{d-2} 4y_0^2 x_0^{d-2} + d^2 x_0^{2d-2} = 2d(d-1) y_0^2 x_0^{d-2} + d^2 x_0^{2d-2} = dx_0^{d-2}(2(d-1)y_0^2 + dx_0^d)$$

and the factor $2(d-1)y_0^2 + dx_0^d$ vanishes once P_0 is a flex (cf. (4.14)). Then, we can finally write

$$Q_{P_0}(t) = \sum_{i=0}^{d-3} \binom{d}{i} (2y_0)^{d-i} x_0^i \cdot t^{d-i} \tag{4.16}$$

The coefficient corresponding to $i = 1$ in (4.16) is

$$\binom{d}{1} (2y_0)^{d-1} x_0 = 2^{d-1} d y_0^{d-1} x_0 \neq 0$$

because $x_0 y_0 \neq 0$ and $d(d-1) \not\equiv 0 \bmod p$ (recall that this last condition implies that $p \neq 2$). But this implies that the highest power of t diving $Q_{P_0}(t)$ is $\leq d-1$ and ≥ 3, so that P_0 is a flex but not a total one. And we are done.

In the sequence, we consider the remaining, and far more delicate, case where $d \equiv 1 \bmod p$.

4.1.2 $d \equiv 1 \bmod p$ and $p \neq 2$

The reader may want to check (HIRSCHFELD; KORCHMáROS; TORRES, 2013, Equation 1.8 and Remark 1.37) for some pertinent remarks concerning the Hessian curve for curves whose degree is $\equiv 1 \bmod p$, and for curves in characteristic 2, whence the usual second derivatives have to be replaced with the Hasse second derivatives. We do not consider $p = 2$ until subsection 4.1.3.

Let us take some steps back and look again at (4.6). With $d \equiv 1 \bmod p$ and $p \neq 2$, it becomes

$$g''(y)(y')^2 + g'(y)y'' = 0 \tag{4.17}$$

The things that were said between (4.4) and (4.5) can be said in the present scenario with the exact same words used there; in particular we have $g'(y) \neq 0$. However, it is not possible now to infer that $y'' \neq 0$ from (4.17): it could well be the case that $g''(y) = 0$ (if $p = 2$ this is always the case). But suppose, for the moment, that it is $y'' \neq 0$, *i.e.*, that C has finitely many flexes. Then, (4.8) would again be valid and, consequently, we would have $n_1 = d-1$ or $n_1 = d-2$. If $n_1 = d-1$, C would again be given by $X^d + Z^{d-1}Y = 0$. But for this curve, it cannot be made more clear to see that it holds $g''(y) = 0$, *i.e.*, that $y'' = 0$, which is contrary to our assumption. Hence n_1 cannot be $d-1$. If $n_1 = d-2$, C is given by $X^d + Z^{d-2}Y(Y + cZ) = 0$, for some $c \neq 0$, so that $g(y) = y^2 + cy$. The condition $g''(y) \neq 0$, which is equivalent to $y'' \neq 0$, is trivially satisfied, since $p \neq 2$. Letting $f(x, y) = x^d + y^2 + cy$, the mixed derivative f_{xy} still vanishes and the equation $f_{xx}f_y^2 + f_{yy}f_x^2 = 0$ simplifies to $f_{yy}f_x^2 = 0$ (f_{xx} vanishes because $d-1 \equiv 0 \bmod p$), which is

$$2d^2 x^{2(d-1)} = 0 \tag{4.18}$$

From (4.18), it follows that any flex of C must be contained on the line $X = 0$; replacing this into $f(x, y) = 0$, we obtain $y(y + c) = 0$, an equation admitting only two roots. Thus, C has only two flexes. But, if C was to have at least two outer Galois points, it would have at least $(d+1)(d-n_1) = 2(d+1) \geq 10 > 2$ total flexes. This shows, therefore, that if $d \equiv 1 \bmod p$ and $y'' \neq 0$ (and $p \neq 2$), C cannot have more than one outer Galois point.

Suppose now that $y'' = 0$, *i.e.*, that C has infinitely many flexes. Since $y'' = 0$ is equivalent to $g''(y) = 0$ (cf. (4.17)), we can "integrate" this latter equation and obtain

(recall that g is a polynomial)

$$g'(y) = a(y^p) = a(y)^p \tag{4.19}$$

for some polynomial $a(T) \in k[T]$. Integrating once more, (4.19) gives

$$g(y) = a(y)^p \cdot y + b(y)^p \tag{4.20}$$

for some other polynomial $b(T) \in k[T]$. (4.20) therefore allows us to write

$$x^{sp+1} + a(y)^p y + b(y)^p = 0 \tag{4.21}$$

for the (affine) equation of C, where $s \geq 1$. We need not worry about the points contained in the line $Z = 0$, for they reduce to the single singular point Q_1 (remind what point we assumed Q_1 to be when we started the computations in (4.3): it was assumed to be $(0 : 1 : 0)$). Now we show that the curve given by (4.21) has no total flexes outside the line $X = 0$, which is a sufficient condition for us to conclude that C has at most one outer Galois point. First of all, notice that in order for Q_1 to be a singular point, which it is, it is necessary that $\deg a^p = p \cdot \deg a < sp$ and $\deg b^p = p \cdot \deg b < sp$. From this, it follows the following: there is no monomial of degree sp in $a(y)^p \cdot y + b(y)^p$.

Take a point $P_0 = (x_0 : y_0 : 1)$ with $x_0 \neq 0$. Its tangent line, $T_{P_0}C$ is given by

$$T_{P_0}C : x_0^{sp}(x - x_0) + a(y_0)^p(y - y_0) = 0 \tag{4.22}$$

Suppose $a(y_0) = 0$. Then, from (4.22) we see that $T_{P_0}C$ reduces to $x = x_0$, which has the parametrization

$$\begin{cases} x = x_0 \\ y = t \end{cases} \qquad t \in k \tag{4.23}$$

Substitution of (4.23) into (4.21) gives

$$g_0(t) \stackrel{\text{def}}{=} x_0^{sp+1} + a(t)^p t + b(y)^p \tag{4.24}$$

If P_0 was to be a total flex, the polynomial $g_0(t)$ above would have $t = y_0$ as its unique root, whose multiplicity would have to be $sp + 1$, the degree of the curve. In other words: if P_0 is a total flex, we can write $g_0(t) = c(t - y_0)^{sp+1}$ for some $c \in k^\times$. But then, (4.24), together with the observation made above, would lead to a contradiction with the degree of the polynomial (in the variable t) $x_0^{sp+1} + a(t)^p t + b(y)^p$ that appears in its right hand side. Therefore $a(y_0) \neq 0$ must hold for P_0 to be a total flex, and under these circumstances $T_{P_0}C$ may now be parametrized as

$$\begin{cases} x = x_0 + a(y_0)^p \cdot t \\ y = y_0 - x_0^{sp} \cdot t \end{cases} \qquad t \in k \tag{4.25}$$

Substitution of (4.25) into (4.21) now gives

$$g_0(t) = (x_0 + a(y_0)^p t)^{sp+1} + a(y_0 - x_0^{sp} t)^p \cdot (y_0 - x_0^{sp} t) + b(y_0 - x_0^{sp} t)^p \tag{4.26}$$

Again, if P_0 was to be a total flex, the polynomial $g_0(t)$ above would have $t = 0$ (notice that this is the value of the parameter which corresponds to P_0) as its unique root, with multiplicity $sp+1$, the degree of the curve. In particular, the coefficient of the monomial t^{sp} in the polynomial in the right hand side of (4.26) would have to vanish. However, the earlier observation implies that the only "contribution" for such coefficient comes from the term $(x_0 + a(y_0)^p t)^{sp+1}$, and is exactly $x_0 \cdot (a(y_0)^p)^{sp}$ which is $\neq 0$ since both $x_0 \neq 0$ and $a(y_0) \neq 0$. Hence the only total flexes of the curve given by (4.21) are those in the line $X = 0$, therefore this curve cannot have more than one outer Galois point.

And to characteristic two we are now going to.

4.1.3 $d \equiv 1 \bmod p$ and $p = 2$

The "right way" to consider flexes for a curve with affine equation $f(x, y) = 0$ in characteristic 2 is using the following "modified" equation for the Hessian (cf. (HIRSCHFELD; KORCHMÁROS; TORRES, 2013, Equation 1.9)):

$$\tilde{h}(x, y) = f_x^2 \mathcal{D}_{yy} f + f_y^2 \mathcal{D}_{xx} f - f_x f_y f_{xy} \tag{4.27}$$

where $\mathcal{D}_{yy} f$ and $\mathcal{D}_{xx} f$ are the Hasse second derivatives of f with respect to y and x, respectively; writing $f(x, y) = \sum_{i,j} a_{ij} X^i Y^j$ they are given by (cf. (HIRSCHFELD; KORCHMÁROS; TORRES, 2013, Remark 1.37)):

$$\mathcal{D}_{yy} f = \sum_{i,j} a_{ij} \frac{j(j-1)}{2} X^i Y^{j-2} \quad \text{and} \quad \mathcal{D}_{xx} f = \sum_{i,j} a_{ij} \frac{i(i-1)}{2} X^{i-2} Y^j \tag{4.28}$$

We will study $\tilde{h}(x, y)$ for the curve given by (4.3), the curve that interest us. The polynomial $x^d + g(y)$ will be denoted by $f(x, y)$. For this curve, the mixed derivative f_{xy} still vanishes, so that (4.27) simplifies to

$$\tilde{h}(x, y) = f_x^2 \mathcal{D}_{yy} f + f_y^2 \mathcal{D}_{xx} f \tag{4.29}$$

If $\tilde{h}(x, y)$ is non-zero (as an element of $k(C)$), then C has finitely many flexes and we may use equation (3.3) again to conclude that $n_1 = d - 1$ or $n_1 = d - 2$ (cf. also (4.8)). We are now going to show that it is sufficient, for $\tilde{h}$ to be non-zero, that $\mathcal{D}_{yy} f$ be non-zero. First of all, recall that $g(y)$ is a separable polynomial, because $Q_1 = (0 : 1 : 0)$ is the only singular point of C, and also that we assumed $y \mid g(y)$, without loss of generality; therefore we have $g'(y) \neq 0$. We will write $g(y) = \sum_{k=1}^{d-n_1} a_k y^k$. Let us list the relevant derivatives below

- $f_x = dx^{d-1} \quad \rightsquigarrow \quad f_x^2 = d^2x^{2d-2}$
- $\mathcal{D}_{xx}f = \frac{d(d-1)}{2}x^{d-2}$
- $f_y = g'(y)$: the usual derivative
- $\mathcal{D}_{yy}f = \mathcal{D}_{yy}g = \sum_k a_k \frac{k(k-1)}{2}y^{k-2}$

It is immediate to see that $\mathcal{D}_{xx}f$ vanishes if, and only if, $d-1 \equiv 0 \bmod 4$ (recall that $d \not\equiv 0 \bmod 2$), and $\mathcal{D}_{yy}f$ vanishes if, and only if, g has monomials of degree $\equiv 0 \bmod 4$ or $\equiv 1 \bmod 4$ only. If $\mathcal{D}_{yy}f \neq 0$ and $\mathcal{D}_{xx}f = 0$, then (4.27) becomes

$$\tilde{h}(x,y) = f_x^2 \mathcal{D}_{yy}f = d^2x^{2d-2}\mathcal{D}_{yy}f$$

which is clearly non-zero. Suppose now that $\mathcal{D}_{yy}f \neq 0$ and $\mathcal{D}_{xx}f \neq 0$, but that $\tilde{h} = 0$. (4.27) would then give

$$d^2x^{2d-2}\mathcal{D}_{yy}f + (g'(y))^2 d\frac{d-1}{2}x^{d-2} = 0 \rightsquigarrow dx^{d-2}\left(dx^d\mathcal{D}_{yy}f + \frac{d-1}{2}(g'(y))^2\right) = 0 \quad (4.30)$$

and since $dx^{d-2} \neq 0$, from (4.30) it follows, after the substitution $x^d = -g(y)$, that

$$dg(y)\mathcal{D}_{yy}f = \frac{d-1}{2}(g'(y))^2 \quad (4.31)$$

But (4.31) tells that g and g' have roots in common, which cannot happen. Therefore $\tilde{h}(x,y) \neq 0$ also in this case. (4.8) may then be invoked again, from which again we conclude that $n_1 = d-1$ or $n_1 = d-2$. If it was $n_1 = d-1$, $f(x,y)$ would be $x^d + y$; but in this case, $\mathcal{D}_{yy}f = 0$. Hence, it must be $n_1 = d-2$ and $f(x,y) = x^d + y^2 + cy$ for some $c \neq 0$. Here we have $\mathcal{D}_{yy}f = 1$ and $f_y = c$; hence $\tilde{h}(x,y)$ is given by

$$dx^{d-2}\left(dx^d + c^2\frac{d-1}{2}\right) \quad (4.32)$$

If $d-1 \equiv 0 \bmod 4$, the above (4.32) reduces to d^2x^{2d-2}, from which it follows that any flex of C would have to lie in the line $X = 0$. Hence, the only two total flexes of C are those in the line $X = 0$, so that C cannot have more than one outer Galois point (otherwise, remind, it would have at least $(d+1)(d-n_1) = 2(d+1) \geq 10 > 2$ total flexes). If $d-1 \not\equiv 0 \bmod 4$, C will have other flexes besides those on the line $X = 0$. The following is pretty much the same that was done for the analogous case when $d \not\equiv 1 \bmod p$, beginning in page 100. There will be $2d$ flexes outside the line $X = 0$: there are d solutions (in x) to the equation

$$dx^d + c^2\frac{d-1}{2} = 0$$

and for each one of these solutions, there will be two solutions (in y) for the equation

$$x^d + y^2 + cy = 0 \quad (4.33)$$

Take one these flexes just mentioned: $P_0 \stackrel{\text{def}}{=} (x_0 : y_0 : 1)$. Notice that $x_0 y_0 \neq 0$. Its tangent line has the parametrization given below

$$\begin{cases} x = x_0 + ct \\ y = y_0 + dx_0^{d-1} t \end{cases} \qquad t \in k \tag{4.34}$$

and substituting it in (4.33) gives (cf. (4.16))

$$g_0(t) \stackrel{\text{def}}{=} \sum_{k=3}^{d} \binom{d}{k} x_0^{d-k} c^k t^k \tag{4.35}$$

For $k = d-1$, the corresponding coefficient in the right hand side of (4.35) is $dc^{d-1}x_0 t^{d-1}$. Once $d \not\equiv 0 \bmod 2$, $c \neq 0$ and $x_0 \neq 0$, the aforementioned coefficient does not vanish, from which it follows that P_0, yet being a flex, is not a total one. Hence, the only total flexes of C are those in the line $X = 0$ and the curve cannot have more than one outer Galois point.

If $\mathcal{D}_{yy} f = 0$ but $\mathcal{D}_{xx} f \neq 0$ (recall that this happens if, and only if, $d \not\equiv 1 \bmod 4$), we still have $\tilde{h}(x, y) \neq 0$. No matter which one of the possible two values of n_1 is (they are again $d-1$ and $d-2$), we have that any flex of C has to lie in $X = 0$, from which we conclude that, also in this case, C cannot have more than one outer Galois point. Indeed, if $n_1 = d-1$, then

$$\tilde{h}(x, y) = \frac{d(d-1)}{2} x^{d-2}$$

while if $n_1 = d-2$, and with the same notation as before, we have

$$\tilde{h}(x, y) = c^2 \frac{d(d-1)}{2} x^{d-2}$$

We now consider the remaining case: $\mathcal{D}_{yy} f = 0$ and $\mathcal{D}_{xx} f = 0$. The latter implies that $d = 4s+1$, while the former implies that g has monomials whose degrees are $\equiv 0 \bmod 4$ or $\equiv 1 \bmod 4$ only; it thus may be written as

$$g(y) = a_0 y + b_1 y^4 + a_1 y^5 + b_2 y^8 + \ldots + a_k y^{4k+1} + b_{k+1} y^{4k}$$

or as

$$g(y) = a_0 y + b_1 y^4 + a_1 y^5 + b_2 y^8 + \ldots + a_{k-1} y^{4k-3} + b_k y^{4k} + a_k y^{4k+1}$$

In any case, we may write

$$g(y) = y \cdot a(y)^4 + b(y)^4 \tag{4.36}$$

for some polynomials $a(T)$ and $b(T) \in k[T]$. Just like (4.21), we have that the equation for C now reads

$$x^{4s+1} + a(y)^4 y + b(y)^4 \tag{4.37}$$

The exact same chain of arguments used in subsection 4.1.2 and that comes after (4.21) can be used here to conclude that C does not have total flexes outside the line $X = 0$ (the

only difference is that now p will not be 2, but rather 4). Therefore, the curve under these last circumstances cannot have more than one outer Galois point too.

All that was done hitherto is finally summarized in the following

Theorem 7. Let C be a singular curve of degree $d \not\equiv 0 \bmod p$ with $d \geq 4$. Then $\delta'(C) \leq 1$.

4.2 Outer points when $d = p^e$

We now turn to the case where not only $d \equiv 0 \bmod p$, but the stronger condition $d = p^e$ holds, for some $e \geq 1$ (and, as usual $d \geq 4$). For curves under this condition on their degree, the existence of an outer Galois points makes them to be given by an equation like the one in item 2 of Theorem 3. We will suppose C is such a curve and, moreover, that it has not only one, but two outer points, which we suppose to be $P = (1:0:0)$ and $Q = (0:0:1)$. From the "point of view" of P (*i.e.*, applying Theorem 3 for P), C has equation

$$f_1(X,Y,Z) + f_2(Y,Z) = 0 \tag{4.38}$$

where $f_1(X,Y,Z)$ is an additive polynomial in the variable X and $f_2(Y,Z)$ is a homogeneous polynomial in the variables y and z only, both of them having degree p^e. More specifically, f_1 is given by

$$f_1(X,Y,Z) = \prod_{(a,b)\in G_P} (X + aY + bZ) \tag{4.39}$$

where the pair (a,b) is identified, as we did in Chapter 3, with the linear transformation given by the matrix

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

On the other hand, from the "point of view" of the other outer point Q, we may repeat the proof of item 2 of Theorem 3 with $(0:0:1)$ in place of $(1:0:0)$ and conclude that C is also is given by the following equation

$$g_1(Z,Y,X) + g_2(X,Y) = 0 \tag{4.40}$$

where g_1 and g_2 are exactly as their f counterparts, except for that now Z plays the role X plays in (4.38); we write $g_1(Z,Y,X)$ instead of $g_1(X,Y,Z)$ to emphasize this fact.

The crucial thing about the degree of C being not only $\equiv 0 \bmod p$ but a power of p is that from this it follows that (4.38) and (4.40) are two equations **for the same curve** C: there is no projective transformation in passing from one to the other. We explain why. If we were to repeat the proof of Theorem 3 (item 2), we could assume from the beginning that $(1:0:0)$ and $(0:0:1)$ are both outer points, and since, in the notation

of Theorem 3, $l = 1$ the transformation T_τ appearing in (2.13) is the identity matrix. As T_τ is the only projective transformation used throughout the proof to show that C has equation like the one in (4.38), we see that no generality is lost in supposing that C is given by (4.38) and with both $(1:0:0)$ and $(0:0:1)$ being outer points. If it was $\deg C = lp^e$ for some $l > 1$, not divisible by p, (4.38) would be an equation for C **after the suitable projective transformation** T_τ, which would not necessarily be the identity, and, consequently, would possibly mess up with the point $Q = (0:0:1)$.

This being said, we have that the polynomials in the left hand side of (4.38) and of (4.40) should "differ" by a constant $\alpha \in k^\times$:

$$f_1(X,Y,Z) + f_2(Y,Z) = \alpha(g_1(Z,Y,X) + g_2(X,Y)) \tag{4.41}$$

We now write (cf. (GOSS, 1998, Proposition 1.1.5 and Theorem 1.2.1), as well as (3.32))

$$f_1(X,Y,Z) = X^{p^e} + f_{(e-1)}(Y,Z)X^{p^{e-1}} + \ldots + f_{(1)}(Y,Z)X^p + f_{(0)}(Y,Z)X \tag{4.42}$$

and

$$g_1(Z,Y,X) = Z^{p^e} + g_{(e-1)}(Y,X)Z^{p^{e-1}} + \ldots + g_{(1)}(Y,X)Z^p + g_{(0)}(Y,X)Z \tag{4.43}$$

In the above, the polynomials $f_{(i)}(Y,Z)$ are homogeneous polynomials in the variables Y and Z only, whose correspondingly degree is $p^e - p^i$, for $i = 0,\ldots,e-1$. The same holds for the polynomials $g_{(j)}$, but with X instead of Z. Making $Y = 0$ we are, thus, left with

$$f_{(i)}(0,Z) = c_i Z^{p^e - p^i} \quad \text{and} \quad g_{(j)}(0,X) = d_j X^{p^e - p^j} \tag{4.44}$$

for some constants c_i and $d_j \in k$. Using (4.44), and plugging $Y = 0$ into equation (4.41), we obtain

$$\begin{aligned} X^{p^e} + c_{e-1}Z^{p^e-p^{e-1}}X^{p^{e-1}} + \ldots + c_1 Z^{p^e-p}X^p + c_0 Z^{p^e-1}X + cZ^{p^e} = \\ \alpha(Z^{p^e} + d_{e-1}X^{p^e-p^{e-1}}Z^{p^{e-1}} + \ldots + d_1 X^{p^e-p}Z^p + d_0 X^{p^e-1}Z + dX^{p^e}) \end{aligned} \tag{4.45}$$

where $cZ^{p^e} = f_2(0,Z)$ and $dX^{p^e} = g_2(0,X)$. (4.45) contains "mixed monomials" of the form $Z^s X^t$, for $s,t \geq 1$. These mixed monomials that appear on the left hand side all have the form $Z^{p^e-p^i}X^{p^i}$, while the ones appearing on the right hand side have the form $X^{p^e-p^j}Z^{p^j}$, for $i,j = 1,\ldots,e-1$. Being an equation between polynomials, the equality in (4.45) implies that equality must hold for the coefficients of each monomial too and, therefore, we are led to search which of the non-zero mixed monomials on one side are also non-zero on the other, *i.e.*, for which values of i and j we have

$$Z^{p^e-p^i}X^{p^i} = Z^{p^j}X^{p^e-p^j} \tag{4.46}$$

It is immediate that the above (4.46) is true precisely when $p^i + p^j = p^e$, which, for its turn, is true **only when** $p = 2$ and $i = j = e-1$. Therefore, for any p and any $i \leq e-2$, this

implies that, in (4.45), the coefficients of the mixed monomials of the form $Z^{p^e-p^i}X^{p^i}$, as well as those of the form $X^{p^e-p^j}Z^{p^j}$, must vanish, *i.e.*,

$$c_i = 0 = d_i \quad \text{for all } i = 0, \ldots, e-2 \tag{4.47}$$

We will now investigate how (4.47) affects the groups G_P and G_Q.

Back to (4.42), comparing it with (4.39), we can write the coefficient $f_{(0)}(Y,Z)$ as

$$f_{(0)}(Y,Z) = \prod_{(a,b)\in G_P\setminus\{(0,0)\}} (aY + bZ)$$

so that $f_{(0)}(0,Z) = Z^{p^e-1}\prod_{(a,b)\in G_P\setminus\{(0,0)\}} b$. Since $f_{(0)}(0,Z) = c_0 Z^{p^e-1}$ and $c_0 = 0$ (cf. (4.47)), the product $\prod_{(a,b)\in G_P\setminus\{(0,0)\}} b$ must then be zero. Hence, there must exist some non-zero element $(a,b) \in G_P$ such that $b = 0$. We will denote this element by $(a_1, 0)$. As G_P has an $\mathbb{F}_p$-linear structure, it will have at least p elements (a,b) whose second coordinate, b, all vanish: the p multiples of $(a_1, 0)$ (counting the zero element $(0,0)$).

As for $f_{(1)}(Y,Z)$, it is given by the sum of all $\binom{p^e}{p^e-p}$ products each of which is made up by a particular choice of $p^e - p$ amongst the p^e factors $(aY + bZ)$, for $(a,b) \in G_P$. Amid all these products, only one carries a chance of not vanishing when we make $Y = 0$, namely the product consisting of the $p^e - p$ factors distinct from $(va_1, 0)$, $v \in \mathbb{F}_p$. We call it $P_1(Y,Z)$. Therefore, $f_{(1)}(0,Z) = P_1(0,Z)$, and once $f_{(1)}(0,Z) = c_1 Z^{p^e-p}$ with $c_1 = 0$ (cf. (4.47)), it follows that

$$P_1(0,Z) = Z^{p^e-p} \cdot \left(\prod_{(a,b)\neq(va_1,0)} b \right) = 0 \tag{4.48}$$

Similarly to how was argued in the case of $f_{(0)}(Y,Z)$, (4.48) implies the existence of an element $(a_2, b_2) \in G_P$ distinct from $(va_1, 0)$ for all $v \in \mathbb{F}_p$, and such that $b_2 = 0$. Note that $(a_1, 0)$ and $(a_2, 0)$ are, thus, linearly independent: they span a two dimensional subspace of G_P, all of whose elements have their second coordinates equal to zero. In other words, at least p^2 between the p^e elements in G_P have their second coordinates equal to zero.

Repeating the arguments just given, we obtain $e-1$ linearly independent elements, $(a_1, 0), \ldots, (a_{e-1}, 0)$, all of them having their second coordinate vanishing. The subspace spanned by them consists of p^{e-1} elements having their second coordinate equal to zero as well. We now assume $p \neq 2$.

4.2.1 $p \neq 2$

Under this additional hypothesis, the mixed monomials $Z^{p^e-p^{e-1}}X^{p^{e-1}}$ and $X^{p^e-p^{e-1}}Z^{p^{e-1}}$ are still distinct and therefore $c_{e-1} = 0$. This implies the existence of a last element $(a_e, 0) \in G_P$, linearly independent with the older ones; it is "last" in the

sense that we now have a complete description for G_P: it is the $\mathbb{F}_p$-space spanned by the basis $\{(a_1,0),\dots,(a_e,0)\}$. Henceforth, all elements in G_P have their second coordinate equal to zero, and consequently we may write

$$f_1(X,Y,Z) = \prod_{(a,b)\in G_P} (X + aY + bZ) = \prod_{(a,0)\in G_P} (X + aY) \tag{4.49}$$

i.e., $f_1(X,Y,Z)$ does not depend on Z. The exact same considerations are valid for the group G_Q, from which we conclude that the polynomial $g_1(Z,Y,X)$ does not depend on X. We return once more to (4.42), and rewrite it using what we now know from (4.49) as

$$f_1(X,Y) - \alpha g_2(X,Y) = \alpha g_1(Z,Y) - f_2(Y,Z) \tag{4.50}$$

The object in (both sides of) (4.50) is a homogeneous polynomial of degree p^e. On the one hand, the left hand side tells us that this polynomial does not depend on Z; on the other hand, the right hand side tells it does not depend on X. So the only possibility is that it depends only on Y:

$$f_1(X,Y) - \alpha g_2(X,Y) = AY^{p^e} = \alpha g_1(Z,Y) - f_2(Y,Z) \tag{4.51}$$

The constant $A \in k$ in equation (4.51) may be zero, there is no *a priori* reason excluding this to happen. Finally, we use (4.51) to write $f_2(Y,Z) = \alpha g_1(Z,Y) - AY^{p^e}$ and then substitute into (4.38):

$$\prod_{a\in G_P} (X + aY) + \alpha \prod_{s\in G_Q} (Z + sY) - AY^{p^e} = 0 \tag{4.52}$$

After a projective change of coordinates, the above (4.52) can be written like below

$$\prod_{a\in G_P} (X + aY) + \prod_{s\in G_Q} (Z + \alpha^{1/p^e} sY) - A_\star Y^{p^e} = 0$$

where $A_\star$ is 0 or 1, depending on whether A is zero or not. It is worth noting that if A is zero and the groups G_P and G_Q are the same, then the curve will not be irreducible: it will consist of a union of p^e distinct lines.

We now investigate the genus of the curves given by an equation like the one in (4.52). Let us first rewrite (4.52). We change the variables Y and Z and get

$$f(x,z) + g(y,z) + Az^{p^e} = 0 \tag{4.53}$$

and where f_1 and g_1 had their indices dropped out. Recall that $A \in \{0,1\}$. There is no loss in generality to assume that $A = 0$: if $A = 1$ there is a suitable constant $s \in k$ such that $f(s,1) + A = 0$, so that after the projective change $X \mapsto X + sZ$ the previous (4.53) reads:

$$H(X,Y,Z) \stackrel{\text{def}}{=} f(X,Z) + g(Y,Z) = 0$$

where, recall, f and in g are additive separable polynomials in the first variable. One could also take the projective change $Y \mapsto Y + s'Z$, for some appropriate s', instead of the

transformation considered above. We then have that $H_X = x_0 Z^{p^e-1}$ and $H_Y = y_0 Z^{p^e-1}$, for some $x_0 \neq 0$ and $y_0 \neq 0$, from which it follows that the only singular point of C is $(-1:1:0)$. We point out the following: we did not explicitly assumed C to be singular from the beginning of section 4.2: we just assumed C to have 2 extendable outer Galois points and concluded from this that C is singular. Note that the two outer Galois points and the singular point are all contained in the line at infinity $Z = 0$: the Galois points are $(1:0:0)$ and $(0:1:0)$, and the singular point is $(-1:1:0)$.

We could also have started with two monic additive separable polynomials $f(T)$ and $g(T)$ in $k[T]$, both having the same degree p^e, and have considered the curve (assume it is irreducible) given by

$$f_h(X,Z) + g_h(Y,Z) = 0 \tag{4.54}$$

where f_h and g_h are the homogenizations of f and g. Under these conditions, the curve in equation (4.54) has $(1:0:0)$ and $(0:1:0)$ as two extendable outer Galois points (by Theorem 3) and $(-1:1:0)$ as its only singular point, and all of them lie in the line $Z = 0$. The Galois groups are isomorphic to the groups of roots of f and g. Remind that a monic additive separable polynomial is uniquely determined by its group of roots, which is, for its turn, uniquely determined by e $\mathbb{F}_p$-linearly independent elements, once it is an elementary abelian finite group.

With this in mind, in order for the curve in (4.54) to be irreducible, it is necessary that the additive polynomials f and g, or equivalently, the groups G_P and G_Q, be distinct. For otherwise, we could write

$$f_h(X,Z) + f_h(Y,Z) = f_h(X+Y,Z) = Z^{p^e} \cdot f((X+Y)/Z)$$

and once f splits completely in $k[T]$ (recall that k is algebraically closed), we see that the curve would consist in a union of p^e distinct lines. The question of when the left hand side of (4.54) is reducible is fully answered in (DEOLALIKAR, 2002, Proposition 2.6).

We will consider (4.54) in the affine plane $Z \neq 0$. There it reads

$$f(x) + g(y) = 0 \tag{4.55}$$

Let $\mathbb{F}_Q$ be a finite field containing all roots of $f(T)$ and $g(T)$. We say that an additive polynomial is q-additive if all its monomials have degree a power q^i of q. It is well known (see (GARCIA; ÖZBUDAK, 2007, Corollary 2.5)) that if $p(T)$ is a q-additive polynomial splitting in $\mathbb{F}_Q$, then there exists another q-additive polynomial $r(T)$, which also splits in $\mathbb{F}_Q$, such that $p(r(T)) = T^Q - T = r(p(T))$. It then follows that there exist polynomials $a(T)$ and $b(T)$ such that $f(a(T)) = T^Q - T$ and $g(-b(T)) = -T^Q + T$ and so $(a(T), -b(T))$ is a parametrization for the curve, therefore it is a rational curve, *i.e.*, its genus is zero.

Writing

$$f(x) = x^{p^e} + a_{e-1}x^{p^{e-1}} + \ldots + a_1x^p + a_0x$$
$$g(y) = y^{p^e} + b_{e-1}y^{p^{e-1}} + \ldots + b_1y^p + b_0y$$

we see that after the projective change $x \mapsto x - a_0^{-1}b_0y$, the curve C is projectively equivalent to the one with equation

$$x^{p^e} + a_{e-1}x^{p^{e-1}} + \ldots + a_1x^p + a_0x + \beta_e y^{p^e} + \beta_{e-1}y^{p^{e-1}} + \ldots + \beta_1 y^p = 0 \tag{4.56}$$

But then, C has equation like the one in (FUKASAWA, 2011, Theorem 1(4)). By this same result C has infinitely many outer points, and it is strange as well (cf. also Theorem 2). Notice that the rationality of C could also be concluded by (FUKASAWA, 2011, Theorem 1). We summarize this below.

Theorem 8. Let C be an irreducible curve of degree $p^e \geq 4$ for some $p \geq 3$ and $e \geq 1$. If C has two outer Galois points, then it is a strange rational curve with infinitely many extendable outer Galois points.

We go back a few lines above, when we assumed $p \neq 2$, to consider the opposite and remaining case.

4.2.2 $p = 2$

Now the mixed monomial $Z^{2^{e-1}}X^{2^{e-1}}$ appears on both sides of (4.45), so it must be $c_{e-1} = \alpha d_{e-1}$, but not necessarily $c_{e-1} = 0 = d_{e-1}$. Thus, a basis for G_P as an $\mathbb{F}_2$-linear space is given by $\{(a_1,0),\ldots,(a_{e-1},0),(A,B)\}$, for some a_i, A and $B \in k$. Any element in G_P is then given by

$$\left(\sum_{i=1}^{e-1} \nu_i a_i + \nu_e A, \nu_e B\right) \tag{4.57}$$

for some list $(\nu_1,\ldots,\nu_e) \in \mathbb{F}_2^e$. Conversely, any list in $\mathbb{F}_2^e$ gives rise to an element in G_P via (4.57). But as $\mathbb{F}_2 = \{0,1\}$, we can break up G_P into two disjoint sets depending on whether $\nu_e = 0$ or $\nu_e = 1$, which allows us to write the following for the polynomial $f_1(X,Y,Z)$:

$$f_1(X,Y,Z) = \prod_{(\nu_1,\ldots,\nu_{e-1})\in\mathbb{F}_2^{e-1}} \left(X + \sum_i \nu_i a_i Y\right) \cdot \prod_{(\nu_1,\ldots,\nu_{e-1})\in\mathbb{F}_2^{e-1}} \left(X + \sum_i \nu_i a_i Y + AY + BZ\right) \tag{4.58}$$

We will denote by $\hat{f}_1(X,Y)$ the first of the two products that appear above, *i.e.*:

$$\hat{f}_1(X,Y) \stackrel{\text{def}}{=} \prod_{(\nu_1,\ldots,\nu_{e-1})\in\mathbb{F}_2^{e-1}} \left(X + \sum_i \nu_i a_i Y\right)$$

It is clear that this $\hat{f}_1$ is, like f_1, an additive polynomial in the variable X; in fact $\hat{f}_1$ is a degree 2^{e-1} factor of f_1. Thus, (4.58) is rewritten as

$$f_1(X,Y,Z) = \hat{f}_1(X,Y)\cdot\hat{f}_1(X+AY+BZ,Y)$$

Completely analogous considerations hold for G_Q and $g_1(z,y,x)$. We therefore take

$$\{(b_1,0),\ldots,(b_{e-1},0),(S,T)\}$$

to be a basis of G_Q over $\mathbb{F}_2$. Notice that, as can easily be seen, $c_{e-1} = B^{2^{e-1}}$ and $d_{e-1} = T^{2^{e-1}}$; hence $B^{2^{e-1}} = \alpha T^{2^{e-1}}$, so that B vanishes if and only if T does, and in such case the results we obtained for odd characteristic are recovered. Once more, we rewrite (4.41):

$$\hat{f}_1(X,Y)\hat{f}_1(X+AY+BZ,Y)+f_2(Y,Z) = \alpha\hat{g}_1(Z,Y)\hat{g}_1(Z+SY+TX,Y)+\alpha g_2(X,Y) \quad (4.59)$$

Making $X = 0$ in (4.59) leads to

$$f_2(Y,Z) = \alpha\hat{g}_1(Z,Y)\hat{g}_1(Z+SY,Y)+\alpha\gamma Y^{2^e}$$

where $\gamma Y^{2^e} = g_2(0,Y)$. The equation for C is thus given by

$$\hat{f}_1(X,Y)\hat{f}_1(X+AY+BZ,Y)+\alpha\hat{g}_1(Z,Y)\hat{g}_1(Z+SY,Y)+\alpha\gamma Y^{2^e} = 0 \quad (4.60)$$

Suppose it was $B \neq 0$. The polynomial in the left hand side of (4.60) must be invariant under the projective transformation $Z \mapsto Z+\sigma Y$ (and leaving X and Y fixed), for any $\sigma = \sum_i \nu_i b_i$. Substituting this transformation in the polynomial in (4.60) we obtain

$$\hat{f}_1(X,Y)\hat{f}_1(X+(A+B\sigma)Y+BZ,Y)+\alpha\hat{g}_1(Z,Y)\hat{g}_1(Z+SY,Y)+\alpha\gamma Y^{2^e} = 0 \quad (4.61)$$

The product $\hat{g}_1(Z,Y)\hat{g}_1(Z+SY,Y)$ does not change because of the very definition of $\hat{g}_1$. Comparing (4.60) and (4.61) gives

$$\hat{f}_1(X+AY+BZ,Y) = \hat{f}_1(X+(A+B\sigma)Y+BZ,Y) \quad \rightsquigarrow \quad \hat{f}_1(B\sigma Y,Y) = 0 \ \ \forall\sigma \quad (4.62)$$

Note that we used the additiveness of $\hat{f}_1$. From (4.62) it follows that the roots of $\hat{f}_1$ are obtained from the roots of $\hat{g}_1$ by simply multiplying by B. Hence, we may write

$$\hat{g}_1(Z,Y) = \prod_{\lambda}\left(Z+\frac{\lambda}{B}Y\right) \quad (4.63)$$

where $\lambda = \sum_i \nu_i a_i$ runs over the roots of $\hat{f}_1$. After changing Z to Z/B, (4.63) reads

$$\hat{g}_1(Z/B,Y) = \frac{1}{B^{2^e}}\prod_{\lambda}(Z+\lambda Y) = \frac{1}{B^{2^e}}\hat{f}_1(Z,Y) \quad (4.64)$$

One more substitution, of (4.64) into (4.60), and we can finally write the equation of C like below:

$$\hat{f}_1(X,Y)\hat{f}_1(X+AY+Z,Y)+\alpha B^{-2^e}\hat{f}_1(Z,Y)\hat{f}_1(Z+BSY,Y)+\alpha\gamma Y^{2^e} = 0$$

And from here more investigations are still to be done.

4.3 Inner smooth points with $d \not\equiv 1 \bmod p$

If we now consider a singular curve C whose degree d is $\not\equiv 1 \bmod p$, and as usual with $d \geq 4$, we will be able to do a similar analysis to the one we did throughout of section 4.1, the conclusion of which has to do with Theorem 7, and is stated below.

Theorem 9. With C as above, if it is not projectively equivalent to $YX^{d-1} + Z^d = 0$ with d a power of p, then $\delta(C) \leq 1$. Otherwise C has infinitely many inner smooth Galois points (cf. Theorem 1 and also (FUKASAWA; HASEGAWA, 2010)).

Proof. Let $P = (1 : 0 : 0)$ be an inner smooth point for C. Theorem 3 (item 1) then gives the following for the equation of C

$$YX^{d-1} + G_d(Y, Z) = 0$$

where $G_d(Y, Z)$ is a homogeneous polynomial of degree d not divisible by Y (otherwise C would be reducible). It follows that the singular points of C are exactly the points on the line $X = 0$ corresponding to the repeated roots of $G_d(Y, Z)$ (notice that the only point of the curve in the line $Y = 0$ is P). Writing, like we did back in (4.2), $G_d(Y, Z) = \ell_1^{n_1} \cdot \ldots \cdot \ell_s^{n_s}$, where $\ell_i = (z_i Y - y_i Z)$, we have

$$C \cap \ell_X = \{Q_i = (0 : y_i : z_i) \mid i = 1, \ldots, s\}$$

where ℓ_X is the line $X = 0$. By the irreducibility of C, the y_i's must all be non-zero. The point Q_i will be singular if, and only if, $n_i \geq 2$. Without loss of generality, suppose that $\ell_1 = Z$, and hence that $Q_1 = (0 : 1 : 0)$. There are three possible and distinct scenarios, and they are described below.

- $n_1 < d - 1$: in this case Q_1 has multiplicity n_1 and its unique tangent line is ℓ_1.
- $n_1 = d - 1$: in this case Q_1 still has multiplicity $n_1 = d - 1$, but now it is an ordinary singular point: if we write $G_d(Y, Z) = \ell_1^{d-1}\ell_2 = Z^{d-1}(aY + bZ)$, with $ab \neq 0$, then its tangent lines are given by the $d - 1$ distinct factors of $X^{d-1} + aZ^{d-1}$.
- $n_1 = d$: in this case Q_1 has multiplicity $d - 1$, its unique tangent line is $X = 0$ and C is nothing but the curve given by $YX^{d-1} + Z^d = 0$.

These same considerations hold, *mutatis mutandis*, for the other points Q_i. Since C is singular, it has a singular point, which we may assume to be Q_1. If $n_1 < d - 1$ then Q_1 has ℓ_1 as its unique tangent line, and this line intersects C only at Q_1 and P. If $R \neq P$ was another inner smooth Galois point, we would conclude by the same reasoning that the tangent line to Q_1 intersects C only at Q_1 and R, which would then imply that $R = P$. This contradiction shows that P is the unique inner smooth Galois point in such cases (those for which C has a singular point of multiplicity $< d - 1$).

Now if $n_1 = d$, the curve is given by $YX^{d-1} + Z^d = 0$, and the tangent line to Q_1, which is the only singular point, does not pass through P: it intersects the curve only at Q_1. If d is a power of p this curve has infinitely many inner smooth Galois points: any point in C distinct from Q_1 is an inner smooth Galois point (cf. (FUKASAWA; HASEGAWA, 2010, Theorem 1 and Example 1) and also Theorem 1). We therefore suppose that d is not a power of p, and will show that C does not have any total flex other than P. From this we will be able to conclude, using the fact that inner smooth Galois points are total flexes (cf. Corollary 1), that C cannot have any inner smooth Galois point other than P. We, thus, suppose $P_0 = (x_0 : y_0 : 1) \in C$. Note that the only points of the curve in the line $Z = 0$ are P and Q_1, so that we may indeed restrict ourselves to the affine chart $Z \neq 0$. Once $y_0 x_0^{d-1} + 1 = 0$, it must be $x_0 y_0 \neq 0$. The tangent line to C at P_0 is given by (in affine coordinates x and y)

$$T_{P_0}C : (d-1)y_0x^{d-2}(x-x_0) + x_0^{d-1}(y-y_0) = 0 \rightsquigarrow (d-1)y_0(x-x_0) + x_0(y-y_0) = 0 \quad (4.65)$$

and has the following parametrization

$$\begin{cases} x = x_0 + x_0 t = x_0(1+t) \\ y = y_0 - (d-1)y_0 t = y_0(1-(d-1)t) \end{cases} \qquad t \in k \qquad (4.66)$$

Substituting the parametrization given by (4.66) in $yx^{d-1} + 1$, the affine polynomial of the curve, gives

$$g_0(t) \stackrel{\text{def}}{=} y_0 x_0^{d-1}(1-(d-1)t)(1+t)^{d-1} + 1 \qquad (4.67)$$

It suffices, for us to show that P_0 is not a total flex for C, that the coefficient of any monomial of degree $< d$ in $g_0(t)$ be non-zero (recall that the intersection multiplicity $I_{P_0}(C \cap T_{P_0}C)$ is precisely the highest power of t that divides $g_0(t)$). Since $y_0 x_0^{d-1} + 1 = 0$ we may rewrite (4.67) like below

$$g_0(t) = y_0 x_0^{d-1} \left(\sum_{k=1}^{d-1} \left(\binom{d-1}{k} - (d-1)\binom{d-1}{k-1} \right) t^k - (d-1)t^d \right) \qquad (4.68)$$

From (4.68) above, it is immediate to see that P_0 is a total flex for C if, and only if, $\binom{d-1}{k} - (d-1)\binom{d-1}{k-1} = 0$ for all $k = 1, \ldots, d-1$. Take $k = d-1$, for instance. The preceding condition for this value of k reads $1 - (d-1)^2 \equiv 0 \bmod p$, which then implies $d \equiv 0 \bmod p$ or $d \equiv 2 \bmod p$. If none of these is the case, then the coefficient of the monomial t^{d-1} in (4.68) is non-zero, so that P_0 is not a total flex. Thus, suppose $d \equiv 2 \bmod p$ (and also that $p \neq 2$). In this case, the coefficient of the monomial t^2 in (4.68) reduces to $-(d-1)^2$, which is non-zero; hence P_0 cannot be a total flex. Suppose, finally, that $d \equiv 0 \bmod p$ (recall that we also assumed d not to be a power of p). In this case $d - 1 \equiv -1 \bmod p$. (4.67) then becomes

$$g_0(t) = y_0 x_0^{d-1}(1+t)^d + 1 \qquad (4.69)$$

Since d is not a power of p, it is easy to see from (4.69) that $g_0(t)$ will have non-zero terms of degree less than d. Therefore P_0 cannot be a total flex in this case also.

It remains to consider the scenario where $n_1 = d-1$, for which the curve is given by the following equation $YX^{d-1} + Z^{d-1}(aY + bZ) = 0$, for some $ab \neq 0$. Recall that inner smooth points are total flexes (cf. Corollary 1). The only points of C on the line $X = 0$ are Q_1, the singular point, and $Q_2 = (0 : -b : a)$, which is not a total flex: its tangent line, ℓ_2, intersects C at $P \neq Q_2$ also, so that the intersection multiplicity $I_{Q_2}(C \cap \ell_2)$ is $d-1$. Hence, if there was another Galois point R, it would have its x-coordinate different from zero (and would not be P). The orbit of R by the action of G_P, which is generated by $\mathrm{diag}(\zeta_{d-1}, 1, 1)$ (cf. Theorem 3 (item 1)), would then consist of $d-1$ inner smooth points distinct from P, so that C would have at least d inner smooth points (cf. Proposition 1 and Proposition 7). Each one of these inner smooth points is a total flex for C, and to each one of them there corresponds a $(d-(q(C)-1))$ flex. We will now show that $q(C) = 2$, *i.e.*, that the Hessian of C does not vanish on C. Denote by $f(x, y) = yx^{d-1} + ay + b$. The cases $p \neq 2$ and $p = 2$ are considered separately, and we start with the former, where the equation for the Hessian of C reads (cf. (4.9): we made $f = 0$ and cancelled the common $d-1$)

$$f_x^2 f_{yy} + f_y^2 f_{xx} - 2 f_x f_y f_{xy} \tag{4.70}$$

Once $f_{yy} = 0$, (4.70) reduces to

$$f_y^2 f_{xx} - 2 f_x f_y f_{xy} = f_y(f_y f_{xx} - 2 f_x f_{xy}) \tag{4.71}$$

Since $f_y = x^{d-1} + a \neq 0$ (otherwise x would be constant and not have any zeroes), from (4.71) it follows that in order for the Hessian of C to not vanish it suffices that $f_y f_{xx} - 2 f_x f_{xy}$ does not. After carrying out the differentiation processes, we have that this latter function is given by

$$(d-1)(d-2)(x^{d-1} + a) y x^{d-3} - 2(d-1)^2 y x^{2d-4} = (d-1) y x^{d-3}(-d x^{d-1} + (d-2)a) \tag{4.72}$$

and each of the factors in (4.72) is non-zero: $-dx^{d-1} + (d-2)a$ would vanish if, and only if, $p = 2$, which is not the case. Therefore, if $p \neq 2$ the generic order of contact for C equals 2. For $p = 2$, (4.70) must be replaced by (cf. (4.27))

$$f_x^2 \mathcal{D}_{yy} f + f_y^2 \mathcal{D}_{xx} f - f_x f_y f_{xy} \tag{4.73}$$

where $\mathcal{D}_{yy} f$ and $\mathcal{D}_{xx} f$ are the Hasse second derivatives of f with respect to y and x respectively, given by (4.28). Again, $\mathcal{D}_{yy} f = 0$, so that (4.73) simplifies to

$$f_y^2 \mathcal{D}_{xx} f - f_x f_y f_{xy} = f_y(f_y \mathcal{D}_{xx} f - f_x f_{xy}) \tag{4.74}$$

Again, it must be shown that $f_y \mathcal{D}_{xx} f - f_x f_{xy}$ does not vanish. Substituting the derivatives, the aforesaid function becomes

$$\begin{aligned}(d-1)\frac{(d-2)}{2}(x^{d-1}+a)yx^{d-3} - (d-1)^2 yx^{2d-4} = \\ = (d-1)yx^{d-3}\left(\frac{(d-2)}{2}(x^{d-1}+a) - (d-1)x^{d-1}\right)\end{aligned} \tag{4.75}$$

If $d-2 \equiv 0 \bmod 4$, (4.75) turns into

$$(d-1)yx^{d-3}(-(d-1)x^{d-1}) \tag{4.76}$$

while if $d-2 \not\equiv 0 \bmod 4$ (recall that $d-2$ is even, hence, $d-2 \equiv 2 \bmod 4$ in this case), then both $(d-2)/2$ and $d-1$ are odd, so that (4.75) becomes

$$(d-1)yx^{d-3}\left(\frac{d-2}{2}a\right) \tag{4.77}$$

Both (4.76) and (4.77) are non-zero; therefore the curve C also has non-vanishing Hessian if $p = 2$, *i.e.*, its generic order of contact is 2.

Since C has a $(d-1)$-fold point, it is rational, hence its genus $g(C)$ is zero. The divisor $\mathcal{W}(C)$ mentioned in the beginning of section 3.2 has now the following degree (cf. (STöHR; VOLOCH, 1986, p. 6), (FUKASAWA, 2007, Section 2) and also Remark 8)

$$\deg \mathcal{W}(C) = 3d + 3(2g(C) - 2) = 3d - 6 \tag{4.78}$$

and we still have (cf. (3.9))

$$\sum_{P \in C \setminus \{Q_1\}} I_P(C \cap T_P C) - q(C) = \sum_{P \in C \setminus \{Q_1\}} I_P(C \cap T_P C) - 2 \leq \deg \mathcal{W}(C) \tag{4.79}$$

Under the hypothesis that C has at least two inner smooth Galois points, by what we just saw some lines above, the sum in the left hand side of (4.79) is at least $d(d-q(C)) + d(d-1-q(C)) = d(2d-5)$. Substituting this into (4.79) and using (4.78) gives

$$d(2d-5) \leq 3d-6 \rightsquigarrow 2(d-3)(d-1) \leq 0 \tag{4.80}$$

But $d \geq 4$, so (4.80) is never satisfied. Hence C cannot have more than one inner smooth Galois point. And we are finally done.

□

BIBLIOGRAPHY

ARBARELLO, E.; CORNALBA, M.; GRIFFITHS, P.; HARRIS, J. D. **Geometry of algebraic curves**. 1985. ed. New York, NY: Springer, 2010. (Grundlehren der mathematischen Wissenschaften). Citation on page 24.

BARS, F. On the automorphisms groups of genus 3 curves. 2005. Citations on pages 36, 37, 38, 39, 40, and 41.

BAYER, V.; HEFEZ, A. Strange curves. **Communications in Algebra**, Taylor & Francis, v. 19, n. 11, p. 3041–3059, 1991. Available: <https://doi.org/10.1080/00927879108824305>. Citation on page 18.

CHANG, H. C. On plane algebraic curves. **Chinese journal of mathematics**, v. 6, n. 2, p. 185–189, 1978. Citations on pages 20, 24, 43, and 82.

DEOLALIKAR, V. Determining irreducibility and ramification groups for an additive extension of the rational function field. **Journal of Number Theory**, v. 97, p. 269–286, 2002. Citations on pages 32 and 111.

DOLGACHEV, I. V. **Classical Algebraic Geometry: A Modern View**. [S.l.]: Cambridge University Press, 2012. Citations on pages 36 and 37.

DUYAGUIT, M. C. L.; YOSHIHARA, H. Galois lines for normal elliptic space curves. **Algebra Colloquium**, v. 12, p. 205–212, 2005. Citation on page 13.

FUKASAWA, S. On the number of galois points for a plane curve in positive characeristic, ii. **Geometriae Dedicata**, v. 127, p. 131–137, 2007. Citations on pages 25, 31, 50, 52, 54, 70, 98, and 117.

____. On the number of galois points for a plane curve in positive characeristic. **Communications in Algebra**, v. 36, p. 29–36, 2008. Citations on pages 50, 52, 54, and 70.

____. Galois points for a plane curve in arbitrary characteristic. **Geometriae Dedicata**, v. 139, p. 211–217, 2009. Citation on page 13.

____. On the number of galois points for a plane curve in positive characeristic, iii. **Geometriae Dedicata**, v. 146, p. 9–20, 2010. Citations on pages 50, 55, 56, 57, 58, 60, 62, 67, 69, and 73.

____. Classification of plane curves with infinitely many galois points. **Journal of the Mathematical Society of Japan**, v. 63, n. 1, p. 195–209, 2011. Citations on pages 24, 50, and 112.

____. Complete determination of the number of galois points for a smooth plane curve. **Rendiconti del Seminario Matematico della Università di Padova**, v. 129, p. 71–77, 2013. Citations on pages 14, 43, 71, 82, and 86.

____. Automorphism groups of smooth plane curves with many galois points. **Nihonkai Mathematical Journal**, v. 25, n. 1, p. 69–75, 2014. Citation on page 71.

FUKASAWA, S.; HASEGAWA, T. Singular plane curves with infinitely many galois points. **Journal of Algebra**, v. 323, p. 10–13, 2010. Citations on pages 23, 24, 114, and 115.

FUKASAWA, S.; MIURA, K. Galois points for a plane curve and its dual curve. **Rendiconti del Seminario Matematico della Università di Padova**, v. 132, p. 61–74, 2014. Citation on page 19.

GARCIA, A.; ÖZBUDAK, F. Some maximal function fields and additive polynomials. **Communications in Algebra**, v. 35, p. 1553–1566, 2007. Citation on page 111.

GOSS, D. **Basic Structures of Function Field Arithmetic**. [S.l.]: Springer, 1998. Citations on pages 66 and 108.

HIRSCHFELD, J. W. P.; KORCHMáROS, G.; TORRES, F. **Algebraic Curves over a Finite Field**. Princeton University Press, 2013. ISBN 9781400847419. Available: <https://doi.org/10.1515/9781400847419>. Citations on pages 16, 18, 20, 52, 87, 88, 89, 102, and 104.

HOMMA, M. Funny plane curves in characteristic $p > 0$. **Communications in Algebra**, v. 15, p. 1469–1501, 1987. Citation on page 50.

____. A souped-up version of Pardini's theorem and its application to funny curves. **Compositio Mathematica**, Kluwer Academic Publishers, v. 71, n. 3, p. 295–302, 1989. Available: <http://www.numdam.org/item/CM_1989__71_3_295_0/>. Citation on page 54.

____. Galois points for a hermitian curve. **Communications in Algebra**, v. 34, p. 4503–4511, 2006. Citations on pages 19, 50, and 51.

IITAKA, S. **Algebraic Geometry**. 1. ed. [S.l.]: Springer-Verlag, 1982. (Graduate Texts in Mathematics, v. 76). Citations on pages 43 and 44.

MITCHELL, H. H. Determination of the ordinary and modular ternary linear groups. **Transactions of the American Mathematical Society**, v. 12, n. 2, p. 207–242, 1911. Citations on pages 22, 23, and 76.

MIURA, K.; YOSHIHARA, H. Field theory for function fields of plane quartic curves. **Journal of Algebra**, v. 226, p. 283–294, 2000. Citations on pages 13, 18, and 44.

NAKAJIMA, S. p-ranks and automorphism groups of algebraic curves. **Transactions of the American Mathematical Society**, v. 303, n. 2, p. 595–607, 1987. Citations on pages 87 and 89.

NAMBA, M. **Geometry of Projective Algebraic Curves**. [S.l.]: Dekker, 1984. Citation on page 19.

STICHTENOTH, H. **Algebraic Function Fields and Codes**. 2. ed. [S.l.]: Springer-Verlag, 2009. (Graduate Texts in Mathematics, v. 254). Citations on pages 17, 19, 21, 32, 43, and 63.

STöHR, K.-O.; VOLOCH, J. F. Weierstrass points and curves over finite fields. **Proceedings of the London Mathematical Society**, s3-52, n. 1, p. 1–19, 1986. Available: <https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/plms/s3-52.1.1>. Citations on pages 43, 50, 52, 98, and 117.

TZERMIAS, P. The group of automorphisms of the fermat curve. **Journal of Number Theory**, v. 53, p. 173–178, 1995. Citations on pages 40 and 41.

YOSHIHARA, H. Function field theory of plane curves by dual curves. **Journal of Algebra**, v. 239, p. 340–355, 2001. Citations on pages 25, 32, 44, 46, 47, and 52.

____. Rational curve with galois point and extendable galois automorphism. **Journal of Algebra**, v. 321, p. 1463–1472, 2009. Citations on pages 24, 25, and 33.


ICMC
USP
SÃO CARLOS