Global fields and their L-functions

Solomatin, P.

Author: Solomatin, P.
Title: Global field and their L-functions
Issue Date: 2021-03-02

Part III

Isomorphism Classes of Maximal Abelian Quotients of Absolute Galois Groups

Chapter 5

On Abelianized Absolute Galois Groups of Global Function Fields

5.1 Introduction

As we mentioned in the first chapter the famous theorem of Uchida [57] states that the isomorphism class of a global function field K is determined by the isomorphism class of the absolute Galois group $\mathcal{G}_K = \mathrm{Gal}(K^{sep} : K)$ considered as topological group. One of the essential steps in the Uchida's proof is to recover from $\mathcal{G}_K$ its abelian part $\mathcal{G}_K^{ab}$ with some additional data, like decomposition and inertia subgroups. The following questions are natural to ask: what kind of information can one recover from the isomorphism class of the pro-finite abelian group $\mathcal{G}_K^{ab}$? More concretely, does the abelian part of the absolute Galois group determine the global function field K up to isomorphism? If not, which function fields share the same isomorphism class of $\mathcal{G}_K^{ab}$?

For a global function field K of characteristic p with exact constant field $\mathbb{F}_q$, $q = p^n$ we define the invariant d_K as the natural number such that $n = p^k d_K$ with $\gcd(d_K, p) = 1$, $k \in \mathbb{Z}_{\geq 0}$. Let $\mathrm{Cl}^0(K)$ denotes the degree zero part of the class-group of K. In other words, $\mathrm{Cl}^0(K)$ is the abelian group of $\mathbb{F}_q$-rational points of the Jacobian variety associated to the curve X. For any abelian group A and a prime number l we denote by A_l its l-part: $A_l = A \otimes \mathbb{Z}_l$, where $\mathbb{Z}_l$ denotes the ring of l-adic integers. We also denote by $A_{\text{non-}l}$ the non-l part of $A:$ $A_{\text{non-}l} = A/A_l$. The main purpose of this chapter is to prove the following result:

Theorem 5.1. *Suppose K and K' are two global function fields. Then $\mathcal{G}_K^{ab} \simeq \mathcal{G}_{K'}^{ab}$ as pro-finite groups if and only if the following three conditions hold:*

1. *K and K' share the same characteristic p;*
2. *Invariants d_K and $d_{K'}$ coincide: $d_K = d_{K'}$;*
3. *The non p-parts of class-groups of K and K' are isomorphic:*

$$\mathrm{Cl}^0_{\textit{non-p}}(K) \simeq \mathrm{Cl}^0_{\textit{non-p}}(K').$$

In particular, two function fields with the same field of constants $\mathbb{F}_q$ have isomorphic $\mathcal{G}_K^{ab}$ if and only if they have isomorphic $\mathrm{Cl}^0_{\textit{non-p}}(K)$.

The proof of Theorem 5.1 includes explicit reconstruction of the invariants p, d_K and $\mathrm{Cl}^0_{\text{non-}p}(K)$ from $\mathcal{G}_K^{ab}$. More concretely, let $s_l(\mathcal{G}_K^{ab})$ be the least integer k such that $\mathcal{G}_K^{ab}$ has direct summand of the form $\mathbb{Z}/l^k\mathbb{Z}$ and let $p^\star$ denotes $(-1)^{\frac{p-1}{2}}p$ if p is odd and p otherwise, then:

Theorem 5.2. *Given the isomorphism class of the topological group $\mathcal{G}_K^{ab}$ we have:*

1. *The characteristic of K is the unique prime p such $\mathcal{G}_K^{ab}$ has no elements of order p;*
2. *The non-p part $\mathrm{Cl}^0_{\text{non-}p}(K)$ of the class-groups of K is isomorphic to the torsion of the quotient $\mathcal{G}_K^{ab}/\overline{\mathcal{G}_K^{ab}[\mathrm{tors}]}$, where $\overline{\mathcal{G}_K^{ab}[\mathrm{tors}]}$ denotes the closure of the torsion subgroup of $\mathcal{G}_K^{ab}$:*
$$\mathrm{Cl}^0_{\text{non-}p}(K) \simeq (\mathcal{G}_K^{ab}/\overline{\mathcal{G}_K^{ab}[\mathrm{tors}]})[\mathrm{tors}].$$
3. *The natural number d_K is the unique number co-prime to p such that for any prime number $l \neq p$:*
$$\mathrm{ord}_l(d_K) = \begin{cases} 0, & \text{if } l = 2 \text{ and } s_2(\mathcal{G}_K^{ab}) = 1; \\ s_l(\mathcal{G}_K^{ab}) - \mathrm{ord}_l((p^\star)^{l-1} - 1), & \text{otherwise.} \end{cases}$$

Proof. See corollaries 5.12 and 5.13. □

By using these theorems we will establish the following:

Corollary 5.3. *Let K be the rational function field (with genus zero) over a fixed constant field $\mathbb{F}_q$ and let E be an elliptic function field (with genus one) defined over the same constant field, such that[1] $\#\,\mathrm{Cl}^0(E) = q$. Then there exists isomorphism of topological groups $\mathcal{G}_K^{ab} \simeq \mathcal{G}_E^{ab}$.*

This corollary provides some answers to the above questions. For example, it follows that for every q there exists a pair of function fields K, K' over $\mathbb{F}_q$ with $g(K) = 0$, $g(K') = 1$ and $\mathcal{G}_K^{ab} \simeq \mathcal{G}_{K'}^{ab}$. In particular, the genus g_K of K and therefore the Dedekind zeta-function $\zeta_K(s)$ of K are not determined by the isomorphism class of $\mathcal{G}_K^{ab}$ even if the constant field $\mathbb{F}_q$ is fixed. The above example also shows that:

Corollary 5.4. *For every p there exist infinitely many pairwise non-isomorphic function fields K of characteristic p with isomorphic $\mathcal{G}_K^{ab}$.*

Proof. Fix a prime number p and let $q = p^{p^k}$, where k is a non-negative integer. Let F_k and E_k denote rational and elliptic function fields from the previous example with exact constant field $\mathbb{F}_q$. Then, according to the our main theorem for any non-negative integers k, l we have: $\mathcal{G}_{K_l}^{ab} \simeq \mathcal{G}_{E_k}^{ab}$. □

Applying some classical results about the two-part of $\mathrm{Cl}^0(K)$ of hyper-elliptic function fields we will also show that:

[1] the existence of such field is guaranteed by the Waterhouse theorem, see section 5.4.

Corollary 5.5. *For any given q with $p > 2$ infinitely many distinct isomorphism types of $\mathcal{G}_K^{ab}$ occur for function fields with exact constant field $\mathbb{F}_q$.*

Proof. See theorem 5.42 from the last section. □

Unfortunately, the answer to the question about distribution of global fields over fixed constant field $\mathbb{F}_q$ sharing the same $\mathcal{G}_K^{ab}$ is not clear at the moment, since we don't know if there are infinitely many such fields with a given non p-part of the class group. In particular, it seems to be reasonable to state the following **conjecture:** *there are infinitely many curves defined over fixed finite field $\mathbb{F}_q$, $q = p^n$ with order of the group of $\mathbb{F}_q$-rational points of the Jacobian varieties associated to them to be a power of p.* If the conjecture is true then what is the proportion of such curves, say as q fixed and g tends to infinity?

The main idea towards our result was inspired by the work [1], where authors produced an elegant description for the isomorphism class of the topological group $\mathcal{G}_K^{ab}$, where K denotes *imaginary quadratic number field.* But note also that there are many completely different technical details, which point in a different direction.

This chapter has the following structure: in the next section we will sketch the proof of Theorem 5.1. Then we prove all the necessarily lemmas in the section 5.3. Finally, we will discuss the question about construction of non-isomorphic function fields with isomorphic and non-isomorphic abelian parts of their absolute Galois groups and prove corollaries 5.3, 5.4 and 5.5.

5.2 Outline of the Proof

Global class field theory provides an internal description of the abelian part of the absolute Galois group of a global or local field K in terms of arithmetic objects associated to K. We will use the *idèle*-theoretical approach: see section 5.3.2 for details and the classical books [36], [59], [2] for complete discussion. For a given global function field K we denote by $\mathcal{I}_K$ the group of idèles of K and by $\mathcal{C}_K$ the *idèle class-group of* K, i.e. the quotient group of $\mathcal{I}_K$ by the multiplicative group $K^\times$. Recall that we have a split exact sequence:

$$0 \to \mathcal{C}_K^0 \to \mathcal{C}_K \xrightarrow{\deg} \mathbb{Z} \to 0,$$

where $\mathcal{C}_K^0$ is the degree zero part of the idèle class group and the map from $\mathcal{C}_K$ to $\mathbb{Z}$ is the degree map.

Theorem 5.6 (The Main Theorem of Class Field Theory for Global Function FIelds)**.** *In the above settings there exists an isomorphism of topological groups: $\mathcal{C}_K^0 \oplus \widehat{\mathbb{Z}} \simeq G_K^{ab}$.*

Proof. See section 5.3.2. □

We will show that $\mathcal{G}_K^{ab} \simeq \mathcal{G}_{K'}^{ab}$ if and only if $\mathcal{C}_K^0 \simeq \mathcal{C}_{K'}^0$. The key ingredient in the our proof is Pontryagin duality for locally compact abelian groups, which allows us to reduce question about pro-finite abelian groups to the question about discrete torsion groups.

Lemma 5.7. *Let A and B be two pro-finite abelian groups. If $A \oplus \widehat{\mathbb{Z}} \simeq B \oplus \widehat{\mathbb{Z}}$ then $A \simeq B$ in the category of pro-finite abelian groups.*

Proof. See section 5.3.1. □

This lemma reduces our question to the description of $\mathcal{C}_K^0$ as a topological group. Let v denote a place of K and K_v, $\mathcal{O}_v$ denotes the corresponding completion and its ring of integers respectively. Then we derive the following exact sequence.

Lemma 5.8. *There exists an exact sequence of topological groups, where the finite groups have the discrete topology:*

$$1 \to \mathbb{F}_q^\times \to \prod_v \mathcal{O}_v^\times \to \mathcal{C}_K^0 \to \mathrm{Cl}^0(K) \to 1.$$

Proof. See section 5.3.3. □

For the next step we recall in lemma 5.17 the isomorphism $\mathcal{O}_v^\times \simeq \mathbb{F}_{q^n}^\times \times \mathbb{Z}_p^\infty$, where n is the degree of a place v and $\mathbb{Z}_p$ denotes the group of p-adic integers. Denoting by $\mathcal{T}_K$ the group $(\prod_v \mathbb{F}_{q^{\deg(v)}}^\times)/\mathbb{F}_q^\times$ we will get the following exact sequence, see section 5.3.3:

$$1 \to \mathcal{T}_K \times \mathbb{Z}_p^\infty \to \mathcal{C}_K^0 \to \mathrm{Cl}^0(K) \to 1 \tag{5.1}$$

There are two crucial observations about this sequence. First we will prove the following structure theorem for the group $\mathcal{T}_K$:

Theorem 5.9. *Given a function field K with exact constant field $\mathbb{F}_q$, where $q = p^n$ there exists an isomorphism $\mathcal{T}_K \simeq \prod_{l,m}(\mathbb{Z}/l^m\mathbb{Z})^{a_{l,m}}$, where the product is taken over all prime numbers l and all positive integers m and $a_{l,m}$ denotes a finite or countable cardinal number. Moreover, the coefficients $a_{l,m}$ depend only on q and the following holds:*

1. *Each $a_{l,m}$ is either zero or the infinite countable cardinal;*
2. *For $l = p$ we have $a_{p,m} = 0$ for all m;*
3. *For $l \neq p$, $l \neq 2$ there exists a unique non-negative integer $N_q(l)$ such that $a_{l,m}$ is infinite if and only if $m \geq N_q(l)$;*
4. *For $p \neq 2$ and $l = 2$ there exists a unique non-negative integer $N_q(2)$ such that for $q = 1 \mod 4$ we have $a_{2,m}$ is infinite if and only if $m \geq N_q(2)$, and for $q = 3 \mod 4$ we have $a_{2,m}$ is infinite if and only if $m = 1$ or $m \geq N_q(2)$;*
5. *Given two prime powers q_1, q_2 the numbers $N_{q_1}(l)$ and $N_{q_2}(l)$ coincide for all l if and only if $q_1 = p^{n_1}$, $q_2 = p^{n_2}$ with $\frac{n_1}{n_2} = p^m$, for some integer m.*

Proof. See section 5.3.4. For expression of $N_q(l)$ see lemma 5.21 and lemma 5.22. □

Definition 5.10. *The exact sequence of abelian groups $0 \to A \to B \xrightarrow{\psi} C \to 0$ is called* totally non-split *if there is no non-trivial subgroup S of C such that the sequence $0 \to A \to \psi^{-1}(S) \to S \to 0$ splits.*

The second observation about 5.1 is the key point in the our proof.

Theorem 5.11. *All torsion elements of $\mathcal{C}^0_K$ are in $\mathcal{T}_K$. Therefore the exact sequence 5.1 is totally non-split. Moreover, the topological closure of the torsion subgroup of $\mathcal{C}^0_K$ is $\mathcal{T}_K$: $\overline{\mathcal{C}^0_K[\mathrm{tors}]} = \mathcal{T}_K$.*

Proof. See section 5.3.5. □

Because of the description of $\mathcal{T}_K$ this theorem gives us:

Corollary 5.12. *If $\mathcal{G}^{ab}_K \simeq \mathcal{G}^{ab}_{K'}$ as pro-finite groups then $\mathcal{T}_K \simeq \mathcal{T}_{K'}$, in particular the characteristic p and the invariant d_K are determined by the isomorphism class of $\mathcal{G}^{ab}_K$.*

Proof. Since $\mathcal{G}^{ab}_K \simeq \mathcal{C}^0_K \oplus \widehat{\mathbb{Z}}$ and the group $\widehat{\mathbb{Z}}$ is torsion free, we have that $\mathcal{T}_K$ is also the closure of the torsion subgroup of $\mathcal{G}^{ab}_K$. Then theorem 5.9 shows that p is a unique prime such that this group has no elements of order p.

For the natural number d_K consider the torsion group $\mathcal{G}^{ab}_K[\mathrm{tors}]$. By Theorem 5.9 this group has direct summand of the form $\mathbb{Z}/l^k\mathbb{Z}$ for a fixed prime $l \neq p$ if and only if $k \geq N_q(l)$ or $l = 2$, $k = 1$, $p = 3 \mod 4$ and $d_K = 1 \mod 2$. In the proof of Theorem 5.9 we will show that $N_q(l) = \mathrm{ord}_l(d_K) + \mathrm{ord}_l((p^\star)^{l-1} - 1)$, where $p^\star = -p$ if $p = 3 \mod 4$ and $p^\star = p$ otherwise. Which implies the formula:

$$\mathrm{ord}_l(d_K) = \begin{cases} 0, & \text{if } l = 2 \text{ and } s_2 = 1 \\ s_l(\mathcal{G}^{ab}_K) - \mathrm{ord}_l((p^\star)^{l-1} - 1), & \text{otherwise.} \end{cases}$$

□

Since each pro-finite abelian group is isomorphic to the limit of finite abelian groups, by the Chinese remainder theorem it is also isomorphic to the product over prime numbers of its primary components. We will work with these components separately instead of working with the whole group. Keeping the same notation as for finite abelian groups, for any pro-finite abelian group G and a prime number l we denote by G_l the l-part of G: $G \otimes \mathbb{Z}_l$. Now let l be a prime number different from p, we have:

$$1 \to \mathcal{T}_{K,l} \to \mathcal{C}^0_{K,l} \to \mathrm{Cl}^0_l(K) \to 1.$$

Which shows that:

$$\mathrm{Cl}^0_l(K) \simeq \mathcal{C}^0_{K,l} / \overline{\mathcal{C}^0_{K,l}[\mathrm{tors}]}.$$

Corollary 5.13. *If $\mathcal{G}^{ab}_K \simeq \mathcal{G}^{ab}_{K'}$ as pro-finite groups then the non p-parts of the class-groups of K and K' are isomorphic: $\mathrm{Cl}^0_{\text{non-}p}(K) \simeq \mathrm{Cl}^0_{\text{non-}p}(K')$.*

Proof. We know that $\mathcal{G}^{ab}_K \simeq \mathcal{C}^0_K \oplus \widehat{\mathbb{Z}}$ and that $\mathcal{T}_K = \overline{\mathcal{G}^{ab}_K[\mathrm{tors}]}$. Considering the l-part we get:

$$\mathcal{G}^{ab}_{K,l} / \overline{\mathcal{G}^{ab}_{K,l}[\mathrm{tors}]} \simeq (\mathcal{C}^0_{K,l} / \mathcal{T}_{K,l}) \oplus \mathbb{Z}_l.$$

Since $\mathbb{Z}_l$ is torsion free, we have:

$$(\mathcal{G}^{ab}_{K,l} / \overline{\mathcal{G}^{ab}_{K,l}[\mathrm{tors}]})[\mathrm{tors}] \simeq \mathcal{C}^0_{K,l} / \mathcal{T}_{K,l} \simeq \mathrm{Cl}^0_l(K).$$

Finally, note that the p-part of the torsion group of $\mathcal{G}_K^{ab}$ is trivial and hence combining all primes l different from p we get:

$$\mathrm{Cl}^0_{\text{non-}p}(K) \simeq (\mathcal{G}_K^{ab}/\overline{\mathcal{G}_K^{ab}[\text{tors}]})[\text{tors}].$$

□

Proof of Theorem 5.1. The above two corollaries imply the only if part of Theorem 5.1. Now, we are going to discuss the question about the other implication. Our goal is to show that for a given isomorphism class of $\mathcal{T}_K$ and non p-part of the class group there is only one possibility for $\mathcal{C}_K^0$ to fit in the exact sequence 5.1.

Consider the p-part of the exact sequence 5.1:

$$1 \to \mathbb{Z}_p^\infty \to \mathcal{C}^0_{K,p} \to \mathrm{Cl}^0_p(K) \to 1.$$

By using the fact that this sequence is totally non-split we will show, see lemma 5.31 that this implies $\mathcal{C}^0_{K,p} \simeq \mathbb{Z}_p^\infty$, in particular the isomorphism type of $\mathcal{G}^{ab}_{K,p}$ *doesn't depend on* $\mathrm{Cl}^0_p(K)$.

We fix a prime number $l \neq p$ and consider the l-part which is of course also totally non-split:

$$1 \to \mathcal{T}_{K,l} \to \mathcal{C}^0_{K,l} \to \mathrm{Cl}^0_l(K) \to 1. \tag{5.2}$$

Obviously, if $\mathrm{Cl}^0_l(K) \simeq 0$ then $\mathcal{C}^0_{K,l} \simeq \mathcal{T}_{K,l}$. Our goal is to show that even if $\mathrm{Cl}^0_l(K)$ is not the trivial group then the isomorphism type of $\mathcal{C}^0_{K,l}$ is uniquely determined by isomorphism types of $\mathcal{T}_{K,l}$, $\mathrm{Cl}^0_l(K)$ and the fact that the exact sequence 5.2 is totally non-split.

In order to achieve our goal we need the following:

Theorem 5.14. *Let $\{C_i\}$ be a countable set of finite cyclic abelian l-groups with orders of C_i are not bounded as i tends to infinity and let A be any finite abelian l-group. Then up to isomorphism there exists a unique torsion abelian l-group B satisfying two following conditions:*

1. *There exists an exact sequence:* $1 \to A \to B \to \oplus_{i\geq 1} C_i \to 1$;
2. *A is the set of all divisible elements of B:* $A = \cap_{n\geq 1} nB$.

Proof. See section 5.3.6 □

Applying Pontryagin duality to the exact sequence 5.2 we get:

$$1 \leftarrow (\mathcal{T}_{K,l})^\vee \leftarrow (\mathcal{C}^0_{K,l})^\vee \leftarrow (\mathrm{Cl}^0_l(K))^\vee \leftarrow 1.$$

We will show in corollary 6.7 that this sequence dual to the sequence 5.2 satisfies conditions of Theorem 5.14 and therefore $(\mathcal{C}^0_{K,l})^\vee$ is uniquely determined. So its dual $\mathcal{C}^0_{K,l}$ is uniquely determined.

□

5.3 Proof of Lemmas

In this section we are going to prove all the results needed for our proof. Let us start from recalling some basic facts about pro-finite abelian groups. Standard references are [26] and [18].

5.3.1 Preliminaries

Let A be an abelian group. If this group is finitely generated then the structure theorem says that A is isomorphic to $\mathbb{Z}^r \oplus A_{\text{tors}}$ where r is a non-negative integer called rank and A_{tors} is a finite abelian group. Given two such groups we have that they are isomorphic if and only if their ranks are equal and torsion parts are isomorphic. The structure of an infinitely generated abelian group is more complicated. An element x of the abelian group A is *divisible* if for any $n \in \mathbb{N}$ there exists $y \in A$ such that $x = ny$. The group A is *divisible* if all its elements are divisible. For example $\mathbb{Q}$ is divisible. Another example is the so-called *Prüfer p-group* which is defined as union of all p^k roots of unity in $\mathbb{C}^\times$ for a fixed prime number p: $Z(p^\infty) = \{\zeta \in \mathbb{C}^\times | \zeta^{p^k} = 1, k \in \mathbb{N}\}$. Note that we have an isomorphism of abstract groups: $Z(p^\infty) \simeq \mathbb{Q}_p/\mathbb{Z}_p$, where $\mathbb{Q}_p$ denotes the abelian group of p-adic numbers and $\mathbb{Z}_p$ is a subgroup of all p-adic integers.

A group is called *reduced* if it has no non-zero divisible elements.

Lemma 5.15. *Each abelian group A contains a unique maximal divisible subgroup D and it is the direct sum of D and some reduced subgroup R: $A \simeq D \oplus R$.*

The structure of the divisible subgroup is clear.

Lemma 5.16. *Every divisible group D is isomorphic to a direct sum of copies of $\mathbb{Q}$ and $Z(p^\infty)$ for different prime numbers p.*

Proof. The proofs can be found in chapter 3 of [18]. □

The structure of the reduced part of A can be more complicated and usually involves the theory of Ulm invariants. In this chapter we will work with the reduced part directly not referring to the Ulm invariants at all.

Pontryagin Duality

We need to recall some properties of Pontryagin duality for locally compact abelian groups. A good reference including some historical discussion is [29]. Let $\mathbb{T}$ be the topological group $\mathbb{R}/\mathbb{Z}$ given with the quotient topology. If A is any locally compact abelian group then one considers Pontryagin dual $A^\vee$ of A which is the group of all *continuous homomorphisms* from A to $\mathbb{T}$:

$$A^\vee = \text{Hom}(A, \mathbb{T}).$$

This group has the so-called compact-open topology and is a topological, locally compact group. Here we list some properties of Pontryagin duality we use during the proof:

1. Pontryagin duality is a contra-variant functor from the category of locally compact abelian groups to itself;

2. If A is a finite abelian group with the discrete topology then $A^\vee \simeq A$ non-canonically;

3. We have the canonical isomorphism: $(A^\vee)^\vee \simeq A$;

4. Pontryagin dual of a pro-finite abelian group A is a discrete torsion group and vice versa;

5. Pontryagin duality sends direct products to direct sums and vice versa;

6. Pontryagin dual of $\mathbb{Z}_p$ is $Z(p^\infty)$ and dual of $\mathbb{Q}/\mathbb{Z}$ equipped with the discrete topology is the group of pro-finite integers $\widehat{\mathbb{Z}}$;

7. Pontryagin dual of a divisible group A is torsion free and vice versa.

Having stated this we are able to prove our lemmas.

Proof of Lemma 5.7. Let A and B be two pro-finite abelian groups such that $A\oplus\widehat{\mathbb{Z}} \simeq B\oplus\widehat{\mathbb{Z}}$. Applying Pontryagin duality to the above isomorphism we obtain:

$$(A)^\vee \oplus \mathbb{Q}/\mathbb{Z} \simeq (B)^\vee \oplus \mathbb{Q}/\mathbb{Z}.$$

By lemma 5.15 each abelian group is isomorphic to the direct sum of its reduced and divisible components. Using the fact that $\mathbb{Q}/\mathbb{Z}$ is divisible we have that reduced part of $(A)^\vee$ and $(B)^\vee$ are isomorphic. Now, according to the Lemma 5.16 the divisible part of $(A)^\vee \oplus \mathbb{Q}/\mathbb{Z}$ is a direct sum of copies of $\mathbb{Q}$ and $Z(p^\infty)$ and since $\mathbb{Q}/\mathbb{Z} \simeq \oplus_p Z(p^\infty)$ divisible parts of $(A)^\vee$ and $(B)^\vee$ are isomorphic. Therefore $(A)^\vee$ and $(B)^\vee$ are isomorphic and hence $A \simeq B$.

□

5.3.2 Class Field Theory

In this paragraph we briefly review the class field theory for global and local fields of positive characteristic.

The Case of Local Fields

We will start from the description of local aspects of the class field theory. Let L be a local field of positive characteristic $p > 0$. In other words L is a completion of a global function field K with respect to the discrete valuation associated to the place v of K. The field L is isomorphic to the field of Laurant series with constant field $\mathbb{F}_{q^n}$ and the corresponding ring of integers $\mathcal{O}_L$ is the ring of formal power series: $L \simeq \mathbb{F}_{q^n}((x))$, $\mathcal{O}_L \simeq \mathbb{F}_{q^n}[[x]]$. One way to construct abelian extensions of L is to take the algebraic closure $\overline{\mathbb{F}_{q^n}}$ of the constant field $\mathbb{F}_{q^n}$ which has Galois group $\mathrm{Gal}(\overline{\mathbb{F}_{q^n}} : \mathbb{F}_{q^n}) \simeq \widehat{\mathbb{Z}}$. This is the maximal unramified abelian extension of L.

Denoting by $I_L = \mathrm{Gal}^{ram}(L^{ab} : L)$ the inertia subgroup of $\mathcal{G}_L^{ab}$ we have the following split exact sequence:

$$1 \to I_L \to \mathcal{G}_L^{ab} \to \widehat{\mathbb{Z}} \to 1.$$

Recall that we also have the split exact sequence given via the valuation map:

$$1 \to \mathcal{O}_L^\times \to L^\times \to \mathbb{Z} \to 1.$$

The local Artin map: $L^\times \to \mathcal{G}_L^{ab}$ induces isomorphism of topological groups between the pro-finite completion $\widehat{L^\times}$ of $L^\times$ and $\mathcal{G}_L^{ab}$ such that two exact sequences are isomorphic:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \widehat{\mathcal{O}_L^\times} \simeq \mathcal{O}_L^\times & \longrightarrow & \widehat{L^\times} & \longrightarrow & \widehat{\mathbb{Z}} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & I_L & \longrightarrow & \mathcal{G}_L^{ab} & \longrightarrow & \mathrm{Gal}(\overline{\mathbb{F}_{q^n}} : \mathbb{F}_{q^n}) & \longrightarrow & 1
\end{array}$$

The Case of Global Fields

It is possible to give a similar description of $\mathcal{G}_K^{ab}$ in the case where K is a global function field via the so-called idèle-class group. First we note that for a global function field K there also exists the maximal unramified abelian extension M of K. The Galois group $\mathrm{Gal}(M:K)$ is isomorphic to the direct sum $\widehat{\mathbb{Z}} \oplus \mathrm{Gal}(H_K:K)$, where $\widehat{\mathbb{Z}}$ corresponds to the constant field extension and H_K is maximal unramified geometric extension of K. The Galois group $\mathrm{Gal}(H_K:K)$ is finite and one of the theorems of the class field theory establishes an isomorphism of abelian groups:

$$\mathrm{Gal}(H_K:K) \simeq \mathrm{Cl}^0(K),$$

where $\mathrm{Cl}^0(K)$ denotes the ideal class group of K.

Let $\mathcal{I}_K$ denotes the multiplicative group of idèles of K. This is the restricted direct product $\mathcal{I}_K = \prod'_v K_v^\times$, where the product is taken over places v of K with respect to $\mathcal{O}_v^\times$. One defines the basic open sets as $U = \prod'_v U_v$, where U_v open in $K_v^\times$ and for almost all v we have $U_v = \mathcal{O}_v^\times$. Under the topology generated by such U this becomes a topological group. The multiplicative group $K^\times$ is embedded to $\mathcal{I}_K$ diagonally as a discrete subgroup and the quotient $\mathcal{C}_K$ is the *idèle class group* of K. This is a topological group, but it is not pro-finite.

Proof of Theorem 5.6. One defines the global Artin map $\mathcal{C}_K \to \mathcal{G}_K^{ab}$. This map is injective, but not surjective. Similar to the local case it induces isomorphism of the pro-finite completion of $\mathcal{C}_K$ and $\mathcal{G}_K^{ab}$ as topological groups: $\widehat{\mathcal{C}_K} \simeq \mathcal{G}_K^{ab}$, see theorem 6, chapter 9 of [59].

Recall from the introduction that we have a split exact sequence:

$$0 \to \mathcal{C}_K^0 \to \mathcal{C}_K \xrightarrow{\deg} \mathbb{Z} \to 0,$$

where the map from $\mathcal{C}_K$ to $\mathbb{Z}$ is the degree map and $\mathcal{C}_K^0$ is the degree zero part of the idèle class group. We have that $\mathcal{C}_K^0$ is pro-finite, hence complete and therefore $\widehat{\mathcal{C}_K} \simeq \mathcal{C}_K^0 \oplus \widehat{\mathbb{Z}}$. □

5.3.3 Deriving the main exact sequence

Now our goal is to prove lemma 5.8. Let $\mathcal{I}_K^0$ be the group of degree zero idèles of K, i.e. means the kernel of the degree map from $\mathcal{I}_K$ to $\mathbb{Z}$. We have:

$$1 \to K^\times \to \mathcal{I}_K^0 \to \mathcal{C}_K^0 \to 1.$$

Let $\mathrm{Div}(K)$ denote the divisor group and let $\mathrm{Div}^0(K)$ be the subgroup of degree zero divisors. We also have the natural exact sequence, where $\mathbb{F}_q$ is exact field of constants of K:

$$1 \to \mathbb{F}_q^\times \to K^\times \to \mathrm{Div}^0(K) \to \mathrm{Cl}^0(K) \to 1.$$

There is a surjective homomorphism α of topological groups from $\mathcal{I}_K^0$ to $\mathcal{P}^0(K)$, sending an idèle $(a_{P_1}, a_{P_2}, \dots)$ to the divisor $\sum v_{P_i}(a_{P_i}) \cdot P_i$. This is well-defined since for a given idèle almost all $a_P \in \mathcal{O}_{v_P}^\times$. The kernel of this map is $\prod_v \mathcal{O}_v^\times$. Moreover, this map sends principal idèle to principal ideals and hence induces the surjective quotient map $\hat{\alpha}$ from $\mathcal{C}_K^0$ to $\mathrm{Cl}^0(K)$. We have the following snake-lemma diagram:

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & \mathbb{F}_q^\times \arrow[r] \arrow[d] & \prod_v \mathcal{O}_v^\times \arrow[r] \arrow[d] & \ker\hat{\alpha} \arrow[d] \arrow[dddll, rounded corners] & \\
1 \arrow[r] & K^\times \arrow[r] \arrow[d] & \mathcal{I}_K^0 \arrow[r] \arrow[d] & \mathcal{C}_K^0 \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & K^\times/\mathbb{F}_q^\times \arrow[r] \arrow[d] & \mathrm{Div}^0(K) \arrow[r] \arrow[d] & \mathrm{Cl}^0(K) \arrow[r] \arrow[d] & 1 \\
 & 1 & 1 & 1 &
\end{tikzcd}$$

And therefore we have:

$$1 \to \mathbb{F}_q^\times \to \prod_v \mathcal{O}_v^\times \to \mathcal{C}_K^0 \to \mathrm{Cl}^0(K) \to 1.$$

This proves lemma 5.8.

5.3.4 On the Structure of the Kernel

Now we will give an explicit description of the group $\ker\hat{\alpha} \simeq (\prod_v \mathcal{O}_v^\times)/\mathbb{F}_q^\times$. If v is a place of degree n of a global function field K with exact constant field $\mathbb{F}_q$, then K_v is the field of Laurant series with constant field $\mathbb{F}_{q^n}$ and $\mathcal{O}_v$ is the ring of formal power series: $K_v \simeq \mathbb{F}_{q^n}((x))$, $\mathcal{O}_v \simeq \mathbb{F}_{q^n}[[x]]$. A formal power series is invertible if and only if it has non-zero constant term and therefore:

$$\mathcal{O}_v^\times \simeq \mathbb{F}_{q^n}^\times \times (1 + t\mathbb{F}_{q^n}[[t]]).$$

Lemma 5.17. *We have an isomorphism of topological groups: $1 + t\mathbb{F}_{q^n}[[t]] \simeq \mathbb{Z}_p^\infty$, where ∞ means the countable cardinal number.*

Proof. See [36], section on local fields. □

Denoting by $\mathcal{T}_K$ the group $(\prod_v \mathbb{F}_{q^{\deg(v)}}^\times)/\mathbb{F}_q^\times$, we obtain:

$$(\prod_v \mathcal{O}_v^\times)/\mathbb{F}_q^\times \simeq \mathcal{T}_K \times \mathbb{Z}_p^\infty.$$

Description of $\mathcal{T}_K$

At the first time it seems that the group $\mathcal{T}_K$ depends on K since the product $\prod_v \mathcal{O}_v^\times$ is taken over all places of K. Our first goal is to show that it actually depends only on q.

Recall the following classical statement needed in the proof:

Lemma 5.18. *For a fixed global function field K there exists a natural number N such that for every $n \in \mathbb{N}$, $n \geq N$ there exists a place of K of degree n.*

Proof. See chapter 5 of [42]. $\square$

Consider the group $A_K = \prod_v \mathbb{F}^\times_{q^{\deg(v)}}$. By the Chinese reminder theorem we have:

$$A_K = \prod (\mathbb{Z}/l^m\mathbb{Z})^{a_{l,m}},$$

where $a_{l,m}$ is either a non-negative integer or infinite countable cardinal number. Since $\mathbb{F}^\times_{q^n}$ is a cyclic group of order $q^n - 1$ we have the direct description of $a_{l,m}$: it is the cardinality of the set $\{v \in \mathrm{Pl}(K) | \, \mathrm{ord}_l(q^{\deg(v)} - 1) = m\}$. Note that $a_{p,m} = 0$ for all $m \in \mathbb{N}$.

Lemma 5.19. *Each $a_{l,m}$ is either 0 or infinity.*

Proof. Suppose that there exists a place v of degree n such that $\mathrm{ord}_l(q^n - 1) = m$. We will show that then there are infinitely many such v. Our assumption implies that $q^n = 1 \mod l^m$, but $q^n \neq 1 \mod l^{m+1}$. The order of the group $(\mathbb{Z}/l^{m+1}\mathbb{Z})^\times$ is $\phi(l^{m+1}) = l^{m+1} - l^m$, where ϕ denotes the Euler ϕ-function. It means if q^n satisfies our condition then for any $k \in \mathbb{N}$ the quantity $q^{n+k\phi(l^{m+1})}$ also satisfies our condition. In other words, this condition depends only on $n \mod \phi(l^{m+1})$. Since by lemma 5.18 each function field K has places of all except finitely many degrees if there is one v with $\mathrm{ord}_l(q^{\deg(v)} - 1) = m$ then there are infinitely many such places. $\square$

Now, given $l \neq p$ we would like to understand for how many m we have $a_{l,m} = 0$. First we will prove the following elementary number theory lemma.

Lemma 5.20. *Let a be a positive integer such that $\mathrm{ord}_l(a-1) = n \geq 1$ for some prime number l. Then if $l \neq 2$ or $n \geq 2$ we have $\mathrm{ord}_l(a^l - 1) = n + 1$.*

Proof. By the assumption of the lemma there exists an integer b such that $\gcd(b, l) = 1$ and $a = 1 + bl^n \mod l^{n+1}$. Suppose that $l \neq 2$. For some integer c we have:

$$a^l = (1 + bl^n + cl^{n+1})^l = 1 + l(bl^n + cl^{n+1}) + \frac{l(l-1)}{2}(bl^n + cl^{n+1})^2 + \cdots =$$

$$= 1 + l^{n+1}(b + cl) + \frac{l(l-1)}{2} l^{2n}(b + cl)^2 + \ldots .$$

Since $l \neq 2$ we have $a^l = 1 + bl^{n+1} \mod l^{n+2}$.

Now let $l = 2$ and $n \geq 2$. We have: $a = 1 + 2^n + b2^{n+1} \mod 2^{n+2}$ and therefore $a^2 = 1 + 2^{n+1} \mod 2^{n+2}$. $\square$

Lemma 5.21. *For each odd prime number l different from p there exists $N(l)$ such that $a_{l,m}$ is infinite if and only if $m \geq N(l)$. Moreover $N(l)$ depends only on q and not on K.*

Proof. Let $d = l-1$ and $N(l) = \mathrm{ord}_l(q^d - 1)$. Then $q^d = 1$ in the group $(\mathbb{Z}/l^{N(l)}\mathbb{Z})^\times$, but $q^d \neq 1$ in the group $(\mathbb{Z}/l^{N(l)+1}\mathbb{Z})^\times$. Therefore, for each $u \in \mathbb{N}$ such that $u = d \mod \phi(l^{N(l)+1})$ we have: $\mathrm{ord}_l(q^u - 1) = N(l)$. Since K has places of almost all degrees the set $\{v \in \mathrm{Pl}(K) | \deg(v) = d \mod \phi(l^{N(l)+1})\}$ is infinite and hence $a_{l,N(l)} \neq 0$. We would like to show that if $a_{l,m} \neq 0$ then $a_{l,m+1} \neq 0$. We know that there exists a place of the degree d_0 such that $\mathrm{ord}_l(q^{d_0} - 1) = m$. By the previous lemma we have $\mathrm{ord}_l(q^{ld_0} - 1) = m + 1$. Then for any place v from the set $\{v \in \mathrm{Pl}(K) | \deg(v) = ld_0 \mod \phi(l^{m+2})\}$ we have $\mathrm{ord}_l(q^{\deg(v)} - 1) = m + 1$. This shows that if $m \geq N(l)$ then $a_{l,m}$ is infinite.

The last step is to show that $a_{l,m} = 0$ if m is less than $\mathrm{ord}_l(q^d - 1)$. Indeed, the order a of q in the group $\mathbb{F}_l^\times$ divides $(l-1)$ and then $\mathrm{ord}_l(q^a - 1) = \mathrm{ord}_l(q^{a\frac{l-1}{a}} - 1) = \mathrm{ord}_l(q^{l-1} - 1)$, since $\frac{l-1}{a}$ is co-prime to l. It means that if for some u we have $q^u = 1 \mod l$, then $u = ab$ and $\mathrm{ord}_l(q^u - 1) = \mathrm{ord}_l(q^{ab} - 1) \geq \mathrm{ord}_l(q^a - 1) = \mathrm{ord}_l(q^{l-1} - 1)$.

□

Lemma 5.22. *For $l = 2$ the following holds.*

1. *If $p = 2$, then $a_{2,m} = 0$ for all m;*
2. *if $q = 1 \mod 4$, then there exists $N(2)$ such that $a_{2,m}$ is infinite if and only if $m \geq N(2)$;*
3. *if $q = 3 \mod 4$, then there exists $N(2)$ such that $a_{2,m}$ is infinite if and only if $m \geq N(2)$ or $m = 1$;*

Proof. The first statement is trivial. For the second one let $N(2) = \mathrm{ord}_2(q-1)$, then $N(2) \geq 2$. As before we have $q = 1 \mod 2^{N(2)}$, but $q \neq 1 \mod 2^{N(2)+1}$. The group $(\mathbb{Z}/2^{N(2)+1}\mathbb{Z})^\times$ has order $\phi(2^{N(2)+1})$ and hence, for each m such that $m = 1 \mod \phi(2^{N(2)+1})$ we have that $q^m = 1 \mod 2^{N(2)}$, but $q \neq 1 \mod 2^{N(2)+1}$. Since K has places of almost all degrees the set $\{v \in \mathrm{Pl}(K) | \deg(v) = 1 \mod \phi(l^{N(2)+1})\}$ is infinite and hence $a_{2,N(2)} \neq 0$. Now, as in the previous lemma if $a_{l,m} \neq 0$, then $a_{l,m+1}$ is not zero and obviously if $m < N(2)$ we have $a_{2,m} = 0$, here we use the fact that $m \geq 2$.

Finally suppose that $q = 3 \mod 4$. By the same argument as before we have that $a_{2,1}$ is infinite, but then $q^2 = 1 \mod 8$ and hence $a_{2,2} = 0$. Let $N(2) = \mathrm{ord}_2(q^2 - 1) \geq 3$. We have that for $a_{2,N(2)}$ is infinite and for all k such that $1 < k < N(2)$ we have $a_{2,k} = 0$. Because of the same argument as before $a_{2,m}$ is infinite for all $m \geq N(2)$.

□

The next step is to show that $T_q \simeq A_q$. In order to do that we need one elementary lemma.

Lemma 5.23. *For a given prime power q there are infinitely many integer numbers n such that* $\gcd(\frac{q^n-1}{q-1}, q-1) = 1$.

Proof. Consider the factorization of $q-1$ into different prime factors: $q - 1 = l_1^{k_1} \dots l_m^{k_m}$. We know that $q = 1 \mod l_i^{k_i}$ and $q \neq 1 \mod l_i^{k_i+1}$, for all i in $\{1, \dots, m\}$. In other words there exists a natural number a_i co-prime to l_i such that $q = 1 + a_i l_i^{k_i} \mod l_i^{k_i+1}$. Therefore if the natural number n is co-prime to $q-1$ then $q^n = 1 + a_i n l_i^{k_i} \mod l_i^{k_i+1}$ and then $\gcd(\frac{q^n-1}{q-1}, q-1) = 1$. □

Corollary 5.24. *We have an isomorphism $A_q \simeq \mathcal{T}_q$. The characteristic p of the constant field of K is determined by $\mathcal{T}_q$.*

Proof. For the first statement recall that $\mathbb{F}_q^\times$ is embedded diagonally to the product $\prod_v \mathbb{F}^\times_{q^{\deg(v)}}$. Now pick any prime β of K of degree m such that $\gcd(\frac{q^m-1}{q-1}, q-1) = 1$ and split the last product into two parts $\mathbb{F}^\times_{q^m} \oplus \prod_{v\neq\beta} \mathbb{F}^\times_{q^{\deg(v)}}$. Note that $\mathbb{F}_q^\times$ is a subgroup of $\mathbb{F}^\times_{q^m}$ which is direct summand. Since all these finite groups have the discrete topology, the quotient $\prod_{v\neq\beta} \mathbb{F}^\times_{q^{\deg(v)}} \oplus (\mathbb{F}^\times_{q^m}/\mathbb{F}^\times_q)$ is topologically isomorphic to $\mathcal{T}_q$. Finally, since each $a_{n,l}$ is either zero or infinity we have that $A_q \simeq \mathcal{T}_q$.

For the second statement note that p is unique prime such that $a_{p,m} = 0$ for all $m \in \mathbb{N}$.

□

Lemma 5.25. *For odd prime number l we have $N(l) = \mathrm{ord}_l(p^{l-1} - 1) + \mathrm{ord}_l\, d_K$.*

Proof. Recall the isomorphism $\mathbb{Z}_l^\times \simeq (\mathbb{Z}_l)^\times_{\mathrm{tors}} \times (1 + l\mathbb{Z}_l)$, for any odd prime number l. The multiplicative group $1 + l\mathbb{Z}_l$ has the following filtration:

$$\mathbb{Z}_l^\times \supset 1 + l\mathbb{Z}_l \supset 1 + l^2\mathbb{Z}_l \supset \dots$$

For fixed q and $l \neq p$ let d be the order of $q \mod l$. Then by the proof of lemma 5.21 we have: $N(l)$ is the greatest integer such that $q^d \in 1 + l^{N(l)}\mathbb{Z}_l$. Raising q to the power p doesn't change its position in the filtration. On the other hand, lemma 5.20 shows that raising q to the power l shifts the position of q in the filtration exactly by one. Hence for $q = p^{d_K p^n}$, $\gcd(d_K, p) = 1$ we have:

$$N(l) = \mathrm{ord}_l(q^{l-1} - 1) = \mathrm{ord}_l(p^{(l-1)d_K p^k} - 1) = \mathrm{ord}_l(p^{l-1} - 1) + \mathrm{ord}_l(d_K)$$

□

Recall that for a prime number l different from p we define $s_l(\mathcal{T}_q)$ to be the least integer k such that T_q has direct summand of the form $\mathbb{Z}/l^k\mathbb{Z}$. Obviously, if $l \neq 2$ then $s_l(T_q) = N(l)$. More generally, we have:

Lemma 5.26. *For a prime number l different from p the order $\mathrm{ord}_l(d_K)$ is given by the following formula:*

$$\mathrm{ord}_l(d_K) = \begin{cases} 0, & \text{if } (l = 2 \text{ and } s_2 = 1) \\ s_l(\mathcal{T}_q) - \mathrm{ord}_l((p^\star)^{l-1} - 1), & \text{otherwise.} \end{cases}$$

Proof. The case of the odd l is clear, since $p^\star = (-1)^{\frac{p-1}{2}} p$ if p is odd and hence for $l = 1 \mod 2$ we have $(p^\star)^{l-1} = p^{l-1}$. If $l = 2$ then there are two cases. If $p = 1 \mod 4$ then $s_2(T_q) = N(2)$ and obviously $p^\star = p$, hence our formula holds trivially. If $p = 3 \mod 4$ then either $q = 3 \mod 4$ or $q = 1 \mod 4$. In the first case we have $d_K = 1 \mod 2$ and $s_2(\mathcal{T}_q) = 1$ which leads to the our "exceptional case": $l = 2$, $s_2 = 1$. In the second case we have $d_K = 0 \mod 2$ and then $N(2) = s_2(T_q) \geq 2$ and hence $s_2(T_q) = \mathrm{ord}_2(q - 1) = \mathrm{ord}_2(p^{p^k d_K} - 1) = \mathrm{ord}_2(p^{2\frac{d_K}{2}} - 1) = \mathrm{ord}_2(p^2 - 1) + \mathrm{ord}_2(d_K) - 1 = \mathrm{ord}_2(p + 1) + \mathrm{ord}_2(d_K) = \mathrm{ord}_2(p^\star - 1) + \mathrm{ord}_2(d_K)$, since in this case $p^\star = -p$.

□

Now we are able to prove our main result concerning the isomorphism type of the abelian group $\mathcal{T}_q$. For a prime power $q = p^n$ we define d_q to be the non-p part of n : $d_q = \frac{n}{p^{\mathrm{ord}_p n}}$. Trivially, for a function field K with exact constant field $\mathbb{F}_q$ we have $d_K = d_q$.

Theorem 5.27. *Given two powers of p: $q_1 = p^{n_1}$ and $q_2 = p^{n_2}$ groups $\mathcal{T}_{q_1}$ and $\mathcal{T}_{q_2}$ are isomorphic if and only if $d_{q_1} = d_{q_2}$, i.e. $\frac{n_1}{n_2} \in p^{\mathbb{Z}}$.*

Proof. The only invariants of T_q are the sequence of coefficients $a_{l,m}$ for different l, m. We will show that they coincide for all l, m if and only if the condition of the our theorem holds.

First we will prove the if part. We assume that $d_{q_1} = d_{q_2}$. Let l be an odd prime number different from p, then by the formula from the above lemma $s_l(\mathcal{T}_{q_1}) = s_l(\mathcal{T}_{q_2})$ and we have $a_{l,m} = 0$ if and only if $m < s_l(\mathcal{T}_{q_1})$ which shows that coefficients $a_{m,l}$ coincide for $\mathcal{T}_{q_1}$ and $\mathcal{T}_{q_2}$. Suppose that $l = 2$. If $p = 2$ then $a_{2,m} = 0$ for all m in both groups. If $p = 1 \mod 4$ or $d_{q_1} = 0 \mod 2$ then as before $a_{2,m} = 0$ if and only if $m < N_2(l) = s_2(T_{q_1}) = \mathrm{ord}_2(d_{q_1}) + \mathrm{ord}_2(p-1)$ and hence $a_{2,m}$ coincide for both groups. Finally, if $p = 3 \mod 4$ and $d_{q_1} = d_{q_2} = 1 \mod 2$ then $a_{2,m} = 0$ if and only if either $m = 1$ or $m > N(2) = \mathrm{ord}_2(q_1^2 - 1) = \mathrm{ord}_2(q_2^2 - 1)$. The equality $\mathrm{ord}_2(q_1^2 - 1) = \mathrm{ord}_2(q_2^2 - 1)$ holds since: $\mathrm{ord}_2(q_1^2 - 1) = \mathrm{ord}_2(q_1 + 1) + 1 = \mathrm{ord}_2(p^{d_{q_1} p^k} + 1) + 1 = \mathrm{ord}_2(p + 1) + 1$.

Now, suppose that $T_{q_1} \simeq T_{q_2}$. Then by the formula from lemma 5.26 for any odd prime number l different from p we have $\mathrm{ord}_l(d_{q_1}) = \mathrm{ord}_l(d_{q_2})$. By definition we have $\mathrm{ord}_p(d_{q_1}) = \mathrm{ord}_p(d_{q_2}) = 0$. Finally, for $l = 2$ there are two cases. Either both groups contain direct summand of the form $\mathbb{Z}/2\mathbb{Z}$ and then $\mathrm{ord}_2(d_{q_1}) = \mathrm{ord}_2(d_{q_2}) = 0$, or otherwise the formula from lemma 5.26 holds and then $\mathrm{ord}_2(d_{q_1}) = \mathrm{ord}_2(d_{q_2})$. $\square$

This already gives some important corollary. If $q = 2^{2^k}$ for some non-negative integer k, then coefficients $a_{l,m}$ defined as follows:

$$a_{l,m} = \begin{cases} \mathbb{N}, & \text{if } l \neq 2 \text{ and } m \geq \mathrm{ord}_l(2^{l-1} - 1) \\ 0, & \text{otherwise.} \end{cases} \tag{5.3}$$

Corollary 5.28. *Each of the following function fields K satisfies: $\mathcal{G}_K^{ab} \simeq \prod_{l,m} (\mathbb{Z}/l^m\mathbb{Z})^{a_{l,m}} \times \prod_{\mathbb{N}} \mathbb{Z}_2 \oplus \widehat{\mathbb{Z}}$, where $a_{l,m}$ are given by the formula 5.3 :*

1. *The rational function field with $g = 0$ over $\mathbb{F}_{2^{2^k}}$, for any non-zero integer k;*
2. *The elliptic function field $y^2 + y = x^3 + x + 1$, with $g = 1$ over $\mathbb{F}_2$;*
3. *The hyper elliptic function field $y^2 + y = x^5 + x^3 + 1$, with $g = 2$ over $\mathbb{F}_2$;*
4. *The hyper elliptic function field $y^2 + y = (x^3 + x^2 + 1)(x^3 + x + 1)^{-1}$, with $g = 2$ over $\mathbb{F}_2$;*
5. *The function field of the plane quartic $y^4 + (x^3 + x + 1)y + (x^4 + x + 1) = 0$, with $g = 3$ over $\mathbb{F}_2$.*
6. *The elliptic function field $y^2 + y = x^3 + \mu$, with $g = 1$ over $\mathbb{F}_4$, where μ is the generator of $\mathbb{F}_4^\times$.*

In particular, the genus, the constant field and the zeta-function of K are not determined by G_K^{ab}.

Proof. All these fields have trivial $\mathrm{Cl}^0(K)$, see [28]. Because of Theorem 5.27 we have $\mathcal{T}_2 \simeq \mathcal{T}_{2^{2^k}}$. It means that for any K listed above $\mathcal{C}_K^0 \simeq \mathcal{T}_2 \times \prod_{\mathbb{N}} \mathbb{Z}_2$. $\square$

Remark: For given q we will call a prime l *exceptional* if $N(l) > 1$. The question which l are exceptional seems to be very difficult. Of course, if $l^2|(q-1)$, then $a_{l,1} = 0$, so $N(l) \geq 2$. For example if $q = 9$ then $a_{2,1} = a_{2,2} = 0$. But also there are exceptional primes l with $\gcd(l, q-1) = 1$. For example if $q = 7$ and $l = 5$. Then $7^d = 1 \mod 5$ if and only if $d = 4k$, $k \in \mathbb{Z}$, but then $7^d = 49^{2k} = (-1)^{2k} = 1 \mod 25$. This means that 5 is exceptional. We expect that for a given q there are infinitely many exceptional primes, but we have no idea how to prove it even for the case $q = 2$: the first exceptional prime for this case is 1093. This phenomena is closely related to the so-called *Wieferich primes.*

Our next goal is to understand what happens with the exact sequence:

$$1 \to \mathcal{T}_q \times \mathbb{Z}_p^\infty \to \mathcal{C}_K^0 \to \mathrm{Cl}^0(K) \to 1,$$

when $\mathrm{Cl}^0(K)$ is not trivial. Since we are working with infinite groups $\mathcal{C}_K^0$ can still be isomorphic to $\mathcal{T}_q \times \mathbb{Z}_p^\infty$. In the next paragraph we will show that all torsion elements of $\mathcal{C}_K^0$ are in $\mathcal{T}_q$.

5.3.5 On the torsion of $\mathcal{C}_K^0$

Theorem 5.29. *All the torsion elements of $\mathcal{C}_K^0$ are in $\mathcal{T}_q$ and the exact sequence 5.1 is totally non-split. Moreover, the topological closure of the torsion subgroup of $\mathcal{C}_K^0$ is $\mathcal{T}_q$.*

Proof. Suppose that there exists a non-zero $x \in \mathcal{C}_K^0$ such that $x^l = 1$ for some prime number l. We will show that this element has trivial image in the class group. Pick a representative $(x_{v_1}, x_{v_2}, \dots)$ for x as element of $\mathcal{I}_K$, we know that almost all i we have $x_{v_i} \in \mathcal{O}_{v_i}^\times$ and that $x^l = (x_{v_1}^l, x_{v_2}^l, \dots)$ is a principal idèle. Let a be the element of $K^\times$ whose image in $\mathcal{I}_K$ is x^l. We have that a is locally an l-th power and hence by Theorem 1, chapter 9 from [2] we have that a is globally an l-th power and hence x is a principal idèle up to multiplication by the element $(\zeta_{v_1}, \zeta_{v_2}, \dots) \in \mathcal{T}_q$, where each ζ_{v_i} denotes an l-th root of unity in $K_{v_i}^\times$ and hence its image in the class group is trivial.

Since $\mathbb{Z}_p$ is torsion free we have that all the torsion of $\mathcal{C}_K^0$ lies in $\mathcal{T}_q$. Note that each element of the direct sum $\oplus_{l,m}(\mathbb{Z}/l^m\mathbb{Z})^{a_{l,m}}$ is an element of finite order in $\mathcal{T}_q$ and closure of this direct sum is $\mathcal{T}_q$ itself. $\square$

As it was mentioned in the introduction this statement implies the "only if" part of our main Theorem 5.1.

5.3.6 Proof of the inverse implication

Our task in this section is for given K show that the data $\mathrm{Cl}^0_{\text{non-}p}(K), \mathcal{T}_q$ determines $\mathcal{C}_K^0$ up to isomorphism.

The p-part

Our first goal is to show that the p-part of $\mathcal{C}_K^0$ is isomorphic to $\mathbb{Z}_p^\infty$.

We start from an easy example. Consider the exact sequence: $0 \to \mathbb{Z}_p \to \mathbb{Z}_p \to \mathbb{Z}/p^k\mathbb{Z} \to 0$, where the second map is multiplication by p^k. This sequence is totally non-split. We claim that $\mathbb{Z}_p$ is the unique group which can occur in the middle of such a sequence. More concretely:

Example 5.30. *Let A be an abelian pro-p group such that the following sequence is totally non-split: $0 \to \mathbb{Z}_p \to A \to \mathbb{Z}/p^k\mathbb{Z} \to 0$, then $A \simeq \mathbb{Z}_p$.*

Proof. Since $\mathbb{Z}_p$ is torsion free and the sequence is totally non-split then A is also torsion free. Let us denote the quotient map $A \to \mathbb{Z}/p^k\mathbb{Z}$ by ϕ. There exists $x \in A$ such that $\phi(x)$ is the generator of $\mathbb{Z}/p^k\mathbb{Z}$. Moreover, since A is torsion free we know that $p^k x$ is a non-zero element a of $\mathbb{Z}_p$. We claim that the first non-zero coefficient in the p-adic expression $a = a_0 + a_1 p + a_2 p^2 + \dots$ is a_0. Indeed, if a is divisible by p then $p(p^{k-1}x - \frac{a}{p}) = 0$ and hence $p^{k-1}x = \frac{a}{p} \in \mathbb{Z}_p$ since A is torsion free. But then $\phi(p^{k-1}x) = 0$, which contradicts to the our choice of x and hence $a_0 \neq 0$. Then A is generated by $\{x, \mathbb{Z}_p\}$ with the relation $p^k x = a$. Consider the map $\psi : A \to \mathbb{Z}_p$, which sends element x to a and $\mathbb{Z}_p \to p^k\mathbb{Z}_p$. Then ψ is homomorphism: $\psi(p^k x) = \psi(a) = p^k a = p^k \psi(x)$. The kernel of this map is trivial and since $a_0 \neq 0$ then this map is onto. $\square$

This example gives an idea how to prove the following:

Lemma 5.31. *Let A be an abelian pro-p group and let B be a finite abelian p-group such that the following sequence is totally non-split: $0 \to \mathbb{Z}_p^\infty \to A \to B \to 0$. Then $A \simeq \mathbb{Z}_p^\infty$.*

Proof. Since the sequence is totally non-split and $\mathbb{Z}_p$ is torsion free, then A is torsion free also. This means that multiplication by any natural number is injective. It means that Pontryagin dual $A^\vee$ of A is torsion (since A is pro-finite) and divisible (since the dual to the injection is surjection). Consider the dual sequence: $0 \to B^\vee \to A^\vee \to \oplus Z(p^\infty) \to 0$. By the structure theorem of divisible groups $A^\vee$ is isomorphic to the direct sum of copies of $Z(p^\infty)$ and $\mathbb{Q}$. But $A^\vee$ is torsion and hence $A \simeq \mathbb{Z}_p^\infty$. $\square$

This shows that the isomorphism class of $\mathcal{C}_{K,p}^0$ depends only on p. Therefore given two global function fields K_1, K_2 with isomorphic groups $\mathcal{T}_{q_1} \simeq \mathcal{T}_{q_2}$ they share the same characteristic p and hence the p-parts of their *idèle*-class groups are isomorphic: $\mathcal{C}_{K_1,p}^0 \simeq \mathcal{C}_{K_2,p}^0$.

The non p-part

Now we pick the prime number $l \neq p$ and consider the l-part $\mathcal{C}_{K,l}^0$ of $\mathcal{C}_K^0$. If l is such that $\mathrm{Cl}_l^0(K) \simeq \{0\}$ then obviously $\mathcal{T}_{q,l} \simeq \mathcal{C}_{K,l}^0$. Let l be a prime such that $\mathrm{Cl}_l^0(K)$ is not trivial. We know that the following sequence is totally non-split:

$$1 \to \mathcal{T}_{q,l} \to \mathcal{C}_{K,l}^0 \to \mathrm{Cl}_l^0(K) \to 1.$$

Fix a natural number n. Then multiplication by l^n map induces the following commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{T}_{q,l}[l^n] \arrow[r, hook, two heads] \arrow[d, hook] & \mathcal{C}^0_{K,l}[l^n] \arrow[r, "0"] \arrow[d, hook] & \mathrm{Cl}^0_l(K)[l^n] \arrow[d, hook] & \\
1 \arrow[r] & \mathcal{T}_{q,l} \arrow[r] \arrow[d, "l^n"] & \mathcal{C}^0_{K,l} \arrow[r] \arrow[d, "l^n"] & \mathrm{Cl}^0_l(K) \arrow[r] \arrow[d, "l^n"] & 1 \\
1 \arrow[r] & \mathcal{T}_{q,l} \arrow[r] \arrow[d, two heads] & \mathcal{C}^0_{K,l} \arrow[r] \arrow[d, two heads] & \mathrm{Cl}^0_l(K) \arrow[r] \arrow[d, two heads] & 1 \\
& \mathcal{T}_{q,l}/l^n\mathcal{T}_{q,l} \arrow[r] & \mathcal{C}^0_{K,l}/l^n\,\mathcal{C}^0_{K,l} \arrow[r] & \mathrm{Cl}^0_l(K)/l^n\,\mathrm{Cl}^0_l(K) \arrow[r] & 1
\end{tikzcd}$$

Since our main sequence is totally non-split the map from $\mathcal{C}^0_{K,l}[l^n]$ to $\mathrm{Cl}^0_l(K)[l^n]$ is the zero map and the map from $T_{q,l}[l^n]$ to $\mathcal{C}^0_{K,l}[l^n]$ is an isomorphism. Now applying Pontryagin duality to the above diagram we get:

$$\begin{tikzcd}
1 & (\mathcal{T}_{q,l}[l^n])^\vee \arrow[l] & (\mathcal{C}^0_{K,l}[l^n])^\vee \arrow[l, hook', two heads] & (\mathrm{Cl}^0_l(K)[l^n])^\vee \arrow[l, "0"'] & \\
1 & (\mathcal{T}_{q,l})^\vee \arrow[l] \arrow[u, two heads] & (\mathcal{C}^0_{K,l})^\vee \arrow[l] \arrow[u, two heads] & (\mathrm{Cl}^0_l(K))^\vee \arrow[l] \arrow[u, two heads] & 1 \arrow[l] \\
1 & (\mathcal{T}_{q,l})^\vee \arrow[l] \arrow[u, "l^n"] & (\mathcal{C}^0_{K,l})^\vee \arrow[l] \arrow[u, "l^n"] & (\mathrm{Cl}^0_l(K))^\vee \arrow[l] \arrow[u, "l^n"] & 1 \arrow[l] \\
& (\mathcal{T}_{q,l}/l^n\mathcal{T}_{q,l})^\vee \arrow[u, hook] & (\mathcal{C}^0_{K,l}/l^n\,\mathcal{C}^0_{K,l})^\vee \arrow[l] \arrow[u, hook] & (\mathrm{Cl}^0_l(K)/l^n\,\mathrm{Cl}^0_l(K))^\vee \arrow[l] \arrow[u, hook] & 1 \arrow[l]
\end{tikzcd}$$

Because of the construction of $\mathcal{T}_{q,l}$ the group $(\mathcal{T}_{q,l})^\vee$ is isomorphic to the direct sum of finite cyclic groups, for example for $l \neq 2$ we have $(\mathcal{T}_{q,l})^\vee \simeq \oplus_{k \geq N(l)} \oplus_{\mathbb{N}} \mathbb{Z}/l^k\mathbb{Z}$, and therefore $\cap_n l^n(\mathcal{T}_{q,l})^\vee = \{0\}$. It means we have $(\cap_n l^n(\mathcal{C}^0_{K,l})^\vee) \subset (\mathrm{Cl}^0_l(K))^\vee$. Our goal is to show that $(\cap_n l^n(\mathcal{C}^0_{K,l})^\vee) = (\mathrm{Cl}^0_l(K))^\vee$.

Lemma 5.32. *Given any non-zero element x of $(\mathrm{Cl}^0_l(K))^\vee \subset (\mathcal{C}^0_{K,l})^\vee$ and any natural number n there exists an element $c_x \in (\mathcal{C}^0_{K,l})^\vee$ such that $l^n c_x = x$.*

Proof. For fixed n consider the above diagram. Since the second row is exact the image of x in $(\mathcal{T}_{q,l})^\vee$ is zero. Then its image in $(\mathcal{T}_{q,l}[l^n])^\vee$ is also zero. Since $(\mathcal{T}_{q,l}[l^n])^\vee \simeq (\mathcal{C}^0_{K,l}[l^n])^\vee$ it means that image of the non-zero element x in $(\mathcal{C}^0_{K,l}[l^n])^\vee$ is zero. Since the second column is exact this means that x lies in the image of the multiplication by l^n map from $(\mathcal{C}^0_{K,l})^\vee$ to $(\mathcal{C}^0_{K,l})^\vee$ and therefore there exists c_x such that $l^n c_x = x$. □

It means that we have proved:

Corollary 5.33. *The exact sequence $1 \leftarrow (\mathcal{T}_{q,l})^\vee \leftarrow (\mathcal{C}^0_{K,l})^\vee \leftarrow (\mathrm{Cl}^0_l(K))^\vee \leftarrow 1$ satisfies conditions of Theorem 5.14.*

In order to finish our proof of Theorem 5.1 we will to prove theorem 5.14.

Proof of Theorem 5.14

First, let us recall the settings.

Theorem 5.34. *Let $\{C_i\}$ be a countable set of finite cyclic abelian l-groups with orders of C_i are not bounded as i tends to infinity and let A be any finite abelian l-group. Then up to isomorphism there exists a unique torsion abelian l-group B satisfying two following conditions:*

1. *There exists an exact sequence: $1 \to A \to B \to \oplus_{i\geq 1} C_i \to 1$;*
2. *A is the set of all divisible elements of B: $A = \cap_{n\geq 1} nB$.*

Proof of the existence. Given a group A and $\oplus_{i\geq 1} C_i$ let k_i denotes the order of the group C_i. Because of the assumptions of the Theorem, the sequence of orders k_i is not bounded and hence for each natural number N there exists i such that $k_i \geq N$. Let us pick an increasing sequence of indexes j_i, $i \in \mathbb{N}$ such that $k_{j_i} \geq l^i$. Let $\alpha_0, \ldots, \alpha_{n-1}$ be any finite set of generators of A. Consider the sequence a_m of elements of A defined as follows:

$$a_m = \begin{cases} \alpha_{i \mod n}, & \text{if } m = j_i \\ 0, & \text{otherwise.} \end{cases}$$

Consider the abelian group B which is the quotient of the direct sum $A \oplus (\oplus_{i\in\mathbb{N}} X_i\mathbb{Z})$ of countably many copies of $\mathbb{Z}$ and one copy of A by the relations $k_i X_i = a_i$. We have that B contains A as a subgroup and the quotient of B by A is isomorphic to $\oplus_i C_i$. This means that the group B satisfies the first condition of the theorem. Now, consider the group $Z = \cap_{n\geq 1} nB$. Obviously, $Z \subset A$ and we would like to show that actually $Z = A$. This follows from the fact that for any fixed number $N > 1$ the set $\{k_{j_i} X_{j_i} | i \geq \log_l N\}$ generates A and satisfies $k_{j_i} \geq l^i \geq l^{\log_l(N)} \geq N$.

Proof of the uniqueness. Suppose we are given an abelian torsion l-group B which satisfies both conditions of the our theorem. Denote the map from B to $\oplus_{i\geq 1} C_i$ by ϕ. Let $\tilde{x}_i$ denotes a generator of the cyclic group C_i and let k_i denotes the order of C_i. Let x_i be an element of B such that $\phi(x_i) = \tilde{x}_i$, then $k_i x_i \in A$.

Lemma 5.35. *For any positive integer M which is a power of l the set $A_M = \{k_i x_i | k_i \geq M\}$ generates A.*

Proof. Without loss of generality we assume that $M \geq \#A$. Pick a non-zero element $a \in A$. Because of the second property a can be written as $M^2 y$, where $y \in B$. Since the sequence $1 \to A \to B \to \oplus_{i\geq 1} C_i \to 1$ is exact we can write y as finite $\mathbb{Z}$-linear combination of x_{i_j} and an element of A: $y = b_{i_1} x_{i_1} + b_{i_2} x_{i_2} + \cdots + b_{i_n} x_{i_n} + a_0$. Pick the subset S of $i_1, \ldots, i_n$ consisting of indexes of i_j such that $k_{i_j} \geq M$. Since $M^2 x_{i_j} = 0$ if $k_{i_j} < M$ we have : $M^2 \sum_{j\in S} b_{i_j} x_{i_j} = a$. On the other hand $0 = \phi(a) = M^2 \sum_{j\in S} b_{i_j} \tilde{x}_{i_j}$ and hence $M^2 b_{i_j}$ is divisible by k_{i_j} and $a = \sum_{j\in S} \frac{b_{i_j} M^2}{k_{i_j}} k_{i_j} x_{i_j}$. This means that $\{k_i x_i | k_i \geq M\}$ generates A. □

Remark: consider the sequence $a_i = k_i x_i$ of elements of A from the above lemma. We will say that this sequence (a_i) *strongly generates* A, i.e. that for any integer M the set $S_M = \{a_i | i \in S, k_i \geq M\}$ generates A.

Note that B as abstract abelian group is isomorphic to the group generated by elements X_i and a_i such that $k_iX_i = a_i$: $B = \langle X_i, a_i\rangle/\langle k_iX_i - a_i\rangle$. Given another abelian group B' satisfying conditions of our theorem we know that $B' = \langle X'_i, a'_i\rangle/\langle k_iX'_i - a'_i\rangle$. If for any i we have $a_i = a'_i$ as elements of A then, obviously $B \simeq B'$. Our goal is to show that $B \simeq B'$ in any case.

Definition 5.36. *Given two such groups B, B' with generating sequences (a_i), (a'_i) consider the set $S = \{i|a_i = a'_i\}$. We will say that (a_i) and (a'_i) have* large overlap *if the set $\{a_i|i \in S\}$ strongly generates A.*

We have the following observation:

Lemma 5.37. *If two generating sequences (a_i), (a'_i) of groups B and B' have large overlap, then groups B and B' are isomorphic.*

Proof. For each index i consider the difference $a_i - a'_i$. Since B and B' have large overlap, we can write this difference as finite sum $\sum_{m\in S}\lambda^i_m k_m X'_m$ with $k_m \geq k_i$, $\lambda^i_m \in \mathbb{Z}$. Since both k_m and k_i are powers of l the ratio $\frac{k_m}{k_i}$ is an integer. Consider the map ψ from B to B' defined as follows. The map ψ is identity on A. If $i \in S$ then $\psi(X_i) = X'_i$, otherwise $\psi(X_i) = X'_i + \sum_{m\in S}\lambda^i_m\frac{k_m}{k_i}X'_m$. We claim that ψ is a homomorphism: if $i \in S$ then $a_i = \psi(k_iX_i) = k_i\psi(X_i) = k_iX'_i = a'_i$. If $i \notin S$, we have $a_i = \psi(k_iX_i) = k_i(X'_i + \sum_{m\in S}\lambda^i_m\frac{k_m}{k_i}X'_m) = k_i(X'_i) + \sum_{m\in S}\lambda^i_m k_m X'_m = a'_i + (a_i - a'_i) = a_i$. In other words it sends generators of B to elements of B' preserving all relations. We claim moreover that the map ψ is an isomorphism since we will construct the inverse map ϕ from B' to B as follows. The map ϕ is identity on A. For $i \in S$ we have $\phi(X'_i) = X_i$ and for $i \notin S$ we have $\phi(X'_i) = X_i - \sum_{m\in S}\lambda^i_m\frac{k_m}{k_i}X_m$. Then, for $i \notin S$ we have:

$$\phi(\psi(X_i)) = \phi(X'_i + \sum_{m\in S}\lambda^i_m\frac{k_m}{k_i}X'_m) = \phi(X'_i) + \phi(\sum_{m\in S}\lambda^i_m\frac{k_m}{k_i}X'_m) =$$

$$= (X_i - \sum_{m\in S}\lambda^i_m\frac{k_m}{k_i}X_m) + (\sum_{m\in S}\lambda^i_m\frac{k_m}{k_i}X_m) = X_i.$$

In a similar way one shows that $\psi(\phi(X'_i)) = X'_i$. □

Now we will prove:

Corollary 5.38. *Two groups B and B' satisfying conditions of the above theorem are isomorphic.*

Proof. Suppose that there exists a partition of the set of positive integers $\mathbb{N}$ on two sets $\mathbb{N} = I_1 \cup I_2$, $I_1 \cap I_2 = \emptyset$ such that each of the set $\{a_i|i \in I_1\}$ and $\{a'_i|i \in I_2\}$ strongly generates A. Then we define abelian group D to be the quotient of the direct sum $A \oplus (\oplus_{i\in\mathbb{N}}X_i\mathbb{Z})$ of countably many copies of $\mathbb{Z}$ and one copy of A by the relations $k_iX_i = a_i$, $i \in I_1$ and $k_iX_i = a'_i$, $i \in I_2$. Obviously D also satisfies conditions of Theorem 5.34. Moreover D and B and also D and B' have large overlap, therefore by the lemma 5.37 we have: $B \simeq D \simeq B'$.

Now we will show that such partition exists. We will construct this partition inductively. Let $N_0 = 0$ and let N_1 be the minimal integer such that elements of the set $S_1 = \{a_i|i \leq N_1$ and $k_i \geq l\}$ generate A. The reason for this number to exists is the following. The sequence a_i

strongly generates A which implies that there exist indexes i with $k_i \geq l$ such that a_i generate A, but A is a finite group and hence we can pick a finite number of elements with $k_i \geq l$ generating A. Note that dropping out finitely many indexes doesn't affect the fact that each of the sequences a_i and a'_i strongly generates A. Suppose we've constructed the number N_m then let N_{m+1} be a minimal integer such that elements of the set

$$S_{m+1} = \begin{cases} \{a'_i | N_m < i \leq N_{m+1} \text{ and } k_i \geq l^{m+1}\}, & \text{if } m \text{ is odd} \\ \{a_i | N_m < i \leq N_{m+1} \text{ and } k_i \geq l^{m+1}\}, & \text{otherwise.} \end{cases}$$

generate A. Finally, we define $I_1 = \cup_{m\geq 0}\{i \in \mathbb{N} | N_{2m} < i \leq N_{2m+1}\}$ and $I_2 = \cup_{m\geq 1}\{i \in \mathbb{N} | N_{2m-1} < i \leq N_{2m}\}$. □

5.4 Proof of Corollaries

In this section we will prove corollaries 5.3, 5.4 and 5.5. The first two will follow from the existence for a given constant field $k = \mathbb{F}_q$ an elliptic curve E over k with the group $E(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points having order q, since in the case of elliptic curves we have $E(\mathbb{F}_q) \simeq \mathrm{Cl}^0(K_E)$, where K_E denotes the associated to E global function field.

Definition 5.39. *Fix a finite field $\mathbb{F}_q$. Let N be an integer number in the Hasse interval: $N \in [-2\sqrt{q}; 2\sqrt{q}]$. We will call it admissible if there exists an elliptic curve E over $\mathbb{F}_q$ with $q + 1 - \#E(\mathbb{F}_q) = N$.*

The following statement is a part of the classical statement due to Waterhouse [45]:

Theorem 5.40 (Waterhouse)**.** *If $\gcd(p, N) = 1$ then the number N is admissible.*

Corollary 5.41. *Given a finite field $\mathbb{F}_q$ there exists an elliptic curve E over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q$.*

The above remarks finish the proof of corollaries 5.3 and 5.4. Now we will discuss the proof of the corollary 5.5. Our goal is to show :

Theorem 5.42. *Given a constant field $k = \mathbb{F}_q$ with characteristic $p \neq 2$ there are infinitely many non-isomorphic curves X over k with different two-parts of the group of k-rational points on the Jacobian varieties associated to them.*

Proof. For any positive integer N there exists a monic irreducible polynomial of degree N with coefficients in $\mathbb{F}_q$. Let us pick any sequence of such polynomials $D_n(x)$, $n \in \mathbb{N}$ with the property that $\deg(D_n(x)) = n + 2$. Consider the family of affine curves defined by the equation $C_m : y^2 = D_1(x)D_2(x)\dots D_m(x)$. Since D_i, $i \in \mathbb{N}$ are mutually distinct these affine curves are smooth. Let X_m denotes the normalization of the projective closure of C_m. Then X_m is a hyper-elliptic curve of the genus $g_m = \lfloor \frac{\deg(D_1(x)) + \dots + \deg(D_m(x)) - 1}{2} \rfloor$. The Weil-bound insures that the order of the group of $\mathbb{F}_q$-rational points of the Jacobian variety J_m associated to X_m satisfies the following:

$$(\sqrt{q} - 1)^{2g_m} \leq \#J_m(\mathbb{F}_q) \leq (\sqrt{q} + 1)^{2g_m},$$

and therefore the two-part of $J_m(\mathbb{F}_q)$ is bounded from above by $(\sqrt{q}+1)^{2g_m}$. On the other hand theorem 1.4 from [7] states that the two-rank of $J_m(\mathbb{F}_q)$ is at least $m-2$. Therefore, among the family X_m there are infinitely many curves with different two-part of the group $J_m(\mathbb{F}_q)$ and therefore their function fields K_m have non-isomorphic $\mathcal{G}_{K_m}^{ab}$. $\square$