Research in Number Theory

RESEARCH

A complete study of the ramification for any separable cubic global function field

Sophie Marques and Jacob Ward

*Correspondence:
smarques@sun.ac.za
University of Stellenbosch,
Stellenbosch, South Africa

Preface: Dr. Jacob Ward passed away suddenly, before this paper was finished to be reviewed. It is with deep sadness that the second author reviewed the paper without him in honours of his memory. We often spoke about the fact that research should always be accessible and understandable to the young future generations more than anything else and respect the authenticity of different authors with different styles.

Abstract

We explicitly describe the ramified places in any separable cubic extension of a cubic global function field in terms of a unique given parameter. This is all done using the uniqueness of the purely cubic closure, which is a useful new tool for the study of cubic function fields. We give a notion of local standard forms, that is useful for many purposes, including classifying and computing of integral bases. We then determine explicitly the genus of any separable cubic extension of any global function field given the minimal polynomial of the extension. The formulae we obtain is particularly useful for further study owing to the well-understood and straightforward close relation between the parameter we define and ramification within the extension.

Keywords: Cubic, Function field, Finite field, Genus, Ramification

Mathematics Subject Classification: (Primary): 11T06, (Secondary): 11R32, 11R16, 11T55, 11R58

1 Introduction

Let K be an arbitrary field of characteristic p, the authors in [5] (Theorem 1.1) proved that any separable cubic extension of an arbitrary field K admits a generator y, explicitly determined in terms of an arbitrary initial generating equation, such that

(1) $y^3 = a$, with $a \in K$, or
(2) (a) $y^3 - 3y = a$, with $a \in K$, when $p \neq 3$, or
  (b) $y^3 + ay + a^2 = 0$, with $a \in K$, when $p = 3$.

In this paper, the base field K will be a one-variable global function field. As we will show in the following, this classification allows one to deduce the ramification at any place of K to obtain an explicit formulae for the different, and therefore in §3.3, we deduce explicit Riemann–Hurwitz formulae (Theorems 5.2, 5.4, 5.7), which are computable entirely using the single parameter a as above for the minimal polynomial of the extension.

The ramification and Riemann–Hurwitz formulae have previously been studied for function fields extensions as they give important insights toward understanding them better (see [12, Corollaries 2.2, 2.3 and 2.6], [9,10,14]: biquadratic case). Degree 2 separable extensions are Galois either Kummer or Artin-Shreier extensions, therefore the study of ramification and Riemann–Hurwitz formulae are well-known (see [13]).

The study of the ramification is interesting in the way that it uses the new notion of purely cubic closure and it uniqueness, which we have previously defined in the paper [5].

Notably, through this work, when the extension is Galois (Corollary 4.6), we proved that only even degree places can be ramified for cubic extension of the form (2)(a) (which are called impurely cubic extension) but not of the form (1) whereas there are no restrictions on the degree for any other type of cubic extensions. We have also proven that, unlike in the known cases (Kummer and Artin-Schreier), the place at infinity can always be chosen unramified (Corollary 4.7). This makes the study of impure cubics promising as an initial case for a better understanding of situations that do not fall within the traditional Kummer and Artin-Schreier theory. This work does not omit any of the possible cases of separable cubic extensions, and does not exclude any field characteristic. For completeness of the present paper, we chose to include the study of the purely cubic extensions to keep the paper as self-contained as possible.

Importantly, the techniques used have been chosen as such, as they can be generalised for higher degree extensions: For instance, they have been already used in [4]. Moreover, not all Riemann–Hurwitz formulae have equal ranges of applications or usability; the major advantage of our formulae is that there is a very close and understood connection between the form of the parameter and the resulting Riemann–Hurwitz formulae. Not every parameter of the form as in (1) and (2) permits this connection directly, but it is possible to choose parameters in a natural way so that ramification can be read off this parameter easily. We call these *standard forms* for (1) and (2) (see Lemma 4.1, Theorem 4.4, and Lemma 4.9). These choices of parameters are important in addition to our Riemann–Hurwitz formulae, as this well understood relationship between them permits to compute explicit integral bases for any separable cubic function field (see [6]) in a generalisable way for higher degree extensions. Such formulae are also very useful towards a classification of cubic fields given prescribed ramification data (This connect with [2,8]). They possibly as well help to the understanding the structure of the corresponding moduli spaces, computing Weierstrass points, and so on. We do not do this here but see possibility for this based on success with generating these formulae.

Using the present work, one could also algorithmically obtain - for any cubic extension over a rational field given in any arbitrary form - a minimal polynomial such that ramification data can be completely read off by factorising the associated parameter and thereby compute the genus.

2 Notation

Throughout the paper we denote the characteristic of the field by p (including the possibility $p = 0$). We let K denote a one-variable global function field with field of constants k. Let $\overline{K}$ be a fixed algebraic closure of K. For an extension L/K, we let $\mathcal{O}_{L,x}$ denote the integral closure of $k[x]$ in L where x is a transcendental element over k in K. We denote by $\mathfrak{p}$ a place of K. We denote $v_{\mathfrak{p}}(a)$ the valuation of $a \in L$ at $\mathfrak{p}$ (for the definition we refer to [13, §2.2]). The *degree* $d_K(\mathfrak{p})$ of $\mathfrak{p}$ is defined as the degree of its residue field, which we denote by $k(\mathfrak{p})$, over the constant field k. For a place $\mathfrak{P}$ of L over $\mathfrak{p}$, we let $f(\mathfrak{P}|\mathfrak{p}) = [k(\mathfrak{P}) : k(\mathfrak{p})]$ denote the inertia degree of $\mathfrak{P}|\mathfrak{p}$. We let $e(\mathfrak{P}|\mathfrak{p})$ be the ramification index of $\mathfrak{P}|\mathfrak{p}$, i.e., the unique positive integer such that $v_{\mathfrak{P}}(z) = e(\mathfrak{P}|\mathfrak{p})v_{\mathfrak{p}}(z)$, for all $z \in K$. If $v_{\mathfrak{p}}(a) \geq 0$, then we let

$$\overline{a} := a \mod \mathfrak{p}$$

denote the image of a in $k(\mathfrak{p})$.

We will denote g_L for the genus of the function field L defined in [13, Definition 3.3.4]. The differential exponent at a given place is closely related to the ramification at that place and permits one to obtain explicit genus formulae, such as the one obtained in this paper. We will denote by $d(\mathfrak{P}|\mathfrak{p})$ the differential exponent at the place $\mathfrak{p}$ in L/K, as it is defined in [13, §5.6].

Henceforth, we let F denote a field and $p = \text{char}(F)$ the characteristic of this field, where we admit the possibility $p = 0$ unless stated otherwise. We let $\overline{F}$ denote a fixed algebraic closure of F and L/F a cubic extension.

Definition 2.1 ([5, Definition 0.1])

- If $p \neq 3$, a generator y of a cubic extension L/F with minimal polynomial of the form $X^3 - a$ $(a \in F)$ is called a purely cubic generator, and L/F is called a purely cubic extension. If $p = 3$, such an extension is simply called purely inseparable.
- If $p \neq 3$ and a cubic extension L/F does not possess a generator with minimal polynomial of this form, then L/F is called impurely cubic.
- For any cubic extension L/F, we define the purely cubic closure of L/F to be the unique smallest extension F' of F such that LF'/F' is purely cubic. In [5, Theorem 2.1], we prove that the purely cubic closure exists and is unique.

Recall that by [5, Corollary 1.2], if $p \neq 3$, then every impurely cubic extension L/K has a primitive element y with minimal polynomial of the form

$$f(X) = X^3 - 3X - a.$$

We mention this here, as we will use it whenever this case occurs in §3. Throughout the paper, the element y will denote any such choice of primitive element.

3 Constant extensions

In this subsection, we wish to determine when a cubic function field over K is a constant extension of K. We do this before a study of ramification simply because constant extensions are unramified and their splitting behaviour is well understood [13, Chap. 6]. This will also help with identifying the non-constant extensions, as we will see later. In the subsequent sections, we will thus assume that our cubic extension L/K is not constant, which, as 3 is prime, is equivalent to assuming that the extension is geometric (see [13, Definition 5.2.29.]).

3.1 $X^3 - a, a \in K$, when $p \neq 3$

Lemma 3.1 *Let $p \neq 3$, and let L/K be purely cubic, i.e. there exists a primitive element $y \in L$ such that $y^3 = a$, $a \in K$. Then L/K is constant if, and only if, $a = ub^3$, where $b \in K$ and $u \in k^*$ is a non-cube. In other words, there is a purely cubic generator z of L/K such that $z^3 = u$, where $u \in k^*$.*

Proof Suppose that $a = ub^3$, where $b \in K$ and u is a non-cube in k^*. Then $z = \frac{y}{b} \in L$ is a generator of L/K such that $z^3 = u$. The polynomial $X^3 - u$ has coefficients in k, and as a consequence, L/K is constant.

Suppose then that L/K is constant. We denote by l a fixed algebraic closure of k in L, so that $L = Kl$. Let $l = k(\lambda)$, where λ satisfies a cubic polynomial $X^3 + eX^2 + fX + g$ with $e, f, g \in k$. Hence, $L = K(\lambda)$. We denote

$$\alpha = -2 - \frac{(27g^2 - 9efg + 2f^3)^2}{27(3ge - f^2)^3} \in k.$$

As L/F is purely cubic, it then follows by [5, Corollary 1.2 and Theorem 2.1] that either $3eg = f^2$ or the quadratic polynomial $X^2 + \alpha X + 1$ has a root in K. In both cases, there is a generator $\lambda' \in L$ such that

$$\lambda'^3 = \beta \in k.$$

Hence $\lambda' \in l$. The elements λ' and y are two purely cubic generators of L/K, whence by [5, Theorem 3.1], it follows that $y = c\lambda'^j$ where $j = 1$, or 2 and $c \in K$. Thus, $a = c^3\beta^j$, where $\beta \in k$. The result follows. □

3.2 $X^3 - 3X - a, a \in K$, when $p \neq 3$

Via [5, Corollary 1.2 and Theorem 3.3], a proof similar to that of Lemma 3.1 yields the following result.

Lemma 3.2 *Let $p \neq 3$ and L/K be an impurely cubic extension, so that there is a primitive element $y \in L$ such that $y^3 - 3y = a$ (see* [5, Corollary 1.2]*). Then L/K is constant if, and only if,*

$$u = -3a\alpha^2\beta + a\beta^3 + 6\alpha + \alpha^3 a^2 - 8\alpha^3 \in k^*,$$

for some $\alpha, \beta \in K$ such that $\alpha^2 + a_2\alpha\beta + \beta^2 = 1$. In other words, there is a generator z of L/K such that $z^3 - 3z = u$, where $u \in k^*$.

3.3 $X^3 + aX + a^2, a \in K$, when $p = 3$

In this case, one may prove the following result, similarly to the proof of Lemma 3.1, via [5, Corollary 1.2 and Theorem 3.6].

Lemma 3.3 *Let $p = 3$ and L/K be a separable cubic extension, so that there is a primitive element $y \in L$ such that $y^3 + ay + a^2 = 0$ (see* [5, Corollary 1.2]*). Then L/K is constant if, and only if,*

$$u = \frac{(ja^2 + (w^3 + aw))^2}{a^3} \in k^*,$$

for some $w \in K$ and $j = 1, 2$. In other words, there is a generator z of L/K such that $z^3 + uz + u^2 = 0$, where $u \in k^*$.

4 Ramification

In this section, we describe the ramification of any place of K in a cubic extension L/K. We divide the analysis into the three fundamental cubic forms derived in [5, Corollary 1.2].

4.1 $X^3 - a, a \in K$, when $p \neq 3$

We are aware that the purely cubic case might be well-know. Unable to find specific references but also for completeness, we chose to include the proofs in that case too.

If the extension L/K is purely cubic, one may find a purely cubic generator of a form which is well-suited to the determination of ramification, as in the following lemma.

Lemma 4.1 *Let L/K be a purely cubic extension. Given a place $\mathfrak{p}$ of K, one may select a primitive element y with minimal polynomial of the form $X^3 - a$ such that either*

(1) $v_{\mathfrak{p}}(a) = 1, 2$, *or*
(2) $v_{\mathfrak{p}}(a) = 0$.

Such a generator y is said to be in local standard form *at $\mathfrak{p}$.*

Proof Let y be a generator of L such that $y^3 = a \in K$. Given a place $\mathfrak{p}$ of K, we write $v_{\mathfrak{p}}(a) = 3j + r$ with $r = 0, 1, 2$. Via weak approximation, one may find an element $c \in K$ such that $v_{\mathfrak{p}}(c) = j$. Then $\frac{y}{c}$ is a generator of L such that $\left(\frac{y}{c}\right)^3 = \frac{y^3}{c^3} = \frac{a}{c^3}$ and $v_{\mathfrak{p}}\left(\frac{a}{c^3}\right) = r$. Hence we obtain the result. □

When a purely cubic extension L/K is separable, one may also easily determine the fully ramified places in L/K.

Theorem 4.2 *Let $p \neq 3$, and let L/K be a purely cubic extension. Given a purely cubic generator y with the minimal polynomial $X^3 - a$, a place $\mathfrak{p}$ of K is ramified if and only if it is fully ramified if, and only if, $(v_{\mathfrak{p}}(a), 3) = 1$.*

Proof Let $\mathfrak{p}$ be a place of K and $\mathfrak{P}$ be a place of L above $\mathfrak{p}$. Suppose that $(v_{\mathfrak{p}}(a), 3) = 1$. Then $3v_{\mathfrak{P}}(y) = v_{\mathfrak{P}}(y^3) = v_{\mathfrak{P}}(a) = e(\mathfrak{P}|\mathfrak{p})v_{\mathfrak{p}}(a)$. Since $(v_{\mathfrak{p}}(a), 3) = 1$, we obtain $3|e(\mathfrak{P}|\mathfrak{p})$, and as $e(\mathfrak{P}|\mathfrak{p}) \leq 3$, it follows that $e(\mathfrak{P}|\mathfrak{p}) = 3$, so that $\mathfrak{p}$ is fully ramified in L.

Conversely, suppose that $(v_{\mathfrak{p}}(a), 3) \neq 1$. By Lemma 4.1, we know that there exists a generator z of L such that $z^3 - c = 0$ and $v_{\mathfrak{p}}(c) = 0$. A study of all the possible factorisation of $X^3 - a$ mod $\mathfrak{p}$ together with Kummer's theorem [11, Theorem 3.3.7] shows that $\mathfrak{p}$ is either inert or there exists 2 or 3 places above it in L. Thus, $\mathfrak{p}$ cannot be fully ramified in any case. Moreover, there are no partially ramified places. Indeed, if L/K is Galois, then this is clear, and if L/K is not Galois, its Galois closure of L/K is $L(\xi)$ with $K(\xi)/K$ constant, hence unramified, and since the index of ramification is multiplicative in towers, the only possible index of ramification in $L(\xi)/K$ is 3, and so is the only possible index of ramification in L/K. □

4.2 $X^3 - 3X - a, a \in K, p \neq 3$

In order to determine the fully ramified places in extensions of this type, we begin with an elementary but useful lemma. These criteria and notation will be employed throughout what follows.

Lemma 4.3 *We consider the polynomial $X^2 + aX + 1$ where $a \in K$. We suppose this polynomial is irreducible over K. Let c_-, c_+ denote the roots of this polynomial in $\overline{K}$. We denote $K(c)$ the quadratic extension $K(c_\pm)$ of K. Let $\mathfrak{p}$ be a place of K and $\mathfrak{p}_c$ be a place of $K(c)$ above $\mathfrak{p}$. We have:*

(1) *For any place $\mathfrak{p}_c$ of $K(c)$,*

$$v_{\mathfrak{p}_c}(c_\pm) = -v_{\mathfrak{p}_c}(c_\mp).$$

(2) *For any place* $\mathfrak{p}_c$ *of* $K(c)$ *above a place* $\mathfrak{p}$ *of* K *such that* $v_\mathfrak{p}(a) < 0$,

$$v_\mathfrak{p}(a) = -|v_{\mathfrak{p}_c}(c_\pm)|,$$

and otherwise, $v_{\mathfrak{p}_c}(c_\pm) = 0$.

Proof (1) At any place $\mathfrak{p}_c$ of $K(c)$, we have

$$v_{\mathfrak{p}_c}(c_+ \cdot c_-) = v_{\mathfrak{p}_c}(c_+) + v_{\mathfrak{p}_c}(c_-) = v_{\mathfrak{p}_c}(1) = 0,$$

whence

$$v_{\mathfrak{p}_c}(c_+) = -v_{\mathfrak{p}_c}(c_-).$$

(2) As $c_\pm^2 + ac_\pm + 1 = 0$, the elements $c'_\pm = \frac{c_\pm}{a}$ satisfy

$$c'^2_\pm + c'_\pm + \frac{1}{a^2} = 0.$$

Thus, for any place $\mathfrak{p}_c$ of $K(c)$ above a place $\mathfrak{p}$ of K such that $v_\mathfrak{p}(a) < 0$, we obtain

$$v_{\mathfrak{p}_c}(c'^2_\pm + c'_\pm) = -2v_{\mathfrak{p}_c}(a) > 0.$$

By the non-Archimedean triangle inequality, this is possible if, and only if, $v_{\mathfrak{p}_c}(c'_\pm) > 0$ or $v_{\mathfrak{p}_c}(c'_\pm) = 0$. If $v_{\mathfrak{p}_c}(c'_\pm) > 0$, then

$$v_{\mathfrak{p}_c}(c'_\pm) = -2v_{\mathfrak{p}_c}(a) \quad \text{and} \quad v_{\mathfrak{p}_c}(c_\pm) = -v_{\mathfrak{p}_c}(a).$$

If on the other hand $v_{\mathfrak{p}_c}(c'_\pm) = 0$, we obtain

$$v_{\mathfrak{p}_c}(c_\pm) = v_{\mathfrak{p}_c}(a).$$

Thus, the latter together with part (1) of this lemma implies that either

$$v_{\mathfrak{p}_c}(c_+) = v_{\mathfrak{p}_c}(a) \quad \text{and} \quad v_{\mathfrak{p}_c}(c_-) = -v_{\mathfrak{p}_c}(a)$$

or vice versa (with the roles of c_- and c_+ interchanged). Moreover, note that $\mathfrak{p}_c$ is unramified in $K(c)/K$ so that $v_{\mathfrak{p}_c}(a) = v_\mathfrak{p}(a)$. For if, when $p \neq 2$, then $K(c)/K$ has a generator w such that $w^2 = -27(a^2 - 4)$ and $2|v_\mathfrak{p}(-27(a^2 - 4))$, thus by Kummer theory, $\mathfrak{p}$ is unramified and when $p = 2$, $K(c)/K$ has a generator w such that $w^2 - w = \frac{1}{a^2}$ and $v_\mathfrak{p}(\frac{1}{a^2}) \geq 0$, thus by Artin-Schreier theory, we have that $\mathfrak{p}$ is unramified in $K(c)$, thus the first part of (2). For any place $\mathfrak{p}_c$ of $K(b)$ above a place $\mathfrak{p}$ of K such that $v_\mathfrak{p}(a) > 0$. As

$$v_{\mathfrak{p}_c}(c'^2_\pm + c'_\pm) = -2v_{\mathfrak{p}_c}(a) < 0,$$

again using the non-Archimedean triangle inequality, we can only have $v_{\mathfrak{p}_c}(c'^2_{\pm}) < 0$, whence $v_{\mathfrak{p}_c}(c'^2_{\pm}) = -2v_{\mathfrak{p}_c}(a)$. This implies that $v_{\mathfrak{p}_c}(c_{\pm}) = 0$. Finally, via the triangle inequality once more, for any $\mathfrak{p}_c$ such that $v_{\mathfrak{p}_c}(a) = 0$, we must have $v_{\mathfrak{p}_c}(c_{\pm}) = 0$.

□

Theorem 4.4 *Let $p \neq 3$. Let L/K be an impurely cubic extension. Le y be a primitive element with minimal polynomial $f(X) = X^3 - 3X - a$. Then*

(1) *the fully ramified places of K in L are precisely those $\mathfrak{p}$ such that $(v_{\mathfrak{p}}(a), 3) = 1$ and*
(2) *the partially ramified places $\mathfrak{p}$ that is the one with index of ramification 2 are precisely those such that $a \equiv \pm 2 \mod \mathfrak{p}$ and*

  (a) $(v_{\mathfrak{p}}(a^2 - 4), 2) = 1$, *when $p \neq 2$;*
  (b) *there exists $w \in K$ such that $v_{\mathfrak{p}}(1/a + 1 + w^2 - w) < 0$ and $(v_{\mathfrak{p}}(1/a + 1 + w^2 - w), 2) = 1$, when $p = 2$.*

Proof (1) As usual, we let ξ be a primitive 3^{rd} root of unity. We also let r be a root of the quadratic resolvent $R(X) = X^2 + 3aX + (-27 + 9a^2)$ of the cubic polynomial $X^3 - 3X - a$ in $\overline{K}$. As in [1, Theorem 2.3], we know that $L(r)/K(r)$ is Galois, and by [5, Corollary 1.6], we have that $L(\xi, r)/K(\xi, r)$ is purely cubic. We denote by $\mathfrak{p}$ a place in K, $\mathfrak{P}_{\xi,r}$ a place of $L(\xi, r)$ above $\mathfrak{p}$, $\mathfrak{P} = \mathfrak{P}_{\xi,r} \cap L$, and $\mathfrak{p}_{\xi,r} = \mathfrak{P}_{\xi,r} \cap K(\xi, r)$. By [5, Theorem 1.5], we know that that $L(\xi, r)/K(\xi, r)$ is Kummer; more precisely, there exists $v \in K(\xi, r)$ such that $v^3 = c$ where c is a root of the polynomial $X^2 + aX + 1$. We thus obtain a tower $L(\xi, r)/K(\xi, r)/K(\xi)/K$ with $L(\xi, r)/K(\xi, r)$ Kummer of degree 3, and where $K(\xi, r)/K(\xi)$ and $K(\xi)/K$ are both Kummer extensions of degree 2. As the index of ramification is multiplicative in towers and the degree of $L(\xi, r)/K(\xi, r)$ and $K(\xi, r)/K$ are coprime, the places of K that fully ramify in L are those places of K which lie below those of $K(\xi, r)$ which fully ramify in $L(\xi, r)/K(\xi, r)$. As $L(\xi, r)/K(\xi, r)$ is Kummer, the places of $K(\xi, r)$ that ramify in $L(\xi, r)$ are described precisely by Kummer theory (see for example [13, Example 5.8.9]) as those $\mathfrak{p}_{\xi,r}$ in $K(\xi, r)$ such that

$$(v_{\mathfrak{p}_{\xi,r}}(c_{\pm}), 3) = 1.$$

Lemma 4.3 states that if $v_{\mathfrak{p}}(a) < 0$, then $v_{\mathfrak{p}_{\xi,r}}(c_{\pm}) = \pm v_{\mathfrak{p}_{\xi,r}}(a)$ and that otherwise, $v_{\mathfrak{p}_{\xi,r}}(c_{\pm}) = 0$. Thus, the ramified places of L/F are those places $\mathfrak{p}$ below a place $\mathfrak{p}_{\xi,r}$ of $K(\xi, r)$ such that $(v_{\mathfrak{p}_{\xi,r}}(a), 3) = 1$. Also,

$$v_{\mathfrak{p}_{\xi,r}}(a) = e(\mathfrak{p}_{\xi,r}|\mathfrak{p})v_{\mathfrak{p}}(a),$$

where $e(\mathfrak{p}_{\xi,r}|\mathfrak{p})$ is the ramification index of a place $\mathfrak{p}$ of K in $K(\xi, r)$, equal to 1, 2, or 4, and in any case, coprime with 3. Thus, $(v_{\mathfrak{p}_{\xi,r}}(a), 3) = 1$ if, and only if, $(v_{\mathfrak{p}}(a), 3) = 1$. As a consequence of the above argument, it therefore follows that a place $\mathfrak{p}$ of K is fully ramified in L if, and only if, $v_{\mathfrak{p}}(a) < 0$. If L/K is Galois then all the places are fully ramified.

(2) If L/K is not Galois and a ramified place $\mathfrak{p}$ is not fully ramified in L/K, its index of ramification is 2. The Galois closure of L/K is $L(r)/K$. Since $L(r)/K(r)$ is Galois, all the ramified places in $L(r)/K(r)$ are fully ramified and the only possible way that the index of ramification of a place is 2 in L/K is that this place is ramified in $K(r)/K$,

since the index of ramification is multiplicative in tower. By Kummer and Artin-Schreier theory, this implies that $v_{\mathfrak{p}}(a) \geq 0$ when $p \neq 2$ and $v_{\mathfrak{p}}(a) > 0$ when $p = 2$, since $K(r)/K$ is defined by a minimal equation $X^2 = -27(a^2 - 4)$ when $p \neq 2$ and $X^2 - X = 1 + 1/a$ when $p = 2$.
When $v_{\mathfrak{p}}(a) \geq 0$, via Kummer's theorem, for $\mathfrak{p}$ to be partially ramified in L/K, the only possible decomposition of $X^3 - 3X - a$ mod $\mathfrak{p}$ is

$$X^3 - 3X - a = (X - \alpha)^2(X - \beta) \mod \mathfrak{p}$$

with $\alpha \neq \beta$.
The equality $f(X) = (X - \alpha)(X - \beta)^2$ gives us

$$X^3 - 3X - a = (X - \alpha)(X - \beta)^2 = X^3 - (2\beta + \alpha)X^2 + (\beta^2 + 2\alpha\beta)X - \alpha\beta^2.$$

Thus $\alpha = -2\beta$. We therefore have $-3 = \beta^2 - 4\beta^2 = -3\beta^2$ and $a = -2\beta^3$. The first of these implies that

$$3(\beta^2 - 1) = 3\beta^2 - 3 = 0.$$

Thus $\beta = \pm 1$ and $a = \mp 2$. Conversely, when $a = \mp 2 \mod \mathfrak{p}.$, then

$$X^3 - 3X \mp 2 = (X \pm 2)(X \mp 1)^2.$$

Therefore, in order for $\mathfrak{p}$ to be partially ramified we need that $\mathfrak{p}$ ramified in $K(r)$ that is

(a) $(v_{\mathfrak{p}}(a^2 - 4), 2) = 1$, when $p \neq 2$;
(b) there exists $w \in K$ such that $v_{\mathfrak{p}}(1/a + 1 + w^2 - w) < 0$ and $(v_{\mathfrak{p}}(1/a + 1 + w^2 - w), 2) = 1$, when $p = 2$.

Conversely, suppose that $\mathfrak{p}$ is a place such that $a \equiv \mp 2 \mod \mathfrak{p}$ and $\mathfrak{p}$ ramified in $K(r)$. Since $\mathfrak{p}$ cannot be ramified in $K(r)$ without $v_{\mathfrak{p}}(a) \geq 0$ and $L(r)/K$ is Galois, then when $a \equiv \mp 2 \mod \mathfrak{p}$ and $\mathfrak{p}$ ramified in $K(r)$, then the place above $\mathfrak{p}$ in $K(r)$ is unramified in $L(r)/K(r)$ (see proof of (1)) therefore completely split and we must have

$$\mathfrak{p}\mathcal{O}_{L(r),x} = (\mathfrak{P}_{1,r}\mathfrak{P}_{2,r}\mathfrak{P}_{3,r})^2$$

Since $a \equiv \mp 2 \mod \mathfrak{p}$, we have $X^3 - 3X - a = (X - \alpha)(X - \beta)^2 \mod \mathfrak{p}$ with $\alpha, \beta \in k(\mathfrak{p})$ and $\alpha \neq \beta$, by Kummer's theorem, we know that there is at least two place above $\mathfrak{p}$ in L thus either

(a) $\mathfrak{p}\mathcal{O}_{L,x} = \mathfrak{P}_1\mathfrak{P}_2$ where $\mathfrak{P}_i$, $i = 1, 2$ place of L above $\mathfrak{p}$, or
(b) $\mathfrak{p}\mathcal{O}_{L,x} = \mathfrak{P}_1^2\mathfrak{P}_2$ where $\mathfrak{P}_i$, $i = 1, 2$ place of L above $\mathfrak{p}$, or
(c) $\mathfrak{p}\mathcal{O}_{L,x} = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$ where $\mathfrak{P}_i$, $i = 1, 2, 3$ place of L above $\mathfrak{p}$.

By [7, p. 55], we know that $\mathfrak{p}$ is completely split in L (case (c)) if, and only if, (1) $\mathfrak{p}$ is completely split in $K(r)$ and (2) $\mathfrak{p}_r$ completely split in $L(r)$. Thus, either $\mathfrak{p}\mathcal{O}_{L,x} = \mathfrak{P}_1\mathfrak{P}_2$ or $\mathfrak{p}\mathcal{O}_{L,x} = \mathfrak{P}_1^2\mathfrak{P}_2$ where each $\mathfrak{P}_i$ $(i = 1, 2)$ is a place of L above $\mathfrak{p}$. Note that $2 \mid e(\mathfrak{P}_r|\mathfrak{p})$ for any places $\mathfrak{P}_r$ in $L(r)$ above $\mathfrak{p}$. If $\mathfrak{p}\mathcal{O}_{L,x} = \mathfrak{P}_1\mathfrak{P}_2$, then as $e(\mathfrak{P}_i|\mathfrak{p}) = 1$, we have that $2 \mid e(\mathfrak{P}_{i,r}|\mathfrak{P}_i)$ and $\mathfrak{p}\mathcal{O}_{L(r),x} = \mathfrak{P}_{1,r}^2\mathfrak{P}_{2,r}^2$, where $\mathfrak{P}_{i,r}$, $i = 1, 2$ are places above $\mathfrak{p}$ in $L(r)$, which is impossible, as $\mathfrak{p}\mathcal{O}_{L(r),x} = (\mathfrak{P}_{1,r}\mathfrak{P}_{2,r}\mathfrak{P}_{3,r})^2$. Thus, in this case, we must have $\mathfrak{p}\mathcal{O}_{L,x} = \mathfrak{P}_1^2\mathfrak{P}_2$ and $\mathfrak{P}_1$ is split in $K(r)$ and $\mathfrak{P}_2$ ramifies in $K(r)$. □

This theorem yields the following corollaries, the first being immediate.

Corollary 4.5 *When K does not contain a third root of unity. Let L/K be a Galois cubic extension, so that there exists a primitive element y of L with minimal polynomial $f(X) = X^3 - 3X - a$. Then the (fully) ramified places of K in L are precisely those places $\mathfrak{p}$ of K such that $v_{\mathfrak{p}}(a) < 0$ and $(v_{\mathfrak{p}}(a), 3) = 1$.*

Corollary 4.6 *When K does not contain a third root of unity. Let L/K be a Galois cubic extension, so that there exists a primitive element y of L with minimal polynomial $f(X) = X^3 - 3X - a$. Then, only those places of K of even degree can (fully) ramify in L. More precisely, any place $\mathfrak{p}$ of K such that $v_{\mathfrak{p}}(a) < 0$ is of even degree.*

Proof In Lemma 4.3, it was noted that $\sigma(c_\pm) = c_\mp$ where $Gal(K(c_\pm)/K) = \{Id, \sigma\}$, when $c_\pm \notin K$. Let ξ again be a primitive 3^{rd} root of unity. We denote by $\mathfrak{p}$ a place of K and $\mathfrak{p}_\xi$ a place of $K(\xi)$ above $\mathfrak{p}$. We find that

$$v_{\mathfrak{p}_\xi}(c_\pm) = v_{\sigma(\mathfrak{p}_\xi)}(\sigma(c_\pm)) = v_{\sigma(\mathfrak{p}_\xi)}(c_\mp).$$

Note that if $\sigma(\mathfrak{p}_\xi) = \mathfrak{p}_\xi$, it follows that $v_{\mathfrak{p}_\xi}(c_\pm) = v_{\mathfrak{p}_\xi}(c_\mp)$. However, by Lemma 4.3, we have that, for any place $\mathfrak{p}_\xi$ of $K(\xi)$ above a place $\mathfrak{p}$ of K such that $v_{\mathfrak{p}}(a) < 0$, it holds that $v_{\mathfrak{p}_\xi}(c_\pm) = \pm v_{\mathfrak{p}_\xi}(a)$, and that $v_{\mathfrak{p}_\xi}(c_\pm) = -v_{\mathfrak{p}_\xi}(c_\mp)$. Thus, for any place $\mathfrak{p}_\xi$ of $K(\xi)$ above a place $\mathfrak{p}$ of K such that $v_{\mathfrak{p}}(a) < 0$, we find that $v_{\mathfrak{p}_\xi}(c_\pm) \neq v_{\mathfrak{p}_\xi}(c_\mp)$ and thus $\sigma(\mathfrak{p}_\xi) \neq \mathfrak{p}_\xi$.

Therefore, by [13, Theorem 6.2.1], we obtain that $\mathfrak{p}$ is of even degree, for any place $\mathfrak{p}$ of K such that $v_{\mathfrak{p}}(a) < 0$. □

Corollary 4.7 *Suppose that the constant field of K is $\mathbb{F}_q$ with $q \equiv -1 \mod 3$. Let L/K be a Galois cubic extension, so that there exists a primitive element y of L with minimal polynomial $f(X) = X^3 - 3X - a$. Then one can choose a single place $\mathfrak{P}_\infty$ at infinity in K such that $v_{\mathfrak{P}_\infty}(a) \geq 0$.*

Proof One can choose $x \in K\backslash k$ such that the place $\mathfrak{p}_\infty$ at infinity for x has the property that all of the places in K above it are of odd degree. In order to accomplish this, we appeal to a method similar to the proof of [13, Proposition 7.2.6]; because there exists a divisor of degree 1 [13, Theorem 6.3.8], there exists a prime divisor $\mathfrak{P}_\infty$ of K of odd degree; for if all prime divisors of K were of even degree, then the image of the degree function of K would lie in $2\mathbb{Z}$, which contradicts [13, Theorem 6.3.8]. Let d be this degree. Let $m \in \mathbb{N}$ be such that $m > 2g_K - 1$. Then, by the Riemann–Roch theorem [13, Corollary 3.5.8], it follows that there exists $x \in K$ such that the pole divisor of x in K is equal to $\mathfrak{P}_\infty^m$. By definition, the pole divisor of x in $k(x)$ is equal to $\mathfrak{p}_\infty$. It follows that

$$(\mathfrak{p}_\infty)_K = \mathfrak{P}_\infty^m,$$

from which it follows that $\mathfrak{P}_\infty$ is the unique place of K above $\mathfrak{p}_\infty$, and by supposition that $\mathfrak{P}_\infty$ is of odd degree. From this argument, we obtain that, with this choice of infinity, all places above infinity in $k(x)$ are of odd degree. (We also note that we may very well choose m relatively prime to p, whence $K/k(x)$ is also separable; in general, $K/k(x)$ as chosen will not be Galois.)

As $q \equiv -1 \mod 3$, L/K is a Galois extension, and y is a primitive element with minimal polynomial of the form $X^3 - 3X - a$ where $a \in K$, we know that all of the places $\mathfrak{p}$ of K such that $v_{\mathfrak{p}}(a) < 0$, and in particular, all the ramified places, are of even degree (see Corollary 4.6). It follows that the process described in this proof gives the desired construction, and the result follows. □

Remark 4.8 We note that when K is a rational function field, one may use Corollary 4.7 to show that the parameter a has nonnegative valuation at $\mathfrak{p}_\infty$ for a choice of x such that $K = k(x)$, and thus such $\mathfrak{p}_\infty$ is unramified.

4.3 $X^3 + aX + a^2, a \in K, p = 3$

As for purely cubic extensions, there exists a local standard form which is useful for a study of splitting structure and ramification.

Lemma 4.9 *Let $p = 3$, and let L/K be a cubic separable extension. Let $\mathfrak{p}$ be a place of K. Then there is a generator y such that $y^3 + ay + a^2 = 0$ such that $v_\mathfrak{p}(a) \geq 0$, or $v_\mathfrak{p}(a) < 0$ and $(v_\mathfrak{p}(a), 3) = 1$. Such a y is said to be* in local standard form *at $\mathfrak{p}$.*

Proof Let $\mathfrak{p}$ be a place of K. Let y_1 be a generator of L/K such that $y_1^3 + a_1y_1 + a_1^2 = 0$ (this was shown to exist in [3]). By [5, Theorem 3.6], any other generator y_2 with a minimal equation of the same form $y_2^3 + a_2y_2 + a_2^2 = 0$ is such that $y_2 = -\beta(\frac{j}{a_1}y_1 - \frac{1}{a_1}w)$, and we have

$$a_2 = \frac{(ja_1^2 + (w^3 + a_1w))^2}{a_1^3}.$$

Suppose that $v_\mathfrak{p}(a_1) < 0$, and that $3 \mid v_\mathfrak{p}(a_1)$. Using the weak approximation theorem, we choose $\alpha \in K$ such that $v_\mathfrak{p}(\alpha) = 2v_\mathfrak{p}(a_1)/3$, which exists as $3 \mid v_\mathfrak{p}(a_1)$. Then

$$v_\mathfrak{p}(\alpha^{-3}ja_1^2) = 0.$$

Let $w_0 \in K$ be chosen so that $w_0 \neq -\alpha^{-3}ja_1^2$ and

$$v_\mathfrak{p}(\alpha^{-3}ja_1^2 + w_0) > 0.$$

This may be done via the following simple argument: As $v_\mathfrak{p}(\alpha^{-3}ja_1^2) = 0$, then $\overline{\alpha^{-3}ja_1^2} \neq 0$ in $k(\mathfrak{p})$.

We then choose $\underline{\text{some } w_0 \neq}$ $-\alpha^{-3}ja_1^2 \in K$ such that $\overline{w_0} = -\overline{\alpha^{-3}ja_1^2}$ in $k(\mathfrak{p})$. Note that $v_\mathfrak{p}(w_0) = 0$. Thus, $\alpha^{-3}ja_1^2 + w_0 = 0$ in $k(\mathfrak{p})$ and $v_\mathfrak{p}(\alpha^{-3}ja_1^2 + w_0) > 0$. As $p = 3$, it follows that the map $X \to X^3$ is an isomorphism of $k(\mathfrak{p})$, so we may find an element $w_1 \in K$ such that $w_1^3 = w_0 \mod \mathfrak{p}$. Hence

$$v_\mathfrak{p}(\alpha^{-3}ja_1^2 + w_1^3) > 0.$$

We then let $w_2 = \alpha w_1$, so that

$$v_\mathfrak{p}(ja_1^2 + w_2^3) = v_\mathfrak{p}(ja_1^2 + \alpha^3w_1^3) > v_\mathfrak{p}(ja_1^2).$$

Thus, as $v_\mathfrak{p}(a_1) < 0$, we obtain

$$\begin{aligned} v_\mathfrak{p}(ja_1^2 + (w_2^3 + a_1w_2)) &\geq \min\{v_\mathfrak{p}(ja_1^2 + w_2^3), v_\mathfrak{p}(a_1w_2)\} \\ &> \min\{v_\mathfrak{p}(ja_1^2), v_\mathfrak{p}(a_1w_2)\} \\ &= \min\{v_\mathfrak{p}(ja_1^2), v_\mathfrak{p}(a_1) + 2v_\mathfrak{p}(a_1)/3\} \\ &= \min\{2v_\mathfrak{p}(a_1), 5v_\mathfrak{p}(a_1)/3\} \\ &= 2v_\mathfrak{p}(a_1). \end{aligned}$$

Hence

$$\nu_{\mathfrak{p}}(a_2) = \nu_{\mathfrak{p}}\left(\frac{(ja_1^2 + (w^3 + a_1 w))^2}{a_1^3}\right) > 4\nu_{\mathfrak{p}}(a_1) - \nu_{\mathfrak{p}}(a_1^3) = \nu_{\mathfrak{p}}(a_1).$$

We can thus ensure (after possibly repeating this process if needed) that we terminate at an element $a_2 \in K$ for which $\nu_{\mathfrak{p}}(a_2) \geq 0$ or for which $\nu_{\mathfrak{p}}(a_2) < 0$ and $(\nu_{\mathfrak{p}}(a_2), 3) = 1$. □

Remark 4.10 Note that we can do what we have done in the previous Lemma simultaneously at any finite place (see [6, Lemma 1.2]).

Theorem 4.11 *Suppose that $p = 3$. Let L/K be a separable cubic extension. Let y be a primitive element with minimal polynomial $X^3 + aX + a^2$. Let $\mathfrak{p}$ be a place of K and $\mathfrak{P}$ a place of L above $\mathfrak{p}$. Then*

(1) *$\mathfrak{p}$ is fully ramified if, and only if, there is $w \in K$, $\nu_{\mathfrak{p}}(\alpha) < 0$ and $(\nu_{\mathfrak{p}}(\alpha), 3) = 1$ with*

$$\alpha = \frac{(ja^2 + (w^3 + aw))^2}{a^3}.$$

Equivalently, there is a generator z of L whose minimal polynomial is of the form $X^3 + \alpha X + \alpha^2$, where $\nu_{\mathfrak{p}}(\alpha) < 0$ and $(\nu_{\mathfrak{p}}(\alpha), 3) = 1$, and

(2) *$\mathfrak{p}$ is partially ramified if and only if $(\nu_{\mathfrak{p}}(a), 2) = 1$ and there is $w \in K$ such that $\nu_{\mathfrak{p}}(\alpha) \geq 0$ with*

$$\alpha = \frac{(ja^2 + (w^3 + aw))^2}{a^3}.$$

The later is equivalent to the existence of a generator z of L whose minimal polynomial is of the form $X^3 + \alpha X + \alpha^2$, where $\nu_{\mathfrak{p}}(\alpha) \geq 0$.

Proof (1) Let $\mathfrak{p}$ be a place of K, and denote by $\mathfrak{P}$ a place of L above $\mathfrak{p}$. When L/F is Galois, this theorem is simply the usual Artin-Schreier theory (see [11, Proposition 3.7.8]). Otherwise, since the discriminant of the polynomial $X^3 + aX + a^2$ is equal to $\Delta = -4a^3 = -a^3$, by [1, Theorem 2.3], we know that the Galois closure of L/F is equal to $L(\Delta) = L(b)$, where $b^2 = -a$. Let $\mathfrak{p}_b$ a place of $K(b)$ above $\mathfrak{p}$. The extension $L(b)/K(b)$ is an Artin-Schreier extension with Artin-Schreier generator y/b possessing minimal polynomial $X^3 - X + b$. As $L(b)/K(b)$ is Galois, if $\mathfrak{p}_b$ is ramified in $L(b)$, then it must be fully ramified. Furthermore, as the degree $K(b)/K$ is equal to 2, which is coprime with 3, and the index of ramification is multiplicative in towers, it follows that the place $\mathfrak{p}$ is fully ramified in L if, and only if, $\mathfrak{p}_b$ is fully ramified in $L(b)$. By [11, Proposition 3.7.8],

(a) $\mathfrak{p}_b$ is fully ramified in $L(b)$ if, and only if, there is an Artin-Schreier generator z such that $z^3 - z - c$ with $\nu_{\mathfrak{p}_b}(c) < 0$ and $(\nu_{\mathfrak{p}_b}(c), 3) = 1$, and

(b) $\mathfrak{p}_b$ is unramified in $L(b)$ if, and only if, there is an Artin-Schreier generator z such that $z^3 - z - c$ with $\nu_{\mathfrak{p}_b}(c) \geq 0$.

Suppose that there is a generator w such that $w^3 + a_1 w + a_1^2 = 0$, $\nu_{\mathfrak{p}}(a_1) < 0$ and $(\nu_{\mathfrak{p}}(a_1), 3) = 1$. Then over $K(b_1)$, where $b_1^2 = -a_1$, we have an Artin-Schreier generator z of $L(b_1)$ such that $z^3 - z + b_1$. Moreover,

$$\nu_{\mathfrak{p}_{b_1}}(b_1) = \frac{\nu_{\mathfrak{p}_{b_1}}(a_1)}{2} = \frac{e(\mathfrak{p}_{b_1}|\mathfrak{p})\nu_{\mathfrak{p}}(a_1)}{2},$$

where $e(\mathfrak{p}_{b_1}|\mathfrak{p})$ is the index of ramification of $\mathfrak{p}_{b_1}$ over $K(b_1)$, whence $e(\mathfrak{p}_{b_1}|\mathfrak{p}) = 1$ or 2. As a consequence,

$$(v_{\mathfrak{p}_{b_1}}(b_1), 3) = (v_{\mathfrak{p}}(a_1), 3) = 1,$$

and $\mathfrak{p}_{b_1}$ is fully ramified in $L(b_1)$, so that $\mathfrak{p}$ too must be fully ramified in L.
Suppose that there exists a generator w such that $w^3 + a_1 w + a_1^2 = 0$, $v_{\mathfrak{p}}(a_1) \geq 0$. Then over $K(b_1)$, where $b_1^2 = -a_1$, we have a generator z of $L(b_1)$ such that $z^3 - z + b_1$ and

$$v_{\mathfrak{p}_{b_1}}(b_1) = \frac{e(\mathfrak{p}_{b_1}|\mathfrak{p})v_{\mathfrak{p}}(a_1)}{2} \geq 0.$$

Thus $\mathfrak{p}_b$ is unramified in $L(b)$, so that $\mathfrak{p}$ cannot be fully ramified in L, since the ramification index is multiplicative in towers. The theorem then follows by Lemma 4.9.
If L/K is Galois, then the ramified places are all fully ramified.

(2) If L/K is not Galois and a ramified place $\mathfrak{p}$ is not fully ramified in L/K its index of ramification is 2. Moreover, when $\mathfrak{p}$ is not fully ramified we know by (1) and Lemma 4.9 that there is $w \in K$ such that $v_{\mathfrak{p}}(\alpha) \geq 0$ with

$$\alpha = \frac{(ja^2 + (w^3 + aw))^2}{a^3}.$$

The Galois closure of L/K is $L(b)/K$ where $b^2 = -\alpha$ since $L(b)/K(b)$ is Galois then all the ramified places in $L(b)/K(b)$ are fully ramified and the only possible way that the index of ramification of a place is 2 in L/K is that this place is ramified in $K(b)/K$ since the index of ramification is multiplicative in tower. That is

$$(v_{\mathfrak{p}}(a), 2) = (v_{\mathfrak{p}}(\alpha), 2) = 1.$$

Since the Galois closure has also as generator c such that $c^2 = -a$. Therefore, $v_{\mathfrak{p}}(\alpha) > 0$ and $(v_{\mathfrak{p}}(a), 2) = 1$.
Conversely, suppose there is $w \in K$ such that $v_{\mathfrak{p}}(\alpha) > 0$ with

$$\alpha = \frac{(ja^2 + (w^3 + aw))^2}{a^3}$$

and $(v_{\mathfrak{p}}(a), 2) = 1$. If $v_{\mathfrak{p}}(\alpha) > 0$, then $L(b)/K(b)$ is an Artin-Schreier extension by [1, Theorem 2.3], and there is an Artin-Schreier generator $w = \frac{z}{b}$ such that $w^3 - w + b = 0$ and $v_{\mathfrak{p}_b}(b) > 0$, where $\mathfrak{p}_b$ is a place of $K(b)$ above $\mathfrak{p}$. Thus $b \equiv 0 \mod \mathfrak{p}_b$, and the polynomial

$$X^3 - X + b \equiv X^3 - X \mod \mathfrak{p}_b$$

factors as $X(X-1)(X+1)$ modulo $\mathfrak{p}_b$. By Kummer's theorem ([11, Theorem 3.3.7]), we then have that $\mathfrak{p}_b$ is completely split in $L(b)$.
As $\mathfrak{p}_b$ is completely split in $L(b)$, we have that $\mathfrak{p}$ cannot be inert in L. Indeed, if $\mathfrak{p}$ were inert in L, then there are at most two places above $\mathfrak{p}$ in $L(b)$, in contradiction with the proven fact that $\mathfrak{p}_b$ is completely split in $L(b)$.
By [7, p.55], $\mathfrak{p}$ splits completely in L if, and only if, $\mathfrak{p}$ is completely split in $K(b)$ and $\mathfrak{p}_b$ is completely split in $L(b)$.
Also, since by the previous argument $\mathfrak{p}$ cannot be inert in L, we have that either

$$\mathfrak{p}\mathcal{O}_{L,x} = \mathfrak{P}_1\mathfrak{P}_2 \qquad \text{or} \qquad \mathfrak{p}\mathcal{O}_{L,x} = \mathfrak{P}_1\mathfrak{P}_2^2,$$

where $\mathfrak{P}_i$, $i = 1, 2$ are places of L above $\mathfrak{p}$. Let $\mathfrak{P}_b$ be a place of $L(b)$ above $\mathfrak{p}$. When $\mathfrak{p}$ is ramified in $K(b)$, then the index of ramification at any place above $\mathfrak{p}$ in $L(b)$ is divisible by 2, since $L(b)/K$ is Galois by [1, Theorem 2.3], whence $\mathfrak{p}\mathcal{O}_{L,x} = \mathfrak{P}_1\mathfrak{P}_2^2$. □

5 Different exponents and Riemann–Hurwitz formulae

Using the extension data, it is possible to give the Riemann–Hurwitz theorem for each of our forms in [5, Corollary 1.2]. These depend only on information from a single parameter.

5.1 $X^3 - a, a \in K, p \neq 3$

Lemma 5.1 *Let $p \neq 3$. Let L/K be a purely cubic extension and y a primitive element of L with minimal polynomial $f(X) = X^3 - a$. Let $\mathfrak{p}$ be a place of K and $\mathfrak{P}$ a place of L over $\mathfrak{p}$. Then precisely one of the following is true:*

(1) *$d(\mathfrak{P}|\mathfrak{p}) = 0$ if, and only if, $e(\mathfrak{P}|\mathfrak{p}) = 1$.*
(2) *$d(\mathfrak{P}|\mathfrak{p}) = 2$, otherwise. That is, $e(\mathfrak{P}|\mathfrak{p}) = 3$, which by Theorem 4.2 is equivalent to $(v_{\mathfrak{p}}(a), 3) = 1$.*

Proof By Theorem 4.2, either $e(\mathfrak{P}|\mathfrak{p}) = 1$ or $e(\mathfrak{P}|\mathfrak{p}) = 3$.

(1) As the constant field k of K is perfect, all residue field extensions in L/K are automatically separable. The result then follows from [13, Theorem 5.6.3].
(2) If $e(\mathfrak{P}|\mathfrak{p}) = 3$, then as $p \nmid 3$, it follows again from [Theorem 5.6.3, Ibid.] that $d(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{p}) - 1 = 2$. □

We thus find the Riemann–Hurwitz formula as follows for purely cubic extensions when the characteristic is not equal to 3, which resembles that of Kummer extensions, but no assumption is made that the extension is Galois.

Theorem 5.2 (Riemann–Hurwitz I) *Let $p \neq 3$. Let L/K be a purely cubic geometric extension, and y a primitive element of L with minimal polynomial $f(X) = X^3 - a$. Then the genus g_L of L is given according to the formula*

$$g_L = 3g_K - 2 + \sum_{(v_{\mathfrak{p}}(a),3)=1} d_K(\mathfrak{p}).$$

Proof This follows from Lemma 5.3, [13, Theorem 9.4.2], and the fundamental identity $\sum e_if_i = [L : K] = 3$. □

5.2 $X^3 - 3X - a, a \in K, p \neq 3$

Lemma 5.3 *Let $p \neq 3$. Let L/K be an impurely cubic extension and y a primitive element of L with minimal polynomial $f(X) = X^3 - 3X - a$. Let $\mathfrak{p}$ be a place of K and $\mathfrak{P}$ a place of L over $\mathfrak{p}$. Let $\Delta = -27(a^2 - 4)$ be the discriminant of $f(X)$ and $r \in \overline{K}$ a root of the quadratic resolvent $R(X) = X^2 + 3aX + (-27 + 9a^2)$ of $f(X)$. Then precisely one of the following is true:*

(1) *$d(\mathfrak{P}|\mathfrak{p}) = 0$ if, and only if, $e(\mathfrak{P}|\mathfrak{p}) = 1$.*
(2) *If $e(\mathfrak{P}|\mathfrak{p}) = 3$, which by Theorem 4.4 is equivalent to $v_{\mathfrak{p}}(a) < 0$ and $(v_{\mathfrak{p}}(a), 3) = 1$, then $d(\mathfrak{P}|\mathfrak{p}) = 2$.*
(3) *If $e(\mathfrak{P}|\mathfrak{p}) = 2$,*

(a) *If* $p \neq 2$, *by Theorem* 4.4, *this occurs precisely when* Δ *is not a square in* K, $a \equiv \pm 2 \mod \mathfrak{p}$, $(v_{\mathfrak{p}}(\Delta), 2) = 1$. *In this case,* $2 \mid v_{\mathfrak{P}}(\Delta)$ *and* $d(\mathfrak{P}|\mathfrak{p}) = 1$.

(b) *If* $p = 2$, *by Theorem* 4.4, *this occurs when* $r \notin K$, $a \equiv 0 \mod \mathfrak{p}$, *there is* $w_{\mathfrak{p}} \in K$ *such that* $v_{\mathfrak{p}}(\left(\frac{1}{a^2} + 1 - w_{\mathfrak{p}}^2 + w_{\mathfrak{p}}\right), 2) = 1$ *and* $v_{\mathfrak{p}}\left(\frac{1}{a^2} + 1 - w_{\mathfrak{p}}^2 + w_{\mathfrak{p}}\right) < 0$. *Also, in this case, there exists* $\eta_{\mathfrak{P}} \in L$ *such that* $v_{\mathfrak{P}}\left(\frac{1}{a^2} + 1 - \eta_{\mathfrak{P}}^2 + \eta_{\mathfrak{P}}\right) \geq 0$, *and we have for this* $\mathfrak{P}$ *that*

$$d(\mathfrak{P}|\mathfrak{p}) = -v_{\mathfrak{p}}\left(\frac{1}{a^2} + 1 - w_{\mathfrak{p}}^2 + w_{\mathfrak{p}}\right) + 1.$$

Proof Let $\mathfrak{p}$ be a place of K, $\mathfrak{P}_r$ a place of $L(r)$ above $\mathfrak{p}$, $\mathfrak{P} = \mathfrak{P}_r \cap L$, and $\mathfrak{p}_r = \mathfrak{P}_r \cap K(r)$.

(1) As the constant field k of K is perfect, all residue field extensions in L/F are automatically separable. The result then follows from [13, Theorem 5.6.3].

(2) If $e(\mathfrak{P}|\mathfrak{p}) = 3$, then as $p \nmid 3$, it follows again from [Theorem 5.6.3, Ibid.] that $d(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{p}) - 1 = 2$.

(3) When $e(\mathfrak{P}|\mathfrak{p}) = 2$,

(a) if $p \neq 2$, then by [Theorem 5.6.3, Ibid.], $d(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{p}) - 1 = 1$.

(b) if $p = 2$, then we work on the tower $L(r)/K(r)/K$. If $e(\mathfrak{P}|\mathfrak{p}) = 2$, then $e(\mathfrak{p}_r|\mathfrak{p}) = 2$, $e(\mathfrak{P}_r|\mathfrak{p}_r) = 1$ and $e(\mathfrak{P}_r|\mathfrak{P}) = 1$. As $p = 2$, the extension $K(r)/K$ is Artin-Schreier and is generated by an element α such that $\alpha^2 - \alpha = \frac{1}{a^2} + 1$. By Artin-Schreier theory (see [11, Theorem 3.7.8]), as $e(\mathfrak{p}_r|\mathfrak{p}) = 2$, there exists an element $w_{\mathfrak{p}} \in K$ such that

$$\left(v_{\mathfrak{p}}\left(\frac{1}{a^2} + 1 - w_{\mathfrak{p}}^2 + w_{\mathfrak{p}}\right), 2\right) = 1 \quad \text{and} \quad v_{\mathfrak{p}}\left(\frac{1}{a^2} + 1 - w_{\mathfrak{p}}^2 + w_{\mathfrak{p}}\right) < 0.$$

In addition, since $e(\mathfrak{P}_r|\mathfrak{P}) = 1$, there exists $\eta_{\mathfrak{P}} \in L$ such that

$$v_{\mathfrak{P}}\left(\frac{1}{a^2} + 1 - \eta_{\mathfrak{P}}^2 + \eta_{\mathfrak{P}}\right) \geq 0.$$

By Artin-Schreier theory (see [11, Theorem 3.7.8]), we obtain

$$d(\mathfrak{p}_r|\mathfrak{p}) = -v_{\mathfrak{p}}\left(\frac{1}{a^2} + 1 - w_{\mathfrak{p}}^2 + w_{\mathfrak{p}}\right) + 1.$$

By [13, Theorem 5.7.15], we then find by equating differential exponents in the towers $L(r)/K(r)/K$ and $L(r)/L/K$ that

$$d(\mathfrak{P}_r|\mathfrak{p}) = d(\mathfrak{P}_r|\mathfrak{P}) + e(\mathfrak{P}_r|\mathfrak{P})d(\mathfrak{P}|\mathfrak{p}) = d(\mathfrak{P}_r|\mathfrak{p}_r) + e(\mathfrak{P}_r|\mathfrak{p}_r)d(\mathfrak{p}_r|\mathfrak{p}).$$

This implies that

$$d(\mathfrak{P}|\mathfrak{p}) = d(\mathfrak{p}_r|\mathfrak{p}) = -v_{\mathfrak{p}}\left(\frac{1}{a^2} + 1 - w_{\mathfrak{p}}^2 + w_{\mathfrak{p}}\right) + 1,$$

as $e(\mathfrak{P}_r|\mathfrak{P}) = e(\mathfrak{P}_r|\mathfrak{p}_r) = 1$ implies $d(\mathfrak{P}_r|\mathfrak{P}) = d(\mathfrak{P}_r|\mathfrak{p}_r) = 0$. □

We are now able to state and prove the Riemann–Hurwitz formulae for this cubic form.

Theorem 5.4 (Riemann–Hurwitz II) *Let* $p \neq 3$. *Let* L/K *be a cubic geometric extension and* y *a primitive element of* L *with minimal polynomial* $f(X) = X^3 - 3X - a$. *Let* $\Delta = -27(a^2 - 4)$ *be the discriminant of* $f(X)$ *and* r *a root of the quadratic resolvent* $R(X) =$

$X^2 + 3aX + (-27 + 9a^2)$ of the cubic polynomial $X^3 - 3X - a$ in $\overline{K}$. Then the genus g_L of L is given according to the formula

(1) *If $p \neq 2$, then*

$$g_L = 3g_K - 2 + \frac{1}{2}\sum_{\mathfrak{p}\in\mathcal{S}} d_K(\mathfrak{p}) + \sum_{\substack{v_\mathfrak{p}(a)<0 \\ (v_\mathfrak{p}(a),3)=1}} d_K(\mathfrak{p}).$$

where $\mathcal{S}$ is the set of places of K such that both $a \equiv \pm 2 \mod \mathfrak{p}$ and $v_\mathfrak{p}(\Delta, 2) = 1$. Moreover, Δ is a square in K up to a unit if, and only if, the set $\mathcal{S}$ is empty.

(2) *If $p = 2$, then*

$$g_L = 3g_K - 2 + \frac{1}{2}\sum_{\mathfrak{p}\in\mathcal{S}} \left[-v_\mathfrak{p}\left(\frac{1}{a} + 1 - w_\mathfrak{p}^2 + w_\mathfrak{p}\right) + 1 \right] d_K(\mathfrak{p}) + \sum_{\substack{v_\mathfrak{p}(a)<0 \\ (v_\mathfrak{p}(a),3)=1}} d_K(\mathfrak{p}),$$

where $\mathcal{S}$ is the set of places of K such that both $a \equiv 0 \mod \mathfrak{p}$ and there exists $w_\mathfrak{p} \in K$ such that $v_\mathfrak{p}\left(\frac{1}{a} + 1 - w_\mathfrak{p}^2 + w_\mathfrak{p}\right) < 0$ and $\left(v_\mathfrak{p}\left(\frac{1}{a} + 1 - w_\mathfrak{p}^2 + w_\mathfrak{p}\right), 2\right) = 1$. Moreover, if $r \in K$ (hence the extension L/K is Galois), then the set $\mathcal{S}$ is empty.

Proof (1) By [13, Theorem 9.4.2], the term associated with a place $\mathfrak{P}$ of L in the different $\mathfrak{D}_{L/F}$ contributes $\frac{1}{2}d_L(\mathfrak{P})^{d(\mathfrak{P}|\mathfrak{p})}$ to the genus of L, where $\mathfrak{p}$ is the place of K below $\mathfrak{P}$, $d_L(\mathfrak{P})$ is the degree of the place $\mathfrak{P}$, and $d(\mathfrak{P}|\mathfrak{p})$ is the differential exponent of $\mathfrak{P}|\mathfrak{p}$. By the fundamental identity $\sum_i e_i f_i = [L : K] = 3$ for ramification indices e_i and inertia degrees f_i of all places of L above $\mathfrak{p}$, we always have that $f_i = 1$ whenever $\mathfrak{p}$ ramifies in L (fully or partially). Thus from Lemma 5.3, it follows that $d(\mathfrak{P}|\mathfrak{p}) = 2$ if $\mathfrak{p}$ is fully ramified, whereas $d(\mathfrak{P}|\mathfrak{p}) = 1$ if $\mathfrak{p}$ is partially ramified. The result then follows by reading off [Theorem 9.4.2, Ibid.] and using the conditions of Lemma 5.3.

(2) This follows in a manner similar to part (1) of this theorem, via Lemma 5.3 for $p = 2$.

We obtain directly the following corollary when the extension L/K is Galois.

Corollary 5.5 *Let $p \neq 3$. Let L/K be a Galois cubic geometric extension and y a primitive element of L with minimal polynomial $f(X) = X^3 - 3X - a$. Then the genus g_L of L is given according to the formula*

$$g_L = 3g_K - 2 + \sum_{\substack{v_\mathfrak{p}(a)<0 \\ (v_\mathfrak{p}(a),3)=1}} d_K(\mathfrak{p}).$$

5.3 $X^3 + aX + a^2, a \in K, p = 3$

Lemma 5.6 *Suppose that $p = 3$. Let L/K be a separable cubic extension and y a primitive element with minimal polynomial $X^3 + aX + a^2$. Let $\mathfrak{p}$ be a place of K and $\mathfrak{P}$ a place of L above $\mathfrak{p}$. Then precisely one of the following is true:*

(1) *$d(\mathfrak{P}|\mathfrak{p}) = 0$ if, and only if, $e(\mathfrak{P}|\mathfrak{p}) = 1$.*

(2) *When $e(\mathfrak{P}|\mathfrak{p}) = 3$, by Theorem 4.11, there is $w_\mathfrak{p} \in K$ such that $v_\mathfrak{p}(\alpha_\mathfrak{p}) < 0$ and $(v_\mathfrak{p}(\alpha_\mathfrak{p}), 3) = 1$ with*

$$\alpha_\mathfrak{p} = \frac{(ja^2 + (w_\mathfrak{p}^3 + aw_\mathfrak{p}))^2}{a^3}.$$

Then $d(\mathfrak{P}|\mathfrak{p}) = -v_\mathfrak{p}(\alpha_\mathfrak{p}) + 2$.

(3) *$d(\mathfrak{P}|\mathfrak{p}) = 1$ whenever $e(\mathfrak{P}|\mathfrak{p}) = 2$. Moreover, by Lemma 4.11, when $e(\mathfrak{P}|\mathfrak{p}) = 2$, there is generator $z_\mathfrak{p}$ such that $z_\mathfrak{p}^3 + c_\mathfrak{p} z_\mathfrak{p} + c_\mathfrak{p}^2 = 0$ and $v_\mathfrak{p}(c_\mathfrak{p}) \geq 0$ and $(v_\mathfrak{p}(c_\mathfrak{p}), 2) = 1$.*

Proof Let $b \in \overline{K}$ such that $b^2 = -a$, $\mathfrak{p}$ be a place of K, $\mathfrak{P}_b$ be a place of $L(b)$ above $\mathfrak{p}$, $\mathfrak{p}_b = \mathfrak{P}_b \cap K(b)$, $\mathfrak{P} = \mathfrak{P}_b \cap L$.

(1) This is an immediate consequence of [13, Theorem 5.6.3].

(2) Suppose that $\mathfrak{p}$ is ramified in L, whence $\mathfrak{p}_b$ is ramified in $L(b)$. Moreover, by Theorem 4.11, there exists $w_\mathfrak{p} \in K$ such that $v_\mathfrak{p}(\alpha_\mathfrak{p}) < 0$ and $(v_\mathfrak{p}(\alpha_\mathfrak{p}), 3) = 1$, where

$$\alpha_\mathfrak{p} = \frac{(ja^2 + (w_\mathfrak{p}^3 + aw_\mathfrak{p}))^2}{a^3},$$

and furthermore, there exists a generator $z_\mathfrak{p}$ of L such that $z_\mathfrak{p}^3 + \alpha_\mathfrak{p} z_\mathfrak{p} + \alpha_\mathfrak{p}^2 = 0$. Again by [Theorem 5.6.3, Ibid.], the differential exponent $d(\mathfrak{p}_b|\mathfrak{p}) = d(\mathfrak{P}_b|\mathfrak{P})$ of $\mathfrak{p}$ over $K(b)$ (resp. $\mathfrak{P}$ over $L(b)$) is equal to

(a) 1 if $\mathfrak{p}$ is ramified in $K(b)$, whence $e(\mathfrak{p}_b|\mathfrak{p}) = e(\mathfrak{P}_b|\mathfrak{P}) = 2$, and

(b) 0 if $\mathfrak{p}$ is unramified in $K(b)$, whence $e(\mathfrak{p}_b|\mathfrak{p}) = e(\mathfrak{P}_b|\mathfrak{P}) = 1$.

By [1, Theorem 2.3], $L(b)/K(b)$ is Galois and $-\alpha_\mathfrak{p}$ is a square in $K(b)$. We write $-\alpha_\mathfrak{p} = \beta_\mathfrak{p}^2$. Moreover, $w_\mathfrak{p} = \frac{z_\mathfrak{p}}{\beta_\mathfrak{p}}$ and $w_\mathfrak{p}^3 - w_\mathfrak{p} - \beta_\mathfrak{p} = 0$. Moreover,

$$v_{\mathfrak{p}_b}(\beta_\mathfrak{p}) = \frac{v_{\mathfrak{p}_b}(\alpha_\mathfrak{p})}{2} = \frac{e(\mathfrak{p}_b|\mathfrak{p}) v_\mathfrak{p}(\alpha_\mathfrak{p})}{2}$$

with $e(\mathfrak{p}_b|\mathfrak{p}) = 2$ or 1, depending on whether $\mathfrak{p}$ is ramified or not in $K(b)$. Also, $v_{\mathfrak{p}_b}(\beta_\mathfrak{p}) = v_\mathfrak{p}(\alpha_\mathfrak{p})$ when $\mathfrak{p}$ is ramified in $K(b)$, whereas $v_{\mathfrak{p}_b}(\beta_\mathfrak{p}) = \frac{v_\mathfrak{p}(\alpha_\mathfrak{p})}{2}$ when $\mathfrak{p}$ is unramified in $K(b)$ (note that in this case $2|v_\mathfrak{p}(\alpha_\mathfrak{p})$). Thus $v_{\mathfrak{p}_b}(\beta_\mathfrak{p}) < 0$ and $(v_{\mathfrak{p}_b}(\beta_\mathfrak{p}), 3) = 1$ and by [11, Theorem 3.7.8], we also have that the differential exponent $d(\mathfrak{P}_b|\mathfrak{p}_b)$ of $\mathfrak{p}_b$ in $L(b)$ satisfies

$$d(\mathfrak{P}_b|\mathfrak{p}_b) = 2(-v_\mathfrak{p}(\beta_\mathfrak{p}) + 1).$$

By [13, Theorem 5.7.15], the differential exponent of $\mathfrak{p}$ in $L(b)$ satisfies

$$d(\mathfrak{P}_b|\mathfrak{p}) = d(\mathfrak{P}_b|\mathfrak{p}_b) + e(\mathfrak{P}_b|\mathfrak{p}_b) d(\mathfrak{p}_b|\mathfrak{p}) = d(\mathfrak{P}_b|\mathfrak{P}) + e(\mathfrak{P}_b|\mathfrak{P}) d(\mathfrak{P}|\mathfrak{p}).$$

Thus,

(a) if $\mathfrak{p}$ is ramified in $K(b) = K(\beta_\mathfrak{p})$, that is, $(v_\mathfrak{p}(\alpha_\mathfrak{p}), 2) = 1$ by [11, Proposition 3.7.3], then $2(-v_\mathfrak{p}(\alpha_\mathfrak{p}) + 1) + 3 = 1 + 2d(\mathfrak{P}|\mathfrak{p})$ and

$$d(\mathfrak{P}|\mathfrak{p}) = -v_\mathfrak{p}(\alpha_\mathfrak{p}) + 2,$$

whereas

(b) if $\mathfrak{p}$ is unramified in $K(b)$, that is, $2|v_\mathfrak{p}(\alpha_\mathfrak{p})$ again by [11, Proposition 3.7.3], then also

$$d(\mathfrak{P}|\mathfrak{p}) = 2\left(-\frac{v_\mathfrak{p}(\alpha_\mathfrak{p})}{2} + 1\right) = -v_\mathfrak{p}(\alpha_\mathfrak{p}) + 2.$$

(3) This is immediate from Theorem 4.11 and [13, Theorem 5.6.3], via application of the same method as in Lemma 5.3 (3). □

Finally, we use this to conclude the Riemann–Hurwitz formulae for cubic extensions in characteristic 3.

Theorem 5.7 (Riemann–Hurwitz III) *Suppose that $p = 3$. Let L/K be a separable cubic extension and y a primitive element with minimal polynomial $X^3 + aX + a^2$. Then the genus g_L of L is given according to the formula*

$$g_L = 3g_K - 2 + \frac{1}{2}\sum_{\mathfrak{p}\in S}\left(-v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) + 2\right) d_K(\mathfrak{p}) + \frac{1}{2}\sum_{\mathfrak{p}\in T} d_K(\mathfrak{p}),$$

where

(1) *S is the set of places of K for which there exists $w_{\mathfrak{p}} \in K$ such that $v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) < 0$, $(v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}), 3) = 1$ with*

$$\alpha_{\mathfrak{p}} = \frac{(ja^2 + (w_{\mathfrak{p}}^3 + aw_{\mathfrak{p}}))^2}{a^3},$$

and

(2) *T is the set of places of K for which there is generator $z_{\mathfrak{p}}$ such that $z_{\mathfrak{p}}^3 + c_{\mathfrak{p}}z_{\mathfrak{p}} + c_{\mathfrak{p}}^2 = 0$, $v_{\mathfrak{p}}(c_{\mathfrak{p}}) \geq 0$ and $(v_{\mathfrak{p}}(c_{\mathfrak{p}}), 2) = 1$.*

Proof This follows from Lemma 5.6, [13, Theorem 9.4.2], and the fundamental identity $\sum e_i f_i = [L : K] = 3$. □

Acknowledgements
We would like to thank the anonymous referees for their helpful corrections and suggestions to this paper.

Received: 30 April 2019 Accepted: 14 October 2019 Published online: 6 November 2019

References

1. Conrad, K.: Galois groups of cubics and quartics in all characteristics. Unpublished note
2. Jacobson Jr., M.J., Lee, Y., Scheidler, R., Williams, H.C.: Construction of all cubic function fields of a given square-free discriminant. Int. J. Number Theory **11**(6), 1839–1885 (2015)
3. Marques, S., Ward, K.: A complete classification of cubic function fields over any finite field. Preprint (2017)
4. Marques, S.: Generic polynomials for cyclic function field extensions over certain finite fields. Eur. J. Math. **4**(2), 585–602 (2018)
5. Marques, S., Ward, K.: Cubic fields: a primer. Eur. J. Math. **5**(2), 551–570 (2018)
6. Marques, S., Ward, K.: An explicit triangular integral basis for any separable cubic extension of a function field. Eur. J. Math. **5**, 1252–1266 (2018)
7. Neukirch, J.: Algebraic Number Theory. Springer, Berlin (1999)
8. Scheidler, R.: Construction of all cubic fields of a fixed fundamental discriminant. In: Hambleton, S., Williams, H.C. (eds.) Cubic Fields With Geometry, pp. 173–302. Springer, New York (2018)
9. Scheidler, R., Webster, J., Landquist, E., Rozenhart, P., Wu, Q.: An explicit treatment of cubic function fields with applications. Can. J. Math. **62**(4), 787–807 (2010)
10. Scheidler, R., Wu, Q.: An explicit treatment of biquadratic function fields. Contrib. Discret. Math. **2**(1), 43–60 (2007)
11. Stichtenoth, H.: Algebraic Function Fields and Codes. Springer, Berlin (2009)
12. Tutdere, S., Anbar, N., Stichtenoth, H.: On ramification in the compositum of function fields. Bull. Braz. Math. Soc. **40**(4), 539–552 (2009)
13. Villa-Salvador, G.D.: Topics in the Theory of Algebraic Function Fields. Birkhäuser, Boston (2006)
14. Wu, Q., Scheidler, R.: On ramification in the compositum of function fields. Bull. Braz. Math. Soc. **4**, 539–552 (2009)

Publisher's Note