Global fields and their L-functions

Solomatin, P.

Part II

Function Fields and Their L-functions

Chapter 3

Arithmetical Equivalence for Global Function Fields

3.1 Introduction

3.1.1 Preliminaries

Let $q = p^m$, p be a prime number and $k = \mathbb{F}_q$. Let us consider two curves X and Y over k. As usual by a curve we mean a smooth, projective, geometrically connected variety of dimension one over k. If we fix a k-rational generically etale morphisms of X and Y to $\mathbb{P}^1$, then we obtain two finite separable geometric extensions of $\mathbb{F}_q(x)$ and we will denote them by K and K' respectively. By analogy with the number field case discussed in the previous chapter, we have notions of arithmetical equivalence, splitting equivalence, Gassmann equivalence and Dedekind zeta-function. For the sake of coherence let us briefly explain some notions, for details see [42], chapters V and IX.

First we recall that the polynomial ring $A = \mathbb{F}_q[x]$ is an analogue of $\mathbb{Z}$ with prime numbers replaced by monic irreducible polynomials. Prime ideals in $\mathbb{F}_q[x]$ are in one-to-one correspondence with monic irreducible polynomials in $\mathbb{F}_q[x]$. The ring $\mathbb{F}_q[x]$ is also a principal ideal domain. Any finite separable extension K of $\mathbb{F}_q(x)$ is given as quotient $\mathbb{F}_q[x,y]/(g(x,y))$ where $g(x,y) \in \mathbb{F}_q[x,y]$ is a monic, separable, irreducible polynomial in y with with coefficients in $\mathbb{F}_q[x]$. We suppose that this extension is geometric which means that the exact constant field of K is also $\mathbb{F}_q$. This restriction is not very important, but makes some theorems easier to state. Given a finite separable geometric extension K of $\mathbb{F}_q(x)$ we consider the integral closure $\mathcal{O}_K$ of $\mathbb{F}_q[x]$ in K. As in the number field case, in general this is not a principal ideal domain, but is a Dedekind domain, therefore in the function field case, the analogue of the Kummer-Dedekind theorem 1.2 from the previous chapter holds, as before see [33], chapter IV for the general statement about factorization of primes in Dedekind domains. It means the factorization of all except finitely many prime ideals (f) in $\mathcal{O}_K$ is given via factorization of the image of $g(x,y)$ into irreducible polynomials in the polynomial ring $(\mathbb{F}_q[x]/(f(x)))[y]$ associated to the residue field of (f). We say two such extensions K, K' *split equivalently* if for all except finitely many prime ideals (f) there is a bijection from prime ideals in $\mathcal{O}_K$ lying above (f) to those ideals of $\mathcal{O}_{K'}$. They are *arithmetically equivalent* if this bijection is degree preserving for almost all primes. Finally since both extensions K, K' are separable they have common Galois closure which we denote by N. Note that the full constant field of N could be different from $\mathbb{F}_q$. Let $G = \mathrm{Gal}(N/\mathbb{F}_q(x))$, $H = \mathrm{Gal}(N/K)$, $H' = \mathrm{Gal}(N/L)$. See the diagram below.

$$\begin{tikzcd}
 & N \arrow[dl, dash, "H"'] \arrow[dr, dash, "H'"] \arrow[dd, dash, bend right, "G"] & \\
K \arrow[dr, dash] & & L \arrow[dl, dash] \\
 & \mathbb{F}_q(x) &
\end{tikzcd}$$

As before we will say that (G, H, H') form a Gassmann triple if $\mathrm{Ind}_H^G(1_H) \simeq \mathrm{Ind}_{H'}^G(1_{H'})$, where 1_H(and $1_{H'}$) means trivial representation of H(of H' respectively). In this case we will also say that K, K' are Gassmann equivalent. Finally to each such extension one associates its Dedekind zeta-function. Following notations from [42], chapter V we define it as:

$$\zeta_K(s) = \sum_{\mathfrak{a} \geq 0} \mathcal{N}(\mathfrak{a})^{-s},$$

where $\mathfrak{a}$ runs over effective divisors of the corresponding curve X. In particular we include in the definition of $\zeta_K(s)$ infinite places of X and therefore $\zeta_K(s)$ does not depend on the map from X to $\mathbb{P}^1$.

It is not difficult to see that in this settings notions of Gassmann equivalence, splitting equivalence and arithmetical equivalence coincide. But in contrast to the number field case, Theorem 1.23 from the previous chapter is false in its full generality for the function field case. Namely, the implication from 1 to 2 is problematic. The problem is that the Dedekind zeta-function does not determine the splitting type, since in general there exist places in K with the same norm above different places of $\mathbb{F}_q(x)$. One suitable approach here is to change the definition of the zeta-function associated to K. It turns out, that if one replace usual zeta-function by the so-called *lifted Goss zeta-function*, then an analogue of Theorem 1.23 theorem becomes true. We refer an interested reader to [8]. The main purpose of this chapter is to recall and then extend another approach to study arithmetically equivalent global function fields.

3.1.2 Results of the Chapter

Let K/F be a Galois extension of global fields with the Galois group $G = \mathrm{Gal}(K/F)$. Then for any finite dimensional complex representation ρ of G one attaches the Artin L-function $L_F(\rho, s)$. The definition is essentially the same as in the number field case with one exception that we also need to include infinite primes of K. This is a meromorphic function of complex variable s. It also satisfies induction, inflation and additivity properties. Moreover by Theorem of A.Weil if K/F is geometric, ρ is irreducible and non-trivial then $L_K(\rho, s)$ is a polynomial in q^{-s}, see Theorem 9.16B, from [42]. For the sake of brevity we will denote it by $L_F(\rho)$, omitting the variable s.

As we already mentioned, K.Nagata in 1986 published [32] from which a careful reader can extract the following result:

Theorem 3.1. *Let K, K' denote two finite separable geometric extensions of $\mathbb{F}_q(x)$. Let N denote the common Galois closure and $G = \mathrm{Gal}(N/\mathbb{F}_q(x))$, $H = \mathrm{Gal}(N/K)$, $H' = \mathrm{Gal}(N/K')$. Let $\rho_1, \ldots, \rho_n$ denote all irreducible complex representations of G. Let $\psi = \mathrm{Ind}_H^G(1_H)$ and $\psi' = \mathrm{Ind}_{H'}^G(1_{H'})$. The following are equivalent:*

1. *For all i such that $1 \leq i \leq n$, we have $L_K(\rho_i|_H) = L_{K'}(\rho_i|_{H'})$;*
2. *$L_K(\psi|_H) = L_{K'}(\psi|_{H'})$ and $L_K(\psi'|_H) = L_{K'}(\psi'|_{H'})$;*
3. *K and K' are arithmetically equivalently;*
4. *K and K' split equivalently;*
5. *(G, H, H') forms a Gassmann triple.*

In this chapter we improve his argument and prove the above Theorem as a particular case of the following more general result[1]:

Theorem 3.2. *In the above settings let α denotes a complex representation of H and α' denotes a complex representation of H'. Let $\psi = \mathrm{Ind}_H^G(\alpha)$ and $\psi' = \mathrm{Ind}_{H'}^G(\alpha')$. For any representation ρ of G let $\bar{\rho}$ denote the dual representation of ρ.The following are equivalent:*

1. *For all i such that $1 \leq i \leq n$ we have equality of Artin L-functions: $L_K(\alpha \otimes \rho_i|_H) = L_{K'}(\alpha' \otimes \rho_i|_{H'})$*
2. *$L_K(\bar{\alpha} \otimes (\psi|_H)) = L_{K'}(\bar{\alpha'} \otimes (\psi|_{H'}))$, and*
   $L_K(\bar{\alpha} \otimes (\psi'|_H)) = L_{K'}(\bar{\alpha'} \otimes (\psi'|_{H'}))$;
3. *Induced representations ψ and ψ' are isomorphic.*

This Theorem is not just a formal generalisation of Nagata's results but also allows us to use group theory to construct for any given pair of non-isomorphic global function fields a *finite list of L-functions which distinguishes them.* As in the previous section this goal is achieved in two steps. First we need the group-theoretical result discussed in the previous chapter, namely Theorem 2.6. Next, in the settings of Theorem [3.1] we construct a Galois extension M of $\mathbb{F}_q(t)$ containing K and K' such that the Galois group $\mathrm{Gal}(M : \mathbb{F}_q(t))$ is $\tilde{G}$ and $K = M^{\tilde{H}}$, $K' = M^{\tilde{H}'}$ for $\tilde{G}$, $\tilde{H}$, $\tilde{H}'$ as in Theorem [2.6]. Altogether, this gives us:

Theorem 3.3. *For a given pair K and K' of finite separable geometric extensions of $F = \mathbb{F}_q(t)$ there exists a Galois extension M of $\mathbb{F}_q(t)$ with Galois group $\tilde{G}$, such that $K = M^{\tilde{H}}$ and $K' = M^{\tilde{H}'}$ for some subgroups $\tilde{H}$, $\tilde{H}'$ of $\tilde{G}$ with the following properties. There exists an abelian character α of $\tilde{H}$ such that for any abelian character α' of $\tilde{H}'$ the following are equivalent :*

1. *For any irreducible representation ρ of $\tilde{G}$ we have equality of Artin L-functions:*

$$L_K(\alpha \otimes \rho|_{\tilde{H}}) = L_{K'}(\alpha' \otimes \rho|_{\tilde{H}'});$$

[1] In order to get Nagata's result plug in the settings trivial representations $\alpha = 1_H$ and $\beta = 1_{H'}$

2. *$L_K(\bar{\alpha} \otimes (\psi|_{\tilde{H}})) = L_{K'}(\bar{\alpha'} \otimes (\psi|_{\tilde{H}'}))$, and*
   $L_K(\bar{\alpha} \otimes (\psi'|_{\tilde{H}})) = L_{K'}(\bar{\alpha'} \otimes (\psi'|_{\tilde{H}'}))$,
   where $\psi = \mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\alpha)$ and $\psi' = \mathrm{Ind}_{\tilde{H}'}^{\tilde{G}}(\alpha')$;

3. *Induced representations ψ and ψ' are isomorphic.*

Moreover, if those conditions hold then K and K' isomorphic as extensions of $\mathbb{F}_q(t)$.

The chapter has the following structure: in the next section we give a proof of Theorem 3.2. After that we study arithmetical equivalence for global function fields: we provide few explicit examples of non-isomorphic, but arithmetically equivalent global function fields, discuss an algorithm to construct two-parametric family of such pairs for many base fields of different characteristic and briefly review properties of such fields. In the next section we give a proof of Theorem 2.6 and in the last section we give a proof of Theorem 3.3.

3.2 On the L-functions criteria

In this section we are going to prove our main Theorem 3.2, but before that, let us first consider one particular example of Theorem 3.1. This example illustrates the following: we construct two degree two extensions K, K' of $\mathbb{F}_7(x)$ such that $\zeta_K(s) = \zeta_{K'}(s)$, but K and K' are not arithmetically equivalent. Denoting by N the common normal closure of K and K' and keeping notations from the settings of 3.1 we will construct a character χ of $\mathrm{Gal}(N : \mathbb{F}_7(x))$ such that

$$L_K(\chi|_H, s) \neq L_{K'}(\chi|_{H'}, s).$$

Example 3.4. *Consider two elliptic curves E and E' over $\mathbb{F}_7$, affine part of which defined by equations $y^2 = x^3 + 1$ and $y^2 = x^3 + 3x + 1$ respectively. Let us denote by K and K' the corresponding function fields. One checks that*

$$\zeta_K(T) = \frac{7T^2 + 4T + 1}{(1-T)(1-7T)} = \zeta_{K'}(T),$$

where $T = 7^{-s}$. Hence by the theorem of A.Weil, E and E' are $\mathbb{F}_7$-isogenous, but $j(E) = 0$ and $j(E') = 2$ so they are not isomorphic even over the algebraic closure $\overline{\mathbb{F}_7}$ and hence $K \not\simeq K'$.

In the above example we have two quadratic extensions $\mathbb{F}_7(\sqrt{f_i(x)})/\mathbb{F}_7(x)$, where $f_1(x) = x^3 + 1$ and $f_2(x) = x^3 + 3x + 1$. Obviously those are abelian Galois extensions with Galois group C_2. It means that despite the fact that K and K' share the same ζ-function they do not share splitting type(otherwise they must be isomorphic). According to Theorem 3.1 this means that there exists an L-function which distinguishes them. More concretely, let us consider the common Galois closure N. We denote by G, H, H' Galois groups of $\mathrm{Gal}(N/\mathbb{F}_7(x)), \mathrm{Gal}(N/K), \mathrm{Gal}(N/K')$, respectively. We have $G = C_2 \oplus C_2$ and hence there exists a one-dimensional character χ of G such that $\chi|_H = 1_H$ and $\chi|_{H'} \neq 1_{H'}$. Now $L_K(\chi|_H) = \zeta_K$ and therefore this function has a pole at $s = 1$. But, $L_{K'}(\chi|_{H'})$ is an Artin L-function of a non-trivial abelian character, hence it has no poles, see [42],chapter IX. Therefore we see that

$$L_K(\chi|_H) \neq L_{K'}(\chi|_{H'}).$$

This idea gives rise to Theorems 3.1 and 3.2.

Proof of Theorem 3.2. First we show implication **from (1) to (3)**. For any fixed representation ρ of G we consider $L_K(\alpha \otimes \rho|_H)$. This is a meromorphic L-function with no poles outside $s = 0$ and $s = 1$, see [42]. By properties of Artin L-functions this function has a pole at $s = 1$ of order $(\alpha \otimes \rho|_H, 1)_H$, possibly zero. Because of properties of complex representations: $(\alpha \otimes \rho|_H, 1)_H = (\rho|_H, \bar{\alpha})_H$, where $\bar{\alpha}$ means the dual of the representation α. By Frobenius reciprocity we have

$$(\rho|_H, \bar{\alpha})_H = (\rho, \mathrm{Ind}_H^G(\bar{\alpha}))_G.$$

In means that equality $L_K(\alpha \otimes \rho_i|_H) = L_{K'}(\alpha' \otimes \rho_i|_{H'})$ implies

$$(\rho_i, \mathrm{Ind}_H^G(\bar{\alpha}))_G = (\rho_i, \mathrm{Ind}_{H'}^G(\bar{\alpha}'))_G.$$

Since ρ_i runs over all irreducible representations of G it means that

$$\mathrm{Ind}_H^G(\bar{\alpha}) \simeq \mathrm{Ind}_{H'}^G(\bar{\alpha}')$$

and therefore $\mathrm{Ind}_H^G(\alpha) \simeq \mathrm{Ind}_{H'}^G(\alpha')$.

From (3) to (1). By Frobenius reciprocity for each i, $j \in \{1 \dots n\}$ we have:

$$(\mathrm{Ind}_H^G(\alpha \otimes \rho_i|_H), \rho_j)_G \simeq (\alpha \otimes \rho_i|_H, \rho_j|_H)_H \simeq (\alpha, (\bar{\rho}_i \otimes \rho_j)|_H)_H \simeq (\mathrm{Ind}_H^G(\alpha), \bar{\rho}_i \otimes \rho_j)_G,$$

By our assumptions $\mathrm{Ind}_H^G(\alpha) \simeq \mathrm{Ind}_{H'}^G(\alpha')$, we therefore have:

$$(\mathrm{Ind}_H^G(\alpha), \bar{\rho}_i \otimes \rho_j)_G \simeq (\mathrm{Ind}_{H'}^G(\alpha'), \bar{\rho}_i \otimes \rho_j)_G,$$

and hence for each irreducible representation ρ_i, we have:

$$\mathrm{Ind}_H^G(\alpha \otimes \rho_i|_H) \simeq \mathrm{Ind}_{H'}^G(\alpha' \otimes \rho_i|_{H'}).$$

Finally, by the Artin induction property it follows that:

$$L_K(\alpha \otimes \rho_i|_H) = L_{\mathbb{F}_q(x)}(\mathrm{Ind}_H^G(\alpha \otimes \rho_i|_H)),$$

and therefore we are done.

From (2) to (3). As before from equality of L-functions we obtained equality of orders of poles at $s = 1$ and therefore following equalities:

$$(\bar{\alpha} \otimes (\psi|_H), 1_H)_H = (\bar{\alpha'} \otimes (\psi|_{H'}), 1_{H'})_{H'}$$

and

$$(\bar{\alpha} \otimes (\psi'|_H), 1_H)_H = (\bar{\alpha'} \otimes (\psi'|_{H'}), 1_{H'})_{H'}.$$

By Frobenius reciprocity we have:

$$(\bar{\alpha} \otimes (\psi|_H), 1_H)_H = (\alpha, \psi|_H)_H = (\psi, \psi)_G$$

and

$$(\bar{\alpha'} \otimes (\psi|_{H'}), 1_{H'})_{H'} = (\alpha', \psi|_{H'})_{H'} = (\psi', \psi)_G$$

Therefore assumptions of (2) implies $(\psi, \psi)_G = (\psi, \psi')_G = (\psi', \psi')_G$. Let us consider the scalar of product of the virtual representation $\psi - \psi'$ with itself: $(\psi - \psi', \psi - \psi')_G = (\psi, \psi)_G - 2(\psi, \psi')_G + (\psi', \psi')_G = 0$. Which implies that ψ and ψ' are isomorphic.

From (3) to (2)

Note that $L_K(\bar{\alpha} \otimes (\psi|_H)) = L_{\mathbb{F}_q(x)}(\mathrm{Ind}_H^G(\bar{\alpha} \otimes (\psi|_H)))$. Therefore in order to get equality of L-functions it is enough to show:

$$\mathrm{Ind}_H^G(\bar{\alpha} \otimes (\psi|_H)) \simeq \mathrm{Ind}_{H'}^G(\bar{\alpha'} \otimes (\psi|_{H'})).$$

Let ρ_i run over irreducible representations of G. By Frobenius reciprocity we have:

$$(\mathrm{Ind}_H^G(\bar{\alpha} \otimes (\psi|_H)), \rho_i)_G = (\bar{\alpha} \otimes \psi|_H, \rho_i|_H)_H = (\bar{\alpha}, \rho_i|_H \otimes \bar{\psi}|_H)_H = (\bar{\psi}, \rho_i \otimes \bar{\psi})_G.$$

Since $\psi = \psi'$ we have:

$$(\bar{\psi}, \rho_i \otimes \bar{\psi})_G = (\bar{\psi'}, \rho_i \otimes \bar{\psi})_G = (\bar{\alpha'}, \rho_i|_{H'} \otimes \bar{\psi}|_{H'})_{H'} = (\bar{\alpha'} \otimes \psi|_{H'}, \rho_i|_{H'})_{H'} = (\mathrm{Ind}_{H'}^G(\bar{\alpha'} \otimes (\psi|_{H'})), \rho_i)_G$$

Which means that two representations are isomorphic:

$$\mathrm{Ind}_H^G(\bar{\alpha} \otimes (\psi|_H)) \simeq \mathrm{Ind}_{H'}^G(\bar{\alpha'} \otimes (\psi|_{H'})).$$

By replacing ψ by ψ' we obtained the second equality of L-functions. □

Note that if α is the trivial representation, then $L_K(\alpha \otimes \rho_H) = L_K(\rho_H)$. Therefore equality of L-functions for each irreducible ρ: $L_K(\rho|_H) = L_{K'}(\rho|_{H'})$ implies arithmetical equivalence and vice versa.

This remark generalises the fact that equality of zeta-functions in the number field case is the same as arithmetical equivalence. At first sight this generalisation to the function field side seems to be not very natural, since it depends on the k-rational map of the curve X to $\mathbb{P}^1$ and not given in the intrinsic terms of X, but as we will see in the next section, this map is very important for the notion of arithmetical equivalence: it is possible to map curves X and Y to $\mathbb{P}^1$ in two different ways, such that their function fields are arithmetically equivalent under the first pair of maps, but not arithmetically equivalent under the second pair of maps.

3.3 On Gassmann Equivalence

3.3.1 Examples

In order to find examples of arithmetically equivalent function fields we must find a non-trivial example of a Gassmann triple (G, H, H') and solve the inverse Galois problem for G. As we already mentioned in 1.4.2 Gassmann triples corresponding to field extensions of degree up to 15 were classified in [5]. It follows that fields with Galois group $G \simeq \mathrm{PGL}_3(\mathbb{F}_2) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$ give rise to at least two non-trivial Gassmann triples: one in degree seven and one in degree fourteen. Also, fields with Galois group $G \simeq \mathrm{PSL}_2(\mathbb{F}_{11})$ give rise to at least one pair of arithmetically equivalent fields of degree eleven.

Using Magma we compute the Galois group of the splitting field of a given polynomial $f \in \mathbb{F}_q(x)[y]$ chosen in some particular way and find all intermediate subfields. By doing that for many different f we find explicit equations of arithmetically equivalent function fields and compare their properties.

Some Constructions

Here are some examples.

Example 3.5. *Let $p = 7$, $q = p^2$ and let α be a generator of $\mathbb{F}_q^*$. Consider the function field extension of $\mathbb{F}_q(x)$ given by $f(y) = y^{p+1} + y - x^{p+1}$. Its splitting field N has degree 168 and Galois group* $\mathrm{Gal}(N : \mathbb{F}_q(x)) \simeq \mathrm{PGL}_3(\mathbb{F}_2)$. *Inside this field we have at least two pairs of arithmetically equivalent global function fields:*

1. $K_1 : y^7 + 6x^8y^3 + \alpha^{28}x^{12}y + 4$ *and* $K_1' : y^7 + 5x^8y^3 + \alpha^4x^{12}y + 6$;
2. $K_2 : y^{14} + 3x^8y^6 + \alpha^4x^{12}y^2 + 5$ *and* $K_2' : y^{14} + 3x^8y^6 + \alpha^{28}x^{12}y^2 + 5$;

Note that since these fields arise from non-trivial triple (G, H, H') it means that they are not isomorphic as extensions of $\mathbb{F}_q(x)$, but it may happen that K and K' isomorphic as abstract fields. Indeed, one could check that in this case we have $K_1 \simeq K_1'$ and $K_2 \simeq K_2'$ as fields.

An interesting question is: is it possible to find arithmetically equivalent function fields K and K' that are not isomorphic as abstract fields? It was mentioned in [6] that a result by J.P. Serre states that the function field of the normal closure of the field given by $y^{p+1} - xy + 1$ over $\mathbb{F}_p$ has Galois group $\mathrm{PSL}_2(\mathbb{F}_p)$. By working out this example for $p = 7$ and $p = 11$ one finds a positive answer to the above question:

Example 3.6. *Consider the curve defined by the affine equation $y^8 - xy + 1$ over $\mathbb{F}_7$. The corresponding function field N of the normal closure has degree 168 and the Galois group is* $G \simeq \mathrm{PGL}_3(\mathbb{F}_2) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$. *Inside this field we have at least two pairs of arithmetically equivalent global function fields:*

1. $K_1 : y^7 + 2y^3 + 2y + 6x^2$ *and* $K_1' : y^7 + y^3 + 5y + 4x^2$;
2. $K_2 : y^{14} + 4y^6 + 5y^2 + 5x^2$ *and* $K_2' : y^{14} + 4y^6 + 2y^2 + 5x^2$;

Being arithmetically equivalent they share the same zeta-function and therefore their Weil-polynomials $f_K(T)$ are the same. Since $\#\,\mathrm{Pic}^0(C)[\mathbb{F}_q] = h = f_K(1)$ is the class number, we have that in contrast to the number fields they share the same class numbers, see [10]. But they have different class groups[2], hence they are not isomorphic. Indeed according to Magma we have:

$$\mathrm{Cl}(K_1) \simeq \mathrm{Cl}(K_2) \simeq \mathbb{Z}/8\mathbb{Z}$$

but

$$\mathrm{Cl}(K_1') \simeq \mathrm{Cl}(K_2') \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

The fact that $\mathrm{Cl}(K_1) \simeq \mathrm{Cl}(K_2)$ and $\mathrm{Cl}(K_1') \simeq \mathrm{Cl}(K_2')$ is not coincidence: $K_1 \simeq K_2$ and $K_1' \simeq K_2'$ as abstract fields. Another important remark here is that the genus of K_1 and K_1' is one. They have a rational point over $\mathbb{F}_7$ and therefore correspond to two elliptic curves E and E' defined over $\mathbb{F}_7$. By considering Weierstrass models of E and E' one gets degree two extensions of $\mathbb{F}_7(x)$, such that they are not arithmetically equivalent. More concretely, the curve defined by $y^7 + 2y^3 + 2y + 6x^2 = 0$ is isomorphic to the elliptic curve E_1 defined by $y^2 - x^3 - x = 0$ and the

[2] By a class group we mean the group of $\mathbb{F}_q$-rational points on the Jacobian variety $\mathrm{Jac}(X)$ associated to X.

curve given by the equation $y^7 + y^3 + 5y + 4x^2 = 0$ is isomorphic to the elliptic curve E_2 defined by $y^2 - x^3 - 3x = 0$. This illustrates that the notion of arithmetical equivalence completely depends on the map from X to $\mathbb{P}^1$.

Example 3.7. *Consider the curve defined by the affine equation $y^{12} - xy + 1 = 0$ over $\mathbb{F}_{11}$. The corresponding function field N of the normal closure has degree 660 and the Galois group is $G \simeq \mathrm{PSL}_2(\mathbb{F}_{11})$. Inside this field we have at least one pair of arithmetically equivalent global function fields: $K_1 : y^{11} + 2y^5 + 8y^2 + 10x^2 = 0$ and $K_1' : y^{11} + 2y^5 + 3y^2 + 10x^2 = 0$.*

One checks that K_1 and K_1' are not isomorphic as global fields, also have genus one and that $\mathrm{Cl}(K_1) \simeq \mathrm{Cl}(K_1') \simeq \mathbb{Z}/12\mathbb{Z}$.

Magma scripts

Let us first check example 3.5

```
// Initializing the function field F
p := 7; q := p^2;
K<alpha> := GF(q);
R<x> := FunctionField(K);
P<y> := PolynomialRing(R);
f := y^(p+1) + y - x^(p+1);
FF<alpha> := FunctionField(f);

// Verifying that the Galois of the normal closure of F is isomorphic to PGL_3(F_2)
G0 := PGL(3,2);
G, r, N := GaloisGroup(FF);
"Degree of the normal closure N of K is", #G;
"Is G isomorphic to PGL_3(F_2): ", IsIsomorphic(G,G0);

h := Subgroups(G: IndexEqual := 7);
H_1 := h[1]‘subgroup;
H_2 := h[2]‘subgroup;
"Is H_1 conjugate to H_2 inside G: ", IsConjugate(G, H_1, H_2);

"The group H_1 corresponds to the field extensions: ", GaloisSubgroup(N, H_1);
"The group H_2 corresponds to the field extensions: ", GaloisSubgroup(N, H_2);
```

This script produces the following output which completely aligned with the expectations:

```
Degree of the normal closure N of K is 168
Is G isomorphic to PGL_3(F_2):  true Homomorphism of GrpPerm: G, Degree 8, Order
2^3 * 3 * 7 into GrpPerm: G0, Degree 7, Order 2^3 * 3 * 7 induced by
    (1, 6)(2, 4)(3, 7)(5, 8) |--> (2, 6)(4, 5)
    (1, 4, 8, 2)(3, 6, 5, 7) |--> (1, 6)(2, 4, 3, 7)
Is H_1 conjugate to H_2 inside G:  false
The group H_1 corresponds to the field extensions:  y^7 + 6*x^8*y^3 +
    alpha^28*x^12*y + 4
((((x1 + x4) + x6) + x8)^2 + (((x2 + x3) + x5) + x7)^2)
The group H_2 corresponds to the field extensions:  y^7 + 5*x^8*y^3 +
    alpha^4*x^12*y + 6
((((x1 + x5)^2 + (x6 + x2)^2) + (x8 + x3)^2) + (x4 + x7)^2)
```

Let us also check that for instance fields K_1, K_1' from 3.6 indeed split equivalently. To do so we pick a few random prime ideals $\mathcal{P}$ in $\mathbb{F}_q[x]$ and compare factors of reductions of $y^7 + 2y^3 + 2y + 6x^2$ and $y^7 + y^3 + 5y + 4x^2$ modulo $\mathcal{P}$:

```
p := 7;
Fq := GF(p);
k<x> := RationalFunctionField(Fq);

for i in [1..10] do
  P := RandomIrreduciblePolynomial(Fq, i);
  R<x> := ExtensionField<k, x | P>;
  RR<y> := PolynomialRing(R);
  f := y^7 + 2*y^3 + 2*y + 6*x^2;
  g := y^7 + y^3 + 5*y + 4*x^2;
  "Factorization of f mod", P, Factorization(f);
  "Factorization of g mod", P, Factorization(g);
end for;
```

The above code confirms that indeed at least for some randomly chosen primes $\mathcal{P}$ there exists a degree preserving bijection between ideals of $\mathcal{O}_{K_1}$ lying above $\mathcal{P}$ to those ideals of $\mathcal{O}_{K_1'}$:

```
...
Factorization of f mod x^2 + 5*x + 3
[
    <y + 6*x + 5, 1>,
    <y^3 + (3*x + 6)*y^2 + 4*x*y + 4, 1>,
    <y^3 + (5*x + 3)*y^2 + 3*x*y + 4, 1>
]
Factorization of g mod x^2 + 5*x + 3
[
    <y + 3*x + 6, 1>,
    <y^3 + (5*x + 3)*y^2 + (x + 5)*y + x + 6, 1>,
    <y^3 + (6*x + 5)*y^2 + (6*x + 2)*y + x + 6, 1>
]
Factorization of f mod x^3 + 4*x^2 + 4*x + 6
[
    <y^7 + 2*y^3 + 2*y + 6*x^2, 1>
]
Factorization of g mod x^3 + 4*x^2 + 4*x + 6
[
    <y^7 + y^3 + 5*y + 4*x^2, 1>
]
...
```

Construction by Torsion Points on Elliptic Curves

All the above examples work only for some particular characteristic p of the base field. Moreover, for any example of non-isomorphic Gassmann equivalent pair (K, K') given above fields K and K' actually become isomorphic after a constant field extension. It means that corresponding curves X and Y are twists of each other. In this section we discuss an algorithm to construct examples of families of pairs of arithmetically equivalent global function fields of arbitrary characteristic p of the ground field, provided p is greater than three. By using this approach we found geometrically non-isomorphic arithmetically equivalent global fields.

Let l denote a prime number. As it follows from [5] that extensions with Galois group $G \simeq \mathrm{Gl}_2(\mathbb{F}_l)$ play an important role in the construction of arithmetically equivalent fields. If E is an ordinary elliptic curve defined over $\mathbb{Q}$, then the group $E[l]$ of l-torsion points of E allows us to construct arithmetically equivalent number fields, as in [9]. But in contrast to the number field case, in the function field settings torsion points on elliptic curves over $\mathbb{F}_q(t)$ do not always allow to construct extensions with Galois group isomorphic to $\mathrm{Gl}_2(\mathbb{F}_l)$. The crucial difference appears because of constant field extensions.

More concretely, consider the function field F of the projective line defined over $\mathbb{F}_q$: $F \simeq \mathbb{F}_q(t)$, where $q = p^m$, p is prime. Suppose for simplicity that $p > 3$ and pick parameters a, $b \in \mathbb{F}_q[t]$. Consider an elliptic curve E over F defined by the equation $y^2 = x^3 + ax + b$. For any prime number $l \neq p$ let us consider $\phi_{l,E}(u)$ the l-division polynomial of E. This is a polynomial with coefficients in F and with roots corresponding to x-coordinates of l-torsion points of the elliptic curve E, for example:

$$\phi_{3,E}(u) = 3u^4 + au^2 + 12bu - a^2.$$

Finally, let $R(t, y) = \mathrm{Res}_x(\phi_{l,E}(x), y^2 - (x^3 + ax + b))$ be the resultant with respect to x. This is a polynomial in t and y, whose roots correspond to the coordinates of l-torsion points of E. Generically this is separable polynomial and it generates the finite field extension $K(y)$ of $\mathbb{F}_q(t)$: $K(y) = \frac{\mathbb{F}_q(t)[y]}{(R(t,y))}$. We will denote the Galois group of the normal closure of K over F by G. Let H be the subgroup of $\mathbb{F}_l^\times$ generated by q. The analogue of the so-called *Serre's open image Theorem* for function fields proved by Igusa in 1959 states that for big enough l depending on q we have the following exact sequence, see [3]:

$$1 \to \mathrm{SL}_2(\mathbb{F}_l) \to G \to H \to 1.$$

Moreover, in this sequence $\mathrm{SL}_2(\mathbb{F}_l)$ corresponds to the geometric extension of F and H corresponds to the constant field extension. If $q = 1 \mod l$ then H is trivial and we obtain a geometric extension with $G \simeq \mathrm{SL}_2(\mathbb{F}_l)$. By taking a quotient of G by ± 1, we will get $\mathrm{PSL}_2(\mathbb{F}_l)$. The action of ± 1 is given by gluing points with the same x-coordinate. Therefore, the splitting field of $\phi_{l,E}(x)$ is the geometric extension of $\mathbb{F}_q(t)$ with Galois group $\mathrm{PSL}_2(\mathbb{F}_l)$. Now if $l = 7$ or $l = 11$ we obtain a family of arithmetically equivalent pairs.

Example 3.8. *In the above settings let $p = 29$ and $l = 7$, $a = t$, $b = t + 1$. Then: $\phi_{7,E}(x)$ is a polynomial of degree 24. The splitting field of $\phi_{7,E}(x)$ is a finite geometric extension $K/\mathbb{F}_{29}(t)$ with the Galois group isomorphic to $\mathrm{PSL}_2(\mathbb{F}_7)$. Inside this normal closure following two arithmetically equivalent fields are not isomorphic:*

$$K[x]/(x^7 + 20tx^6 + 14t^2x^5 + (6t^3 + 11t^2 + 22t + 11)x^4 + (5t^4 + 23t^3 + 17t^2 + 23t)x^3+$$
$$+(20t^5 + 13t^4 + 26t^3 + 13t^2)x^2 + (5t^6 + 20t^5 + 5t^3 + 21t^2 + 14t + 18)x+$$
$$+23t^7 + 26t^6 + 19t^5 + 10t^4 + 5t^3 + 13t^2 + 25t)$$

and

$$K[x]/(x^7 + 16tx^6 + 2t^2x^5 + (18t^3 + 10t^2 + 20t + 10)x^4 + (27t^4 + 3t^3 + 6t^2 + 3t)x^3+$$
$$+(27t^5 + 17t^4 + 5t^3 + 17t^2)x^2 + (t^6 + 7t^5 + 16t^4 + 15t^3 + 12t^2 + 8t + 2)x+$$
$$+28t^7 + t^6 + 2t^5 + t^4).$$

According to Magma function fields given above have genus 1 and a $\mathbb{F}_{29}$-rational point, therefore they are isomorphic to the function fields of two elliptic curves. Those elliptic curves have different j-invariant, namely 16 and 15 respectively. Therefore, they are geometrically non-isomorphic.

3.3.2 Properties of Arithmetically Equivalent Fields

In this section we will briefly discuss common properties of arithmetically equivalent global fields that will shed some light on the previous examples. Recall the statement 1.18 from the introduction:

Lemma 3.9. *Let G be a finite group and $H \subset G$ a subgroup of index n. Suppose one of the following conditions holds:*

1. *$n \leq 6$;*
2. *H is cyclic;*
3. *$G = \mathbb{S}_n$ the full symmetric group of order n;*
4. *$n = p$ is prime and $G = \mathbb{A}_p$ is the alternating group of order p.*

then any Gassmann triple (G, H, H') is trivial.

Taking into account our main Theorem this statement has the following application to the function field side:

Corollary 3.10. *Let K be a finite separable geometric extension of $\mathbb{F}_q(t)$ of degree n and let N be its Galois closure with Galois group G. Let H be a subgroup of G such that $K = N^H$. Suppose one of the conditions from the previous lemma holds. Let $H' \subset G$ be a subgroup and let $K' = N^{H'}$. Fields K and K' are isomorphic if and only if for each irreducible representation ρ of G we have $L_K(\rho|_H) = L_{K'}(\rho|_{H'})$.*

Adele Rings

Let K be a global field and let A_K denote the Adele ring of K. By definition this is the restricted product of all local completions K_v with respect to $\mathcal{O}_v$, where v denotes a place of K. It has a topology coming from restricted product and therefore it is a topological abelian group.

The first remarkable fact is that in the number field case we have the following implications: $A_K \simeq A_L \Rightarrow \zeta_K = \zeta_L \iff K$ and L arithmetically equivalent. And moreover there exists an example of arithmetically equivalent number fields with non-isomorphic Adele rings, see [44].

On the other hand in the function field side we have the following: $A_K \simeq A_L \iff \zeta_K = \zeta_L \Leftarrow K$ and L arithmetically equivalent. For the proof of equivalence see [55]. Roughly speaking the reason here is that in the function fields case the isomorphism type of the local completion $\mathcal{O}_v$ depends only on the degree of v. For number fields this is not the case.

Ideal Class Group

Arithmetically equivalent function fields share the same zeta-function and therefore they also share the same class-number. Indeed the by the analogue of the class-number formula the order of the class group is given as $L(0)$ where $\zeta_K(s) = \frac{L(s)}{(1-q^{-s})(1-q^{1-s})}$. But their class-groups may be different, as in example [3.6]. Nevertheless exactly as in the number field case we have a Perlis invariant v associated to each Gassmann-triple (G, H, H') . In the function field case also for any prime number $l \neq p$ co-prime to v one has:

$$\mathrm{Cl}_l(K) \simeq \mathrm{Cl}_l(K').$$

In order to see this one could replace word-by-word the construction from the number field case, but probably a slightly more interesting approach is the following taken from [22]. Recall that the class-group is by definition the group of $\mathbb{F}_q$-rational points on the Jacobian $\mathrm{Jac}(X)$ associated to X. Now, to each relation between induced representations of trivial characters one associates isogeny relations between Jacobians of corresponding curves. In the case of Gassmann equivalence one has $\mathrm{Ind}_H^G 1 \simeq \mathrm{Ind}_{H'}^G 1$ which leads to isogenies between Jacobians of corresponding curves X, X'. Degrees of these isogenies are given in terms of the triple (G, H, H') and closely related to the invariant v. This shows that if l is co-prime to v then there exists an isogeny from $\mathrm{Jac}(X)$ to $\mathrm{Jac}(X')$ of degree co-prime to l which leads to the isomorphism of l-parts of class groups.

3.4 On Monomial Representations

The main purpose of this section is to prove Theorem 2.6. Before doing that let us recall some basic facts from the theory of induced representations. Let G be a finite group and H a subgroup. Let χ be a one-dimensional representation of H. Consider the induced representation ψ of G: $\psi = \mathrm{Ind}_H^G \chi$. By definition ψ acts on the vector space V which could be associated with the direct sum of lines $\oplus \mathbb{C}_{g_i}$ where each $\mathbb{C}_{g_i}$ corresponds to the i-th left coset G/H. Such a pair $(\psi, \oplus \mathbb{C}_{g_i})$ is called a *monomial representation.* Let H' be another subgroup of G and $\psi' = \mathrm{Ind}_{H'}^G \chi'$ for one-dimensional χ' of H'. We will say that we have morphism of pairs

$(\psi, \oplus\mathbb{C}_{g_i})$, $(\psi', \oplus\mathbb{C}_{g'_j})$ if we have a morphism of representations f: $\psi \to \psi'$ such that for each line $\mathbb{C}_{g_i}$ we have $f(\mathbb{C}_{g_i}) \subset \mathbb{C}_{g'_j}$ for some j.

Lemma 3.11. *Suppose we have an isomorphism of monomial representations $(\psi, \oplus\mathbb{C}_{g_i}) \simeq (\psi', \oplus\mathbb{C}_{g'_j})$. Then H is a conjugate of H' in G.*

Proof. For the reference see [16]. □

Example 3.12. *Let G be the group of multiplicative quaternions with generators a and b. Consider the subgroups $H_a = \{1, a, -1, -a\}$ and $H_b = \{1, b, -1, -b\}$. Let χ_a be an isomorphism $H_a \simeq \mu_4^*$ sending element a to i. Let χ_b be the same character for H_b. Then one has $\mathrm{Ind}_{H_a}^G \chi_a \simeq \mathrm{Ind}_{H_b}^G \chi_b$ as representations, but not as monomial representations.*

Let us recall settings for Theorem 2.6. Let G be a finite group and H a subgroup of index n and $C_l = \mu_l$ be a cyclic group of order l, where l is an odd prime. Let us consider semi-direct products $\tilde{G} = C_l^n \rtimes G$ and $\tilde{H} = C_l^n \rtimes H$, where G acts on C_l^n by permuting its component as cosets G/H. Let $g_1, \ldots, g_n$ be representatives of left cosets $G = \cup_i g_i H$. Without loss of generality we assume that $g_1 = e$ is the identity element. Note that g_i for $i \neq 1$ cannot fix the first coset. We define χ to be the homomorphism from $\tilde{H} \to \mu_l$, sending an element $(c_1, \ldots, c_n, g)$ to c_1. This is indeed a homomorphism, since H fixes the first coset. Then the following is true:

Theorem 3.13 (Bart de Smit). *For any subgroup $\tilde{H}' \subset \tilde{G}$ and any abelian character $\chi' : \tilde{H}' \to \mathbb{C}^*$ if $\mathrm{Ind}_{\tilde{H}'}^{\tilde{G}}(\chi') \simeq \mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi)$ then $\tilde{H}'$ and $\tilde{H}$ are conjugate in $\tilde{G}$.*

Proof. **Step 1.** Consider cosets $\tilde{G}/\tilde{H}$. We claim that each such coset for $i > 1$ can be represented as $\gamma_i = (1, 1, \ldots, 1, g_i)$, where $g_i \in G/H$. This is true since elements of the form $(\zeta_1, \zeta_2, \ldots, \zeta_n, 1)$ are in $\tilde{H}$, where $(\zeta_1, \zeta_2, \ldots, \zeta_n) \in C_l^n$.

Step 2. Let us consider element $\alpha = (\zeta, 1, \ldots, 1, \ldots, 1) \in \tilde{H}$ where $\zeta \in \mu_l$, $\zeta \neq 1$ is in the first position. Such element fixes each coset $\gamma_i \tilde{H}$. Therefore if $\psi = \mathrm{Ind}_{\tilde{H}}^{\tilde{G}}(\chi)$ then $\psi(\alpha)$ is a diagonal matrix with l-th roots of unity on the diagonal. Moreover, it is the matrix with the first element is ζ on the diagonal and each other diagonal element equals to one. Indeed, by definition of induced representation on the i-th position we have $\chi(\gamma_i^{-1}\alpha\gamma_i)$ and it is easy to see that $\gamma_i^{-1}\alpha\gamma_i$ has 1 on the first position, provided $i \neq 1$.

Step 3. We claim that $\psi'(\alpha_i)$ is also a diagonal matrix, where $\psi' = \mathrm{Ind}_{\tilde{H}'}^{\tilde{G}}(\chi')$. We know that this is a matrix with exactly one non-zero element in each row and column. Suppose it is not a diagonal, therefore it changes at least two elements and hence trace of this matrix is $\sum_{k=1}^{n-2} \zeta_i$, where ζ_i are roots of unity. Since $\psi \simeq \psi'$ we have $n - 1 + \zeta = \sum_{k=1}^{n-2} \zeta_i$, which can't be true since the absolute value of the left hand side is strictly bigger than $n - 2$. Here we use the fact that $l > 2$ and therefore $\zeta \neq \pm 1$.

Step 4. Let A be an isomorphism of representations ψ and ψ'. We will show that it is *an isomorphism of monomial representations* $(\psi, \oplus\mathbb{C}_i) \simeq (\psi', \oplus\mathbb{C}_j)$. Indeed, it suffices to show that in the given basis A is written as permutation matrix. Suppose it is not and therefore we have at least two non-zero elements in one columm. Also it has another non-zero element in some of those two rows, otherwise $\det(A)$ must be zero which is not since A is an isomorphism. We have $A\psi(\alpha) = \psi'(\alpha)A$ which is easy to calculate since $\psi(\alpha)$ and $\psi'(\alpha)$ are diagonal. By comparing elements from left and right hand sides one has $\zeta = 1$ which leads to the contradiction. □

3.5 The Proof of Theorem 3.3

In this section we will prove Theorem [3.3]. We will denote by F the rational function field with the base field $\mathbb{F}_q$: $F = \mathbb{F}_q(t)$, where $q = p^m$, p is prime. It is enough to show that for any separable geometric extension K of F of degree n, with extension N of K, N normal over F and Galois Groups $G = \mathrm{Gal}(N/F)$ and $H = \mathrm{Gal}(N/K)$ there exist an odd prime l and Galois extension M over F with $\mathrm{Gal}(M/F) \simeq C_l^n \rtimes G$ and $\mathrm{Gal}(M/K) = C_l^n \rtimes H$, where G acts on components of C_l^n by permuting them as cosets G/H. We will prove this statement in a few steps.

The Chebotarev density Theorem for function fields see [42] theorem[9.13B], insures us that for any sufficiently large number T we could find a prime $\mathfrak{p}$ of F which has degree T and splits completely in N. Note that if prime splits completely in N then it also splits completely in K. Now, we pick an odd prime number l co-prime to the characteristic p, to $q-1$, to the order of G and to the class number h_K of K. Then we pick a large enough number T divisible by $(l-1)$. Finally we pick a prime $\mathfrak{p}$ of F of degree T which splits completely in N. Let $\mathfrak{b}_\mathfrak{1}, \ldots, \mathfrak{b}_\mathfrak{n}$ denote primes of K lying above it. We have:

Lemma 3.14. *In the above settings there exists cyclic ramified extension L_l of K of degree l ramifing only at $\mathfrak{b}_\mathfrak{1}$.*

Proof. Consider the modulus $\mathfrak{m} = \mathfrak{b}_\mathfrak{1}$ and associated ray class group $\mathrm{Cl}_\mathfrak{m}(K)$. We will show this group has a subgroup of order l. Let $\mathcal{O}_K$ denotes the ring of integers of K with respect to the field extension K/F. Class field theory shows that we have the following exact sequence of abelian groups:

$$0 \to \mathbb{F}_q^* \to (\mathcal{O}_K/\mathfrak{m})^* \to \mathrm{Cl}_\mathfrak{m}(K) \to \mathrm{Cl}(K) \to 0,$$

We claim that $\mathrm{Cl}_\mathfrak{m}(K)$ contains a subgroup of order l and since l is prime to the order of $\mathrm{Cl}(K)$ the fixed field corresponding to this subgroup is ramified at $\mathfrak{b}_\mathfrak{1}$.

Indeed the order of $(\mathcal{O}_K/\mathfrak{m})^*$ is $N(\mathfrak{b}_1) - 1 = q^T - 1$, where $N(\mathfrak{a})$ denotes the norm of an ideal $\mathfrak{a}$. Since T is divisible by $(l-1)$ this quantity is divisible by l. It follows that the order of $\mathrm{Cl}_m(K)$ is divisible by l and therefore we have a cyclic extension of K of degree l which ramifies only at $\mathfrak{b}_1$. □

The next step is to take the common normal closure M of N and L_l.

Lemma 3.15. *The Galois group $\mathrm{Gal}(M/F)$ of the common normal closure M of N and L_l over F is $C_l^n \rtimes G$.*

Proof. By construction N is normal over F and $K = N^H$. Consider the set $\mathrm{Hom}(K, N)$ of all embeddings of K into N. This has an action of G on it isomorphic to the action of G on G/H. For each element $\sigma_i \in \mathrm{Hom}(K, N)$ consider the field K^{σ_i} and corresponding cyclic extension $L^{\sigma_i} = L \otimes_{K^{\sigma_i}} N$. We claim that the composites NL^{σ_i} are linearly disjoint over N when σ_i runs over the set $\mathrm{Hom}(K, N)$. Indeed, consider the set of primes of N which lie over $\mathfrak{p}$ and ramify in the composite NL^{σ_i} over N. Since $H^{\sigma_i} = \mathrm{Gal}(M/K^{\sigma_i})$ fixes K^{σ_i} this set is invariant under the action of H^{σ_i} and not invariant under the action of g for each $g \in G$, $g \notin H^{\sigma_i}$. Hence all NL^{σ_i} ramifies in different primes of N lying above $\mathfrak{p}$. Therefore we have n disjoint C_l-extensions

NL^{σ_i}/N in M and G permutes them as cosets G/H. It follows that we have the following exact sequence:

$$1 \to C_l^n \to \mathrm{Gal}(M/F) \to G \to 1$$

Since the order of G is co-prime to l, by the Schur–Zassenhaus theorem see [43], we have a section from $\gamma : G \to \mathrm{Gal}(M/F)$ which means that this sequence splits and $\mathrm{Gal}(M/F) \simeq C_l^n \rtimes G$ as desired.

□