Analogue of the Kronecker–Weber Theorem in positive characteristic

Gabriel D. Villa–Salvador

Abstract. The classical Kronecker–Weber Theorem establishes that the maximal abelian extension of the field of rational numbers is the union of all cyclotomic number fields. In 1974, D. Hayes proved the analogue in characteristic $p > 0$. Hayes' result says that the maximal abelian extension of the rational function field $\mathbb{F}_q(T)$ is the composite of three pairwise linearly disjoint extensions. The first one is the union of all cyclotomic function fields relative to the infinite prime, the pole divisor of T, introduced by L. Carlitz. The second one is the union of all cyclotomic function fields relative to the zero divisor of T and where the infinite prime is totally wildly ramified and is the only ramified prime. Finally, the third one is the union of all constant extensions. The proof of Hayes is based on the Reciprocity Law. In this work we describe another approach to Hayes' analogue of the Kronecker–Weber Theorem that uses tools from the classical case as well as from the ramification theory of Artin–Schreier extensions and the arithmetic of Witt vectors developed by H. Schmid.

Keywords. Kronecker–Weber Theorem, Cyclotomic Function Fields, Arithmetic of Witt Vectors, Artin–Schreier Extensions, Maximal Abelian Extension, Ramification Theory.

AMS classification. Primary 11R60; Secondary 11R18, 11R37, 11R58, 14H05.

Introduction

We may understand by *class field theory* the study of abelian extensions of global fields and local fields. In some sense, the simplest object of these two families of fields is the field of rational numbers $\mathbb{Q}$. Therefore, one of the objectives in class field theory is to take care of the maximal abelian extension of $\mathbb{Q}$. The first one to study the maximal abelian extension of $\mathbb{Q}$ as such was Leopold Kronecker in 1853 [11]. He claimed that every finite abelian extension of $\mathbb{Q}$ was contained in a cyclotomic field $\mathbb{Q}(\zeta_n)$ for some $n \in \mathbb{N}$. The proof of Kronecker was not complete as he himself was aware.

Heinrich Weber provided a proof of Kronecker's result in 1886 [27]. Weber's proof was also incomplete but the gap was not noticed up to more than ninety years later by Olaf Neumann [16]. The result is now known as the *Kronecker–Weber Theorem*. This theorem is the object of this work.

David Hilbert gave a new proof of Kronecker's original statement in 1896 [10]. This was the first correct complete proof of the theorem. Because of this some people call the result the *Kronecker–Weber–Hilbert Theorem*. However, as we mentioned above, Hilbert was not aware of the gap in Weber's proof. Hilbert's Twelfth Problem is precisely to extend the Kronecker–Weber Theorem to any base number field.

There is a close analogy between algebraic number fields and algebraic functions of one variable. When the field of constants of a function field is a finite field, the analogy is much deeper. The reason is that both families of fields have finite residue fields. These families is what we know as *global fields*. The analogue of the Kronecker–Weber Theorem for function fields is to find explicitly the maximal abelian extension of a rational function field with field of constants the finite field of q elements $k = \mathbb{F}_q(T)$.

One natural question here is if there exists something similar to cyclotomic fields in the case of function fields. Note that in full generality we have "*cyclotomic*" extensions of an arbitrary base field F, namely, $F(\zeta_n)$ where ζ_n denotes a generator of the group $W_n = \{\xi \in \bar{F} \mid \xi^n = 1\}$, $\bar{F}$ denoting a fixed algebraic closure of F. However, in our case, $k(\zeta_n)/k$ is just an extension of constants.

Leonard Carlitz established an analogue of cyclotomic number fields to the case of function fields in [3, 4]. David Hayes [7] developed the ideas of Carlitz and he was able to describe explicitly the maximal abelian extension A of k. Hayes' description of A is analogous to the Kronecker–Weber Theorem. His result may well be called the *Kronecker–Weber–Hilbert–Hayes Theorem* but we will call it just the Kronecker–Weber Theorem in characteristic p. Hayes' approach to find A is the use of the Artin–Takagi reciprocity law in class field theory.

The main purpose of this expository paper is to present another approach to Hayes' result. The main tools of this description are based on the Artin–Schreier–Witt theory of p–cyclic extensions of fields of characteristic p and particularly the arithmetic of these extensions developed by Ernst Witt [29, 30] and Hermann Ludwig Schmid [22, 23, 24]. We may say that this approach is of combinatorial nature since, based on the results of Witt and Schmid, we compare the number of certain cyclic extensions with the number of such extensions contained in A. We find that these two numbers are the same and from here the result follows.

The organization of the paper is the following. After reviewing the results of Kronecker, Weber and Hilbert, we present a proof of the classical Kronecker–Weber Theorem based on the original ideas of Hilbert by using Minkowski's discriminant theorem and ramification groups. In Sections 3 and 4 we give a brief exposition of the Carlitz–Hayes cyclotomic function fields and the description of the maximal abelian extension A of k. After recalling the Takagi–Artin reciprocity law theorem, we describe, in Section 6, the proof of Hayes. In Section 7 we recall some results on Witt Vectors and some relations among the several "*conductors*" of extensions, particularly Schmid's computation of the conductor of a cyclic p–extension, where p is the characteristic. These results are the main tools in the combinatorial proof of the Kronecker–Weber Theorem, which is presented in the last section.

Notation

- For $n \in \mathbb{N}$, $\mathbb{Q}(\zeta_n)$ denotes the cyclotomic number field obtained by adjoining the n–th roots of unity to the field of rational numbers $\mathbb{Q}$.
- For a number field or a local field L, $\mathcal{O}_L$ denotes the ring of integers of L.
- If L/K is an extension of global or local fields, $\mathfrak{D}_{L/K}$ denotes the different of the extension and $\mathfrak{D}_L := \mathfrak{D}_{L/\mathbb{Q}}$.
- $\mathrm{con}_{L/K}$ is used to denote the conorm of a divisor in K to the corresponding divisor in L.
- For any prime $\mathfrak{p}$, $v_\mathfrak{p}$ is the valuation associated to $\mathfrak{p}$.
- For $m \in \mathbb{N}$, C_m will denote the cyclic group of m elements.
- If L/K is a finite Galois extension of local fields, the i–th ramification group G_i, $i \geq 0$ is $G_i = \{\sigma \in G \mid \sigma x - x \in \mathfrak{p}^i \text{ for all } x \in \mathcal{O}_L\}$. G_0 is the inertia group.
- k denotes the rational congruence function field $\mathbb{F}_q(T)$.
- $\mathfrak{p}_\infty$ denotes the infinite prime in k.
- R_T denotes the ring of polynomials $\mathbb{F}_q[T]$.
- $R_T^+ := \{P \in R_T \mid P \text{ is monic and irreducible}\}$.
- For $M \in R_T$, $\Lambda_M := \{u \in \bar{k} \mid u^M = 0\}$.
- For $M \in R_T$, λ_M denotes a fixed generator of the R_T–module Λ_M.
- The field $k(\Lambda_M) = k(\lambda_M)$ will also be denoted by k_M.
- If $\alpha \in L$ is an algebraic element over K, $\mathrm{Irr}(\alpha, x, K) \in K[x]$ denotes the irreducible polynomial of α over K.
- In k, the finite primes will indistinctly be written as the prime divisor $\mathfrak{p}$ or the prime element P in R_T^+ of $\mathfrak{p}$, that is, the divisor of P in k is equal to $\frac{\mathfrak{p}}{\mathfrak{p}_\infty^{\deg P}}$.
- In a function field F the principal divisor of a nonzero element α of F will be denoted by $(\alpha)_F$ or (α) if the underlying field F is clear.
- If $a \in F$ and F is a field of characteristic $p > 0$, then $\wp(a) = a^p - a$.
- The operations $\overset{\bullet}{+}$, $\overset{\bullet}{-}$ and $\overset{\bullet}{\times}$ denote the sum, difference and product respectively of Witt vectors.

1 The classical case

The Kronecker–Weber Theorem establishes

Theorem (Kronecker–Weber). Every finite abelian extension of the field of rational numbers $\mathbb{Q}$ is contained in a cyclotomic extension $\mathbb{Q}(\zeta_n)$. □

The theorem was first stated by Leopold Kronecker (1823–1891) in [11]. He wrote (see [21]):

> "... We obtain the remarkable result that the root of every abelian equation with integer coefficients can be represented as a rational function of roots of unity ..."

In his paper, Kronecker understands by abelian equations those with cyclic Galois group. The general case follows from this one. His formulation was only for cyclic extensions. Kronecker gave the generalization for arbitrary abelian number fields later on in his 1877 paper [12, page 69]. The approach of Kronecker used Lagrangian resolvents obtained by adjoining the n–th roots of unity to cyclic extensions of degree n over a fixed number field.

What Kronecker did not provide was the proof for the case of cyclic extensions of degree 2^n, $n \geq 3$. When p is an odd prime, the cyclotomic field extension $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$ is cyclic with Galois group $C_{p-1} \times C_{p^{n-1}}$. When $p = 2$ and $n \geq 3$, $\mathbb{Q}(\zeta_{2^n})/\mathbb{Q}$ is not a cyclic extension and in fact $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^n})/\mathbb{Q}) \cong C_2 \times C_{2^{n-2}}$. In particular there exist two cyclic subextensions of degree 2^m in $\mathbb{Q}(\zeta_{2^n})/\mathbb{Q}$, $2 \leq m \leq n-2$ and three cyclic subextensions of degree 2. The problem with the prime 2 was already admitted by Kronecker himself.

Heinrich Weber (1842–1913) tried in [27] to give a complete proof of Kronecker's result in 1886. His work was based on Kronecker's ideas. It seems that for about ninety five years nobody noticed that Weber's proof also had a gap. The gap was first observed by Olaf Neumann in [16]. In 1896/1897, David Hilbert gave a new proof of Kronecker's result in [10]. This is the first complete proof of the Kronecker–Weber Theorem and thus some people suggest that the theorem should be called the *Kronecker–Weber–Hilbert Theorem.* Hilbert says in his paper that Weber had given a complete and general proof of Kronecker's result. As noticed by Neumann, this was not so. Weber [28] finally gave his first complete valid proof in 1909.

2 A proof of the Kronecker–Weber Theorem based on ramification groups

In this section we present the fundamental steps of a proof of the Kronecker–Weber Theorem (see [14]). We use freely results on ramification groups, see [25] for instance.

Proposition 2.1. *Let $K/\mathbb{Q}$ be an abelian extension such that the prime $p \in \mathbb{N}$ is tamely ramified. Then there exists an extension L of $\mathbb{Q}$ and a subfield $F \subseteq \mathbb{Q}(\zeta_p)$ such that*

(a).- *Every unramified prime in K is unramified in L.*

(b).- *p is unramified in L.*

(c).- *$FK = FL$.*

SKETCH OF PROOF: Since p is tamely ramified, the first ramification group G_1 of p is trivial. Since $K/\mathbb{Q}$ is abelian, the inertia group $I = I(\mathfrak{p}|p)$, where $\mathfrak{p}$ is a prime of K dividing p, is contained in $\mathbb{F}_p^* = \left(\mathbb{Z}/p\mathbb{Z}\right)^*$ so that the ramification index $e = e(\mathfrak{p}|p)$ divides $p-1$. In particular $p \neq 2$. We consider the unique extension F with $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\zeta_p)$ of degree e over $\mathbb{Q}$. Then F and $L = (FK)^I$ are the fields satisfying the proposition. □

Applying Proposition 2.1 and induction on the number of ramified primes we obtain as a corollary the Kronecker–Weber Theorem when $K/\mathbb{Q}$ is tamely ramified. The substantial part of the proof of the theorem is when wild ramification is present. We consider first a special case and divide this case in two parts: p odd and $p = 2$.

Proposition 2.2. *Let $K/\mathbb{Q}$ be a cyclic extension of degree p over $\mathbb{Q}$ with p an odd prime such that p is the only ramified prime. Then the different of the extension satisfies $\mathfrak{D}_K = \mathfrak{p}^{2(p-1)}$ where $\mathfrak{p}$ is the only ideal of K dividing p.*

SKETCH OF PROOF: We have $e = e(\mathfrak{p}|p) = p$. Choose $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Let

$$f(x) = x^p + a_{p-1}x^{p-1} + \cdots + a_1 x + a_0 = \mathrm{Irr}(\pi, x, \mathbb{Q}) \in \mathbb{Z}[x]$$

be the irreducible polynomial of π over $\mathbb{Q}$. All the nonzero terms $a_i\pi^i \neq 0$, $0 \leq i \leq p-1$ have different $v_{\mathfrak{p}}$ valuations: $v_{\mathfrak{p}}(a_i\pi^i) = pv_p(a_i) + i \equiv i \bmod p$.

Since $\pi^p + a_{p-1}\pi^{p-1} + \cdots + a_1\pi + a_0 = 0$ it follows that $p|a_i$ for all $0 \leq i \leq p-1$ since otherwise $v_p(a_j) = 0$ for some j and

$$\begin{aligned}\infty = v_{\mathfrak{p}}(0) &= v_{\mathfrak{p}}(\pi^p + a_{p-1}\pi^{p-1} + \cdots + a_1\pi + a_0)\\ &= \min_{0\leq i\leq p-1}\{p, pv_p(a_i) + i\} = \min_{p\nmid a_j}\{j\} \neq \infty.\end{aligned}$$

Now $\mathfrak{D}_K = \langle f'(\pi)\rangle = \mathfrak{p}^k$ with $k = \sum_{i=0}^{\infty}(|G_i| - 1)$ where G_i denotes the i–th ramification group corresponding to $\mathfrak{p}$ over p. Since $\mathrm{Gal}(K/\mathbb{Q})$ is of order p, we obtain $|G_i| - 1 = 0$ or $p-1$ so that $p-1|k$. We have

$$f'(\pi) = p\pi^{p-1} + (p-1)a_{p-1}\pi^{p-2} + \cdots + 2a_2\pi + a_1.$$

Writing $a_p = 1$, it follows that for $a_i \neq 0$ we have $v_{\mathfrak{p}}(ia_i\pi^{i-1}) \equiv (i-1) \bmod p$. In particular, for all $i \neq j$ and $a_i \neq 0 \neq a_j$, we obtain $v_{\mathfrak{p}}(ia_i\pi^{i-1}) \neq v_{\mathfrak{p}}(ja_j\pi^{j-1})$. Thus

$$k = v_{\mathfrak{p}}(\mathfrak{D}_K) = v_{\mathfrak{p}}(f'(\pi)) = \min_{\substack{1\leq i\leq p\\ a_i\neq 0}}\left\{v_{\mathfrak{p}}(ia_i\pi^{i-1})\right\} = v_{\mathfrak{p}}(i_0) + v_{\mathfrak{p}}(a_{i_0}) + i_0 - 1,$$

for some i_0. The case $i_0 = p$ is not possible since $v_{\mathfrak{p}}(pa_p\pi^{p-1}) = 2p-1 \not\equiv 0 \bmod (p-1)$. Therefore $1 \leq i_0 \leq p-1$. Thus

$$v_{\mathfrak{p}}(a_{i_0}\pi^{i_0-1}) = pv_p(a_{i_0}) + i_0 - 1 < 2p - 1 = v_{\mathfrak{p}}(pa_p\pi^{p-1})$$

and since $p|a_{i_0}$, we have $v_p(a_{i_0}) = t \geq 1$. Therefore $2p - 1 > tp + i_0 - 1$, so that $t = 1$ and $k < 2p - 1$. Since we have wild ramification $k > p - 1$ and therefore $p - 1 < p + i_0 - 1$. Because $p - 1|k$ we obtain finally that $i_0 = p - 1$ and that $k = 2(p - 1)$. □

Proposition 2.3. *Let p be a prime number, $p > 2$, and let $K/\mathbb{Q}$ be a cyclic extension of degree p where p is the only ramified prime in $K/\mathbb{Q}$. Then $K \subseteq \mathbb{Q}(\zeta_{p^2})$.*

Proof: Let $L/\mathbb{Q}$ be an abelian extension such that $[L : \mathbb{Q}] = p^2$ and such that p is the only ramified prime. Let G_0 be the inertia group of p and let $E := L^{G_0}$. Then p is unramified in $E/\mathbb{Q}$ and therefore $E/\mathbb{Q}$ is an unramified extension. It follows that $E = \mathbb{Q}$ and that $G_0 = G := \mathrm{Gal}(L/\mathbb{Q})$. Since $L/\mathbb{Q}$ is wildly ramified, we have that the first ramification group G_1 is not trivial, $G_1 \neq \{1\}$. Let $F := L^{G_1}$. Then p is tamely ramified in $F/\mathbb{Q}$. It follows that $F = \mathbb{Q}$ and that $G_1 = G$. We have $|G_1| = |G_0| = |G| = p^2$.

Let G_r be the first ramification group such that $|G_r| < p^2$. We have $r \geq 2$. Now, since $G_{r-1}/G_r \subseteq \mathfrak{p}^{r-1}/\mathfrak{p}^r \cong \mathcal{O}_L/\mathfrak{p} \cong \mathbb{F}_p$, it follows that $|G_{r-1}/G_r| = p$ and $|G_{r-1}| = p$.

Let H be any subgroup of G of order p. Consider $\mathfrak{b} := \mathfrak{p} \cap \mathcal{O}_{L^H}$. From Proposition 2.2 we obtain $\mathfrak{D}_{L^H} = \mathfrak{b}^{2(p-1)}$. Thus

$$\mathfrak{D}_L = \mathfrak{D}_{L/L^H}\, \mathrm{con}_{L^H/L}\, \mathfrak{b}^{2(p-1)} = \mathfrak{D}_{L/L^H}\mathfrak{p}^{2p(p-1)}.$$

In other words, the different $\mathfrak{D}_{L/L^H} = \mathfrak{D}_L\mathfrak{p}^{-2p(p-1)}$ is independent of the group H. If $H \neq G_r$, then the ramification groups for the extension L/L^H are given by

$$G_i \cap H = \begin{cases} H & \text{if } 0 \leq i \leq r-1 \\ 1 & \text{if } i > r \end{cases}.$$

Thus, $\mathfrak{D}_{L/L^H} = \mathfrak{p}^s$ with $s = \sum_{i=0}^{\infty}(|G_i \cap H| - 1) = r(p-1)$.

On the other hand, for $H = G_r$, we have

$$\mathfrak{D}_{L/L^{G_r}} = \mathfrak{p}^t \quad \text{with} \quad t = \sum_{i=0}^{\infty}(|G_i \cap G_r| - 1) \geq (r+1)(p-1).$$

Hence, H is the unique subgroup of G of order p and G is a cyclic group. Now let K and K' be two cyclic extensions of degree p over $\mathbb{Q}$ and such that p is the only ramified prime in either one. If $K \neq K'$ then KK' would be a noncyclic extension of degree p^2 over $\mathbb{Q}$ with p the only ramified prime. It follows that $K = K'$ and that K is the only subfield of $\mathbb{Q}(\zeta_{p^2})$ of degree p over $\mathbb{Q}$. □

Theorem 2.4. *Let p be an odd prime. Let $K/\mathbb{Q}$ be an abelian extension of degree p^m where p is the only ramified prime. Then K is the only subfield of $\mathbb{Q}(\zeta_{p^{m+1}})$ of degree p^m over $\mathbb{Q}$ and in particular $K/\mathbb{Q}$ is a cyclic extension.*

PROOF: Let L be the unique subfield of $\mathbb{Q}(\zeta_{p^{m+1}})$ of degree p^m over $\mathbb{Q}$. The field LK is an abelian extension of $\mathbb{Q}$ where p is the only ramified prime. If $LK/\mathbb{Q}$ were not a cyclic extension, then it would contain a noncyclic subextension of degree p^2. Hence $K/\mathbb{Q}$ is a cyclic extension. Since $\mathrm{Gal}(LK/\mathbb{Q}) \subseteq \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q}) \cong C_{p^m}^2$, we obtain that $\mathrm{Gal}(LK/\mathbb{Q})$ is of exponent p^m. Therefore $\mathrm{Gal}(LK/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q}) \cong C_{p^m}$ and $L = K$. □

Now for the even prime, $p = 2$, first we consider a quadratic extension $K/\mathbb{Q}$ such that 2 is the only finite ramified prime. Write $K = \mathbb{Q}(\sqrt{d})$ with d a square free integer. The discriminant of K is $\delta_K = \pm d, \pm 4d$. Since δ_K is a power of 2 it follows that $d = \pm 1$ or $d = \pm 2$. Therefore $K = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\zeta_4)$ or $K = \mathbb{Q}(\sqrt{2})$ or $K = \mathbb{Q}(\sqrt{-2})$. In either case, $K \subseteq \mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, \sqrt{-2})$.

Theorem 2.5. *If $K/\mathbb{Q}$ is a cyclic extension of degree 2^m with $m \geq 2$, with 2 the only finite ramified prime, then $K \subseteq \mathbb{Q}(\zeta_{2^{m+2}})$. Furthermore, $K = \mathbb{Q}(\zeta_{2^{m+2}}) \cap \mathbb{R} = \mathbb{Q}(\zeta_{2^{m+2}} + \zeta_{2^{m+2}}^{-1}) := K_m$ or $K = K_{m-1}(i) = \mathbb{Q}(\zeta_{2^{m+2}} - \zeta_{2^{m+2}}^{-1})$.*

PROOF: First we consider an abelian real extension $K/\mathbb{Q}$ of degree 2^m (not necessarily cyclic) such that 2 is the only ramified prime. However, since $\mathbb{Q}(\sqrt{2})$ is the only real quadratic extension with 2 the only ramified prime, it follows that K is cyclic. Thus KK_m is cyclic so that $K = K_m$.

Now consider a nonreal cyclic extension $K/\mathbb{Q}$ of degree 2^m and with 2 the only finite ramified prime. Let $M := K(i)$ and $M^+ := M \cap \mathbb{R}$. If $K \neq M$, that is, $i \notin M$, $K^+ \neq M^+$ and $K^+ = K_{m-1}$ because it is a real extension of degree 2^{m-1} over $\mathbb{Q}$. It follows that $M^+ = K_m$. Since $M = M^+(i)$, we have $M = \mathbb{Q}(\zeta_{2^{m+2}})$ and $\mathrm{Gal}(M/\mathbb{Q}) \cong C_2 \times C_{2^m}$. There exist three subfields of M of index 2, namely, $\mathbb{Q}(\zeta_{2^{m+1}})$, K_m and $K_{m-1}(i)$. Since $K/\mathbb{Q}$ is a cyclic nonreal extension, we obtain that $K = K_{m-1}(i)$. □

Theorem 2.6 (Kronecker–Weber). *Let $K/\mathbb{Q}$ be a finite abelian extension. Then there exists $n \in \mathbb{N}$ such that $K \subseteq \mathbb{Q}(\zeta_n)$.*

PROOF: Since $K/\mathbb{Q}$ is an abelian extension, we have $\mathrm{Gal}(K/\mathbb{Q}) \cong \oplus_{i=1}^r C_{n_i}$ where each n_i is a prime power. Consider $K_i := K^{H_i}$ the fixed field under $H_i := \oplus_{\substack{j=1\\ j\neq i}}^r C_{n_j}$, $1 \leq i \leq r$. Then $K = K_1 \cdots K_r$. If we prove that each $K_i \subseteq \mathbb{Q}(\zeta_{m_i})$ for some $m_i \in \mathbb{N}$, then $K \subseteq \mathbb{Q}(\zeta_{m_1}, \ldots, \zeta_{m_r}) \subseteq \mathbb{Q}(\zeta_{m_1 \cdots m_r})$. Therefore we may assume that $K/\mathbb{Q}$ is a cyclic extension of degree p^m where p is a prime.

From Proposition 2.1, there exist an extension L of $\mathbb{Q}$ and $F \subseteq \mathbb{Q}(\zeta_n)$ for some $n \in \mathbb{N}$ such that $FK = FL$ and that the only possible ramified prime in $L/\mathbb{Q}$ is p. In fact, n can be chosen to be $n = q_1 \cdots q_t$ where the ramified primes of $K/\mathbb{Q}$ are $q_1, \ldots, q_r$ and possibly p. Therefore

$$L \cap F = \mathbb{Q} \quad \text{and} \quad \mathrm{Gal}(LF/\mathbb{Q}) \cong \mathrm{Gal}(L/\mathbb{Q}) \times \mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{Gal}(FK/\mathbb{Q}).$$

It follows from Theorems 2.4 and 2.5 that $L \subseteq \mathbb{Q}(\zeta_{p^l})$ for some l. Thus $K \subseteq FK = FL \subseteq \mathbb{Q}(\zeta_{q_1\cdots q_r})\mathbb{Q}(\zeta_{p^l}) = \mathbb{Q}(\zeta_{p^l q_1\cdots q_r})$. □

3 Cyclotomic function fields

The analogue of the Kronecker–Weber Theorem in characteristic $p > 0$ is: given a congruence rational function field $k := \mathbb{F}_q(T)$, find explicitly the maximal abelian extension A of k.

In [3] and [4] Leonard Carlitz established a theory of cyclotomic function fields parallel to the classical one. David Hayes [7] developed this theory. In this section we present the basic properties of the Carlitz–Hayes cyclotomic function fields. More details can be consulted in [7] and [26].

Let T be a transcendental fixed element over the finite field of q elements $\mathbb{F}_q$ and consider $k := \mathbb{F}_q(T)$. Here the pole divisor $\mathfrak{p}_\infty$ of T in k is called *the infinite prime*. Let $R_T := \mathbb{F}_q[T]$ be the ring of polynomials in T. Here k plays the role of $\mathbb{Q}$ and R_T the role of $\mathbb{Z}$. Consider the ring $\operatorname{End}_{\mathbb{F}_q}(\bar{k})$ of $\mathbb{F}_q$–endomorphisms of $\bar{k}$, a fixed algebraic closure of k,

$$\operatorname{End}_{\mathbb{F}_q}(\bar{k}) = \{\varphi\colon \bar{k}\to\bar{k}\colon \varphi(a+b) = \varphi(a)+\varphi(b), \varphi(\alpha a) = \alpha\varphi(a)\forall a,b\in\bar{k}, \alpha\in\mathbb{F}_q\}.$$

Since the field k consists of two parts: $\mathbb{F}_q$ and T, we consider two special elements of $\operatorname{End}_{\mathbb{F}_q}(\bar{k})$: the Frobenius automorphism φ of $\bar{k}/\mathbb{F}_q$, and μ_T multiplication by T. More precisely, let $\varphi, \mu_T \in \operatorname{End}_{\mathbb{F}_q}(\bar{k})$ be given by

$$\begin{aligned} \varphi\colon \bar{k} &\to \bar{k} \quad , & \mu_T\colon \bar{k} &\to \bar{k} \\ u &\mapsto u^q & u &\mapsto Tu. \end{aligned}$$

Note that $\varphi\circ\mu_T = \mu_T^q\circ\varphi$ and in particular $\varphi\circ\mu_T \neq \mu_T\circ\varphi$. For any $M \in R_T$, the substitution $T\mapsto \varphi+\mu_T$ in M gives a ring homomorphism $R_T \xrightarrow{\xi} \operatorname{End}_{\mathbb{F}_q}(\bar{k})$, $\xi(M(T)) = M(\varphi+\mu_T)$. That is, if $u\in\bar{k}$ and $M\in R_T$, then

$$\xi(M)(u) = a_d(\varphi+\mu_T)^d(u)+\cdots+a_1(\varphi+\mu_T)(u)+a_0u$$

where $M(T) = a_dT^d+\cdots+a_1T+a_0$. In this way $\bar{k}$ becomes an R_T–module. The action is denoted as follows: if $M\in R_T$ and $u\in\bar{k}$, $M\circ u = u^M := \xi(M)(u)$. We obtain $u^M = \sum_{i=0}^d \left[{M \atop i}\right] u^{q^i}$ where $\left[{M \atop i}\right]$ is a polynomial in R_T of degree $(d-i)q^i$ and $\left[{M \atop 0}\right] = M$, $\left[{M \atop d}\right] = a_d$. We have for all $M,N\in R_T$ and $\alpha,\beta\in\mathbb{F}_q$

$$\left[{\alpha M+\beta N \atop i}\right] = \alpha\left[{M \atop i}\right]+\beta\left[{N \atop i}\right], \quad \left[{T^{d+1} \atop i}\right] = T\left[{T^d \atop i}\right]+\left[{T^d \atop i-1}\right]^q,$$

with $d\in\mathbb{N}\cup\{0\}$.

This action of R_T on $\bar{k}$ is the analogue of the action of $\mathbb{Z}$ on $\bar{\mathbb{Q}}^*$: $n\in\mathbb{Z}$, $x\in\bar{\mathbb{Q}}^*$, $n\circ x := x^n$. Of course the action of R_T is an additive action on $\bar{k}$ and $\mathbb{Z}$ acts multiplicatively on $\bar{\mathbb{Q}}^*$.

The analogy of these two actions runs as follows. If $M \in R_T$, let $\Lambda_M := \{u \in \bar{k} \mid u^M = 0\}$ which is analogous to $\Lambda_m := \{x \in \bar{\mathbb{Q}}^* \mid x^m = 1\}$, $m \in \mathbb{Z}$. We have that Λ_M is an R_T–cyclic module. Indeed we have $\Lambda_M \cong R_T/(M)$ as R_T–modules. A fixed generator of Λ_M will be denoted by λ_M. We have that λ_M^A, $A \in R_T$, is a generator of Λ_M if and only if $\gcd(A, M) = 1$. Note that if $\alpha \in \mathbb{F}_q^*$, then $\Lambda_{\alpha M} = \Lambda_M$, so we may assume, in case of convenience, M is a monic polynomial.

The irreducible polynomial $p(u) = \operatorname{Irr}(\lambda_M, u, k) \in k[u]$ of λ_M is given by

$$p(u) = \Psi_M(u) := \prod_{\substack{A \in R_T \\ \gcd(A,M)=1 \\ \deg A < \deg M}} (u - \lambda_M^A).$$

The polynomial $\Psi_M(u)$ is called the *M–th cyclotomic polynomial.*

Let $k_M := k(\Lambda_M) = k(\lambda_M)$. Then k_M/k is an abelian extension with Galois group $G_M := \operatorname{Gal}(k_M/k) \cong \big(R_T/(M)\big)^*$ the multiplicative group of invertible elements of $R_T/(M)$. The isomorphism is given as follows. For $\sigma \in G_M$, $\sigma\lambda_M$ is a generator of Λ_M. Hence $\sigma\lambda_M = \lambda_M^A$ for $A \in R_T$ relatively prime to M. We have that A is unique modulo M. So $\sigma \mapsto A \bmod M$ is the isomorphism. Thus

$$[k_M : k] = |G_M| = \big|\big(R_T/(M)\big)^*\big| =: \Phi(M).$$

This result is the analogue of $\operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong U_m := \big(\mathbb{Z}/m\mathbb{Z}\big)^*$, where U_m denotes the group of integers modulo m relatively prime to m, $\Psi_M(u)$ is the analogue of the classical cyclotomic polynomial $\Phi_m(x) = \prod_{\substack{1 \le i \le m \\ \gcd(i,m)=1}} (x - \zeta_m^i)$ and, $\Phi(M)$ is the analogue of the classical Euler phi function: $\varphi(m) = |\{i \in \mathbb{Z} \mid 1 \le i \le m, \gcd(i, m) = 1\}|$. We have that $\Phi(M)$ is a multiplicative function: $\Phi(MN) = \Phi(M)\Phi(N)$ for $M, N \in R_T$ with $\gcd(M, N) = 1$. If $P \in R_T$ is an irreducible polynomial and $n \in \mathbb{N}$ then $\Phi(P^n) = q^{nd} - q^{(n-1)d} = q^{(n-1)d}(q^d - 1)$.

The ramification in the extension k_{P^n}/k with $P \in R_T^+$ and $n \in \mathbb{N}$ is given by the following result which can be found with complete proofs in [17, Section 3.2].

Theorem 3.1. *The prime P is fully ramified in k_{P^n}/k. The ramification index is $e_P = \Phi(P^n) = [k_{P^n} : k] = q^{(n-1)d}(q^d - 1)$, where $d = \deg P$. Any other finite prime in k is unramified in k_{P^n}/k. If $P = \mathfrak{p}_\infty$, $e_P = e_\infty = e_{\mathfrak{p}_\infty} = q - 1$, $f_P = f_\infty = f_{\mathfrak{p}_\infty} = 1$, $h_P = h_\infty = h_{\mathfrak{p}_\infty} = \Phi(M)/(q - 1)$.*

The extension k_M/k is a geometric extension, that is, the field of constants of k_M is $\mathbb{F}_q$ and every subextension $k \subsetneqq K \subseteq k_M$ is ramified. □

One important fact when we consider cyclotomic function fields, is the behavior of $\mathfrak{p}_\infty$ in any k_M/k where always $e_\infty = q - 1$ and $f_\infty = 1$. In particular $\mathfrak{p}_\infty$ is *always* tamely ramified. Furthermore, for any subextension L/K with $k \subseteq K \subseteq L \subseteq k_M$ for some $M \in R_T$, if the prime divisors of K dividing $\mathfrak{p}_\infty$ are unramified, then they are fully decomposed.

In any extension k_M/k, the inertia group of $\mathfrak{p}_\infty$ is $G_0 \cong \mathbb{F}_q^* \subseteq \big(R_T/(M)\big)^* \cong G_M$.

4 The maximal abelian extension of *k*

Let A be the maximal abelian extension of k. The expression of A can be given explicitly, namely, A is explicitly generated for suitable finite extensions of k, each one of which is generated by roots of an explicit polynomial. Indeed A is the composite of three pairwise linearly disjoint extensions E/k, $k_{(T)}/k$ and k_∞/k.

$\underline{E/k}$: Consider the usual cyclotomic extensions of k, that is, the constant extensions of k. So $E = \bigcup_{n=1}^{\infty} \mathbb{F}_{q^n}(T)$. We have

$$G_E := \operatorname{Gal}(E/k) \cong \hat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p,$$

where $\hat{\mathbb{Z}}$ is the Prüfer ring and $\mathbb{Z}_p$, p a prime number, is the ring of p–adic numbers. We have that E/k is an unramified extension.

$\underline{k_{(T)}/k}$: Consider the union of all Carlitz–Hayes cyclotomic function fields $k_{(T)} := \bigcup_{M \in R_T} k_M$. We have

$$G_T := \operatorname{Gal}(k_{(T)}/k) \cong \varprojlim_{M \in R_T} \big(R_T/(M)\big)^*.$$

$\underline{k_\infty/k}$: The field $Ek_{(T)}$ is an abelian extension of k but can not be the maximal one since $\mathfrak{p}_\infty$ is tamely ramified in $Ek_{(T)}/k$ and there exist abelian extensions K/k where $\mathfrak{p}_\infty$ is wildly ramified. For instance, consider $K = k(y)$ where $y^p - y = T$. Then K/k is a cyclic extension of degree p, where p is the characteristic of k and $\mathfrak{p}_\infty$ is the only ramified prime in K/k and it is wildly ramified.

We change our “variable” T by $T' = 1/T$ and we now consider the cyclotomic function fields corresponding to the variable T' instead of T. Namely

$$k_{(T')} = k_{(1/T)} := \bigcup_{M' \in R_{T'}} k(\Lambda_{M'}), \quad R_{T'} = \mathbb{F}_q[T'].$$

We have that $k_{(T')}$ shares much with $k_{(T)}$. For instance, if $q = p^2$ and $z^p - z = \frac{T^2+T+1}{T(T+1)}$, then $K := k(z) \subseteq k_{(T)} \cap k_{(T')}$.

In order to find some subextension of $k_{(T')}$ linearly disjoint to $k_{(T)}$, consider $L_{T'} := \bigcup_{m=1}^{\infty} k(\Lambda_{(T')^m})$. In $L_{T'}/k$ the only ramified primes are $\mathfrak{p}_\infty$, which is totally ramified, and the prime $\mathfrak{p}_0$ corresponding to the zero divisor of T. The prime $\mathfrak{p}_0$ is now the infinite prime in $k_{(T')}$ and it is tamely ramified with ramification index $q-1$. Let $G_0' \cong \mathbb{F}_q^* \cong \big(R_{T'}/(T')\big)^*$ be the inertia group of $\mathfrak{p}_0$. Then $k_\infty := L_{T'}^{G_0'}$ is an abelian extension of k where $\mathfrak{p}_\infty$ is the only ramified prime and it is totally wildly ramified, that is, for any finite extension F/k, $k \subsetneqq F \subseteq k_\infty$, $\mathfrak{p}_\infty$ is totally ramified in F and has no tame ramification. This is equivalent to have that the Galois group and the first ramification group are the same.

The extension $B := k_{(T)} \cdot k_\infty \cdot E$ is an abelian extension with $k_{(T)}, k_\infty, E$ pairwise linearly disjoint. Why $A = B$? Hayes’ proof answers this question.

5 Reciprocity Law

Consider the *idèle group* J_k of k which is defined as

$$J_k := \{(\ldots, x_{\mathfrak{p}}, \ldots) \in \prod_{\mathfrak{p}\in\mathbb{P}_k} k_{\mathfrak{p}} \mid x_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^* \text{ for almost all } \mathfrak{p}\}.$$

Here $\mathbb{P}_k$ denotes the set of all prime divisors in k, $k_{\mathfrak{p}}^*$ is the completion of k at $\mathfrak{p}$, $\mathcal{O}_{\mathfrak{p}}$ is the valuation ring at $\mathfrak{p}$ in $k_{\mathfrak{p}}$, $k_{\mathfrak{p}}^* = k_{\mathfrak{p}} \setminus \{0\}$ and $\mathcal{O}_{\mathfrak{p}}^*$ is the group of units of $\mathcal{O}_{\mathfrak{p}}$.

The topology of J_k is given as follows: a basis of the open sets consists of the subsets $\prod_{\mathfrak{p}\in\mathbb{P}_k} A_{\mathfrak{p}}$ where $A_{\mathfrak{p}} \subseteq k_{\mathfrak{p}}^*$ is an open set for all $\mathfrak{p}$ and $A_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}^*$ for almost all $\mathfrak{p} \in \mathbb{P}_{\mathfrak{p}}$.

The *idèle class group* of k is defined by $C_k = J_k/k^*$ where k^* is embedded in J_k via the diagonal map. Consider a finite abelian extension K/k. Let S be a finite set of prime divisors of k such that S contains all the ramified primes in K. Let I^S be the free abelian group generated by $\mathbb{P}_k \setminus S$. Let $\psi_{K/k}\colon I^S \to \mathrm{Gal}(K/k)$, $\psi_{K/k}(\mathfrak{p}) = \left[\frac{K/k}{\mathfrak{p}}\right]$ be the Artin map.

We say that the *reciprocity law* holds for K/k if there exists a group homomorphism $\psi\colon J_k \to \mathrm{Gal}(K/k)$ such that

(a).- ψ is continuous,

(b).- $\psi(k^*) = 1$,

(c).- $\psi((x)) = \psi_{K/k}((x)^S)$ for $x \in J_k^S := \{(x_{\mathfrak{p}})_{\mathfrak{p}\in\mathbb{P}_k} \mid x_{\mathfrak{p}} = 1 \text{ for } \mathfrak{p} \in S\}$, where S consists of the ramified primes in K/k and $(x)^S := \prod_{\mathfrak{p}\notin S} \mathfrak{p}^{v_{\mathfrak{p}}(x_{\mathfrak{p}})} \in I^S$.

In this case $k^* \subseteq \ker\psi$ so ψ induces $\tilde{\psi}\colon C_k = J_k/k^* \to \mathrm{Gal}(K/k)$. If ψ exists, it is unique.

The global class field theory is given by the following theorem.

Theorem 5.1 (Takagi–Artin). (a).- *Every finite abelian extension K/k satisfies the reciprocity law.*

(b).- *The Artin map $\psi_{K/k}$ is surjective and* $\ker\psi_{K/k} = k^*N_{K/k}(J_K)$ *where*

$$N_{K/k}\colon J_K \to J_k$$

is the norm map. Thus $\psi_{K/k}$ induces an isomorphism from $C_k/N_{K/k}(C_K)$ onto $\mathrm{Gal}(K/k)$*.*

(c).- *(Existence Theorem). For each open subgroup N of finite index in C_k, there exists a unique finite abelian extension K/k such that $N_{K/k}C_K = N$.*

PROOF: See [5]. □

6 The proof of David Hayes

The proof of D. Hayes is given in [7]. Let $B = k_{(T)}k_\infty E$. The question is why B is the maximal abelian extension of k. First, Hayes constructed a group homomorphism $\psi\colon J_k \to \mathrm{Gal}(B/k)$. Since $k_{(T)}, k_\infty$ and E are pairwise linearly disjoint, we have $\mathrm{Gal}(B/k) \cong G_{(T)} \times G_\infty \times G_E$ where $G_{(T)} = \mathrm{Gal}(k_{(T)}/k)$, $G_\infty = \mathrm{Gal}(k_\infty/k)$ and $G_E = \mathrm{Gal}(E/k) \cong \hat{\mathbb{Z}}$.

For his construction, Hayes decomposed $J = J_k$ as the direct product of four subgroups and defined ψ directly in each one of the four subgroups. Indeed, the map is trivial on one factor and the other three factors map into $G_{(T)}$, G_∞ and G_E respectively. The factorization is given as follows:

$$J \cong k^* \times U_T \times k_{\mathfrak{p}_\infty}^{(1)} \times \mathbb{Z}$$

both algebraically and topologically. Here k^* is the diagonal in J. Next, let $k_{\mathfrak{p}_\infty}$ be the completion of k at $\mathfrak{p}_\infty$. If $\xi \in k_{\mathfrak{p}_\infty}^*$, ξ can be written uniquely as $\xi = u\pi_\infty^n$ where $\pi_\infty = 1/T$, which is a prime element at $\mathfrak{p}_\infty$, $u \in U_\infty = \mathcal{O}_{\mathfrak{p}_\infty}^*$ and $n \in \mathbb{Z}$. Then the group $k_{\mathfrak{p}_\infty}^{(1)}$ is defined by $k_{\mathfrak{p}_\infty}^{(1)} := \ker(\mathrm{sgn}_{\mathfrak{p}_\infty}) \cap U_\infty$, where $\mathrm{sgn}_{\mathfrak{p}_\infty}\colon k_{\mathfrak{p}_\infty}^* \to k^*$ is given by $\mathrm{sgn}_{\mathfrak{p}_\infty}(\xi) = u \bmod \pi_\infty$. We have that $k_{\mathfrak{p}_\infty}^{(1)} \times \mathbb{Z}$ is isomorphic to $\ker(\mathrm{sgn}_{\mathfrak{p}_\infty})$ with isomorphism $(\alpha, n) \mapsto \alpha\pi_\infty^n$. Finally let $U_T := \{(x_\mathfrak{p})_{\mathfrak{p}\in\mathbb{P}_k} \in J \mid x_{\mathfrak{p}_\infty} = 1 \text{ and } x_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^* \text{ for all } \mathfrak{p}\}$.

The next step in Hayes' construction consisted in proving that there exists a natural isomorphism $\psi_T\colon U_T \to G_{(T)}$, both algebraically and topologically, and that $k_{\mathfrak{p}_\infty}^{(1)}$ is naturally isomorphic to $G_\infty \cong \{f(1/T) \in \mathbb{F}_q[[1/T]] \mid f(0) = 1\}$ being the isomorphism denoted by ψ_∞.

Now $\psi_\mathbb{Z}\colon \mathbb{Z} \to G_E \cong \hat{\mathbb{Z}}$ is the map such that $\psi_\mathbb{Z}(1)$ is the Frobenius automorphism. Therefore $\psi_\mathbb{Z}$ is a dense continuous monomorphism. In short, we have

$$\psi_T\colon U_T \xrightarrow{\cong} G_{(T)}, \quad \psi_\infty\colon k_{\mathfrak{p}_\infty}^{(1)} \xrightarrow{\cong} G_\infty \quad \text{and} \quad \psi_\mathbb{Z}\colon \mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}.$$

We proceed with Hayes definition of the map ψ. Let $\psi\colon J \to \mathrm{Gal}(B/k) \cong G_{(T)} \times G_\infty \times G_E$ given as follows. For $\xi \in J$ we write $\xi = d_T(\xi)\xi_T\xi_\infty\xi_\mathbb{Z}$ where

$$d_T(\xi) = \mathrm{sgn}(\xi_{\mathfrak{p}_\infty}) \cdot \prod_{\substack{\mathfrak{p}\in\mathbb{P}_k \\ \mathfrak{p}\neq\mathfrak{p}_\infty}} \pi_\mathfrak{p}^{v_\mathfrak{p}(\xi_\mathfrak{p})} \in k^*, \pi_\mathfrak{p} = P \quad \text{with} \quad (P) = \frac{\mathfrak{p}}{\mathfrak{p}_\infty^{\deg P}}, \quad P \in R_T^+,$$

$$\xi_T \in U_T, \quad \xi_\infty \in k_{\mathfrak{p}_\infty}^{(1)}, \quad \xi_\mathbb{Z} \in \mathbb{Z}$$

(note that $\xi_\infty \neq \xi_{\mathfrak{p}_\infty}$) and this decomposition of ξ corresponds to the decomposition $J \cong k^* \times U_T \times k_{\mathfrak{p}_\infty}^{(1)} \times \mathbb{Z}$. The homomorphism ψ is finally defined by

$$\psi(\xi) = \psi_T(\xi_T^{-1})\psi_\infty(\xi_\infty^{-1})\psi_\mathbb{Z}(\xi_\mathbb{Z}).$$

Then ψ is a continuous dense homomorphism from J into $\mathrm{Gal}(B/k)$ whose kernel is k^*.

The final step in Hayes' proof is the following. Let A be the maximal abelian extension of k. We have $B \subseteq A$. Let $\psi^* \colon J \to \mathrm{Gal}(A/k)$ be the reciprocity law homomorphism. Let $\mathrm{rest} \colon \mathrm{Gal}(A/k) \to \mathrm{Gal}(B/k)$ be the restriction map. Then we obtain $\mathrm{rest} \circ \psi^* = \psi$ and since $\ker \psi = \ker \psi^* = k^*$, it follows that $\ker \mathrm{rest} = 1$ so that $\mathrm{rest} = \mathrm{Id}$ and $A = B$. This proves the Kronecker–Weber Theorem in characteristic $p > 0$.

Hayes also proved that $A = k_{(T)} k_{(T')}$ with $T' = 1/T$. However, as we have noticed, $k_{(T)}$ and $k_{(T')}$ are not linearly disjoint.

7 Witt vectors and the conductor

One of the main tools for another proof of the Kronecker–Weber Theorem in positive characteristic is the study of p–cyclic extensions of k. As we saw, in the classical case, the substantial part of the proof of the Kronecker–Weber Theorem is wild ramification. The same holds in characteristic p. We have already used, as examples, some Artin–Schreier extensions. In this section we recall some arithmetic properties of cyclic extensions of degree p^n for fields of characteristic p, namely, some results obtained by Ernst Witt [30] and Ludwig Schmid [24].

All the theory began with the results of Emil Artin and Otto Schreier [2]. A. Albert [1] and E. Witt [30] proved that if F admits a cyclic extension of degree p, then it admits cyclic extensions of degree p^n for any $n \in \mathbb{N}$. Witt's approach, stated in Theorem 7.1 below, opened the door for the construction of Witt vectors.

Theorem 7.1 (Witt [29]). *Let E/F be a cyclic extension of degree p^{n-1}, $n \geq 2$. Then to construct a cyclic extension L/F of degree p^n containing E, the following objects are chosen arbitrarily:*

(a).- *A generator φ of* $\mathrm{Gal}(E/F)$.

(b).- *An element $\chi \in \mathbb{F}_p^*$.*

(c).- *A solution $\delta \in E$ of* $\mathrm{Tr}_{E/F}\, \delta = \chi$.

(d).- *A solution $\gamma \in E$ of $(\varphi - 1)\gamma = \wp\delta$.*

Then L is obtained as $L = E(\theta)$ where $\wp\theta = \gamma$. Any other extension of this type can be obtained substituting γ by $\gamma + c$ with $c \in F$. □

This result was the key for Schmid's construction [24] to generate cyclic extensions of degree p^n in characteristic p. Once he gave a construction of cyclic extensions of degree p^n, he also found in [22] a reciprocity formula for the local norm symbol of cyclic extensions of degree p. Shortly after Schmid's results, Witt [30] generalized Schmid's reciprocity norm formula to cyclic extensions of degree p^n and found a vector generation of Schmid's construction of cyclic extensions of degree p^n. This vector generation is what we call *Witt vectors*.

Witt vectors are constructed as follows. For a vector $\vec{x} = (x_1, x_2, \ldots)$ with a countable (finite or numerable) number of components x_n, in characteristic 0, the *ghost components* of $\vec{x}$ are defined by

$$x^{(t)} := x_1^{p^{t-1}} + p x_2^{p^{t-2}} + \cdots + p^{t-1} x_t = \sum_{i=1}^{t} p^{i-1} x_i^{p^{t-i}}, \quad t = 1, 2, \ldots \tag{7.1}$$

Conversely, x_t can be computed recursively as a polynomial in $x^{(1)}, \ldots, x^{(t)}$ from equation (7.1). This bijective correspondence is expressed by

$$\vec{x} = (x_1, x_2, \ldots \mid x^{(1)}, x^{(2)}, \ldots).$$

The sum $\overset{\bullet}{+}$, the difference $\overset{\bullet}{-}$ and the product $\overset{\bullet}{\times}$ of Witt are defined by

$$\vec{x} \overset{\bullet}{\underset{\times}{\pm}} \vec{y} = \big(?, ?, \ldots \mid x^{(1)} \underset{\times}{\pm} y^{(1)}, x^{(2)} \underset{\times}{\pm} y^{(2)}, \ldots\big).$$

That is, the operations on the ghost components are term by term and on the regular components are computed from the result obtained in the ghost components.

The above construction can be specified as follows. Consider three countable families $\{x_i, y_j, z_l\}_{i,j,l=1}^{N}$ of algebraically independent elements over $\mathbb{Q}$ where $N \in \mathbb{N} \cup \{\infty\}$ and let $R = \mathbb{Q}[x_i, y_j, z_l]_{i,j,l}$. Let R^N be the set $\underbrace{R \times R \times \cdots \times R \times \cdots}_{N}$. We denote also by R^N the ring with the underlying base set R^N itself and the usual operations term by term (this construction corresponds to the one for the ghosts components) and let R_N be the ring with underlying set R^N again but with the following Witt operations. Let $\varphi \colon R_N \to R^N$ be given by $\varphi(a_1, a_2, \ldots, a_N) = \big(a^{(1)}, a^{(2)}, \ldots, a^{(N)}\big)$. We have that φ is a bijective map and the inverse map $\psi \colon R^N \to R_N$ is given by $\psi\big(a^{(1)}, a^{(2)}, \ldots, a^{(N)}\big) = (a_1, a_2, \ldots, a_N)$. Then the Witt operations $\overset{\bullet}{+}$, $\overset{\bullet}{-}$, $\overset{\bullet}{\times}$ are given by

$$\vec{a} \overset{\bullet}{\underset{\times}{\pm}} \vec{b} := \big(a^{\varphi} \underset{\times}{\pm} b^{\varphi}\big)^{\varphi^{-1}} = \big(a^{\varphi} \underset{\times}{\pm} b^{\varphi}\big)^{\psi}.$$

For $m \in \mathbb{N}$ we denote

$$\vec{0} := (0, 0, \ldots, 0, \ldots), \quad \vec{1} = (1, 0, \ldots, 0, \ldots), \quad \vec{m} = m\vec{1} = \underbrace{\vec{1} \overset{\bullet}{+} \vec{1} \overset{\bullet}{+} \cdots \overset{\bullet}{+} \vec{1}}_{m \text{ times}}.$$

Here $\vec{0}$ is the zero element of R_N and $\vec{1}$ is the unity of R_N.

Witt operations can be performed mod p and thus if E is a field of characteristic p, we define

$$W_N(E) = \{(x_1, x_2, \ldots) \mid x_i \in E\}, \quad N \in \mathbb{N} \cup \{\infty\}$$

with the Witt operations mod p. $W_N(E)$ is a commutative ring with unity called the *ring of Witt vectors of length N with coefficients in E*. We have

$$\big(\vec{x} \overset{\bullet}{\underset{\times}{\pm}} \vec{y}\big)^p = \vec{x}^p \overset{\bullet}{\underset{\times}{\pm}} \vec{y}^p \quad \text{for all} \quad \vec{x}, \vec{y} \in W_N(E).$$

An element $\vec{x} = (x_1, \dots, x_n, \dots) \in W_N(E)$ is invertible if and only if $x_1 \neq 0$. We also obtain that $\vec{p^m} = p^m \vec{1} = \big(\underbrace{0, 0, \dots, 0}_{m}, 1, 0, \dots\big)$.

As an example, if $N = n \in \mathbb{N}$ then $W_n(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z}$ as rings and therefore $W_n(\mathbb{F}_p)$ is of characteristic p^n. We also have that $W_\infty(\mathbb{F}_p) \cong \mathbb{Z}_p$, where $\mathbb{Z}_p$ is the ring of p–adic numbers and has characteristic 0.

As we have mentioned, Witt used his vector construction to describe cyclic extensions of degree p^n in characteristic p. Let us describe how this was done. Let F be an arbitrary field of characteristic p and let $W_n(F)$ be the ring of Witt vectors. Let E/F be a finite Galois extension with Galois group $G = \mathrm{Gal}(E/F)$. If $\vec{y} \in W_n(E)$, $\vec{y} = (y_1, \dots, y_n)$ then for $\sigma \in G$ we define

$$\sigma\vec{y} = \vec{y}^{\sigma} := (\sigma y_1, \dots, \sigma y_n),$$

and the *trace* $\mathrm{Tr}_{E/F} \colon W_n(E) \to W_n(F)$ is defined by

$$\mathrm{Tr}_{E/F}\,\vec{y} = \overset{\bullet}{\sum_{\sigma \in G}} \sigma\vec{y} = \big(\mathrm{Tr}_{E/F}\, y_1, ?, \dots, ?\big) \in W_n(F).$$

If $y_1 \in E$ is such that $\mathrm{Tr}_{E/F}\, y_1 \neq 0$, then $\mathrm{Tr}_{E/F}\,\vec{y}$ is invertible in $W_n(F)$. Further, we have $\sigma\big(\vec{y} \underset{\times}{\overset{\bullet}{+}} \vec{z}\big) = \sigma\vec{y} \underset{\times}{\overset{\bullet}{+}} \sigma\vec{z}$. We obtain the analogue of Hilbert's Theorem 90. That is, if $\varphi \colon G \to W_n(E)$ is a map with $\varphi(\sigma) = \vec{a}_\sigma$ such that $\vec{a}_\sigma \overset{\bullet}{+} \sigma\vec{a}_\tau = \vec{a}_{\sigma\tau}$ for all $\sigma, \tau \in G$, then there exists $\vec{b} \in W_n(E)$ such that $\vec{a}_\sigma = (1 \overset{\bullet}{-} \sigma)\vec{b}$ for all $\sigma \in G$.

For $\vec{y} \in W_n(E)$ we define $\wp\vec{y} := \vec{y}^p \overset{\bullet}{-} \vec{y} = (y_1^p, \dots, y_n^p) \overset{\bullet}{-} (y_1, \dots, y_n)$. We have $\wp\vec{x} = 0 \iff \vec{x} \in W_n(\mathbb{F}_p)$. Also for any $\vec{x} \in W_n(F)$ there exists $\vec{y} \in W_n(\bar{F})$, $\bar{F}$ a fixed algebraic closure of F, such that $\wp\vec{y} = \vec{x}$. The proof uses the analogue of Hilbert's Theorem 90. Furthermore if $\vec{y}_0$ is a fixed solution of $\wp\vec{y} = \vec{x}$, then all the solutions are given by $\vec{y}_0 \overset{\bullet}{+} \vec{m}$, $m \in \{0, 1, \dots, p^n - 1\}$.

The generation of cyclic extensions of degree p^n is given by next theorem.

Theorem 7.2. *Let F be any field of characteristic p and $\vec{x} \in W_n(F)$. Then the equation $\wp\vec{y} = \vec{x}$ defines a cyclic extension of F: $E = F(\vec{y}) = F(y_1, \dots, y_n) = F(\wp^{-1}\vec{x})$. Furthermore $\mathrm{Gal}(E/F) \cong C_{p^{n-m}}$ where $y_1, \dots, y_m \in F$, $y_{m+1} \notin F$. Therefore E/F is a cyclic extension of degree p^n if and only if $x_1 \notin \wp(F)$ where $\vec{x} = (x_1, \dots, x_n)$. In this case, $G = \mathrm{Gal}(E/F)$ is generated by $\sigma\vec{y} := \vec{y} \overset{\bullet}{+} \vec{1}$.*

Conversely, if E/F is a cyclic extension of degree p^n, there exists $\vec{x} \in W_n(F)$ such that $E = F(\wp^{-1}\vec{x})$, that is, every extension of degree p^n is obtained by means of an equation of the type $\wp\vec{y} = \vec{x}$.

Finally, if $E = F(\vec{y}) = F(\vec{z})$ with $\vec{y}, \vec{z} \in W_n(E)$ is a cyclic extension of degree p^n with $\wp\vec{y} = \vec{a}$, $\wp\vec{z} = \vec{b}$ with $\vec{a}, \vec{b} \in W_n(F)$, then there exist $\vec{j} \in W_n(\mathbb{F}_p)$ invertible, equivalently, j relatively prime to p, and $\vec{c} \in W_n(F)$ such that $\vec{y} = \vec{j} \overset{\bullet}{\times} \vec{z} \overset{\bullet}{+} \vec{c}$ and $\vec{a} = \vec{j} \overset{\bullet}{\times} \vec{b} \overset{\bullet}{+} \wp c$ and conversely. □

7.1 The conductor

For the details of this section the reader may consult [15]. There are several concepts of "*conductor*". In the proof of the Kronecker–Weber Theorem this concept will be considered. We need to know all cyclic p–extensions of k with ramification at a fixed prime. However, it is necessary to bound the measure of this ramification. The way we delimit the ramification type is precisely by means of the conductor. As an example, for any $\alpha \in \mathbb{N}$, there exists a cyclic extension K of k of degree p such that $K \subseteq k(\Lambda_{P^\alpha})$ but $K \nsubseteq k(\Lambda_{P^{\alpha-1}})$. For instance, take $K = k(y)$ with $y^p - y = \frac{1}{T^\lambda}$, $\gcd(\lambda, p) = 1$ and let $\lambda \to \infty$.

We are interested only in congruence function fields, that is, function fields with finite field of constants. Let $k = \mathbb{F}_q(T)$, $R_T = \mathbb{F}_q[T]$. Let $M \in R_T \setminus \{0\}$ be a nonzero polynomial. Let $\chi\colon \big(R_T/(M)\big)^* \to \mathbb{C}^*$ be a Dirichlet character. If $M \in R_T$ then a Dirichlet character χ has *conductor* M if χ can be defined modulo M but can not be defined modulo N where N is a divisor of M and $N \neq M$. In particular, if $P \in R_T^+$ a Dirichlet character χ has conductor P^α if and only if χ can be defined modulo P^α, $\chi\colon \big(R_T/(P^\alpha)\big)^* \to \mathbb{C}^*$ but can not be defined modulo $P^{\alpha-1}$. If $\mathfrak{f}_\chi$ is the conductor as Dirichlet character of χ and if $\mathfrak{f}'_\chi$ is the Artin conductor of χ, then $\mathfrak{f}_\chi = \mathfrak{f}'_\chi$.

Now we have that the local conductor of $k(\Lambda_{P^\alpha})/k$ at P is P^α and 1 for any other $Q \neq P$, $Q \in R_T^+$. Furthermore $\mathfrak{f}_K = P^\alpha \iff K \subseteq k(\Lambda_{P^\alpha})$ and $K \nsubseteq k(\Lambda_{P^{\alpha-1}})$.

7.2 The conductor according to Schmid

The computation of the conductor of cyclic extensions of degree p^n of k is one of the main ingredients of the combinatorial proof of the Kronecker–Weber Theorem. We describe briefly the results of Hasse, Witt and Schmid relative to some arithmetic properties of p–cyclic extensions and particularly the result of Schmid [24] about the conductor.

First, from the normal form of an Artin–Schreier extension found by Helmut Hasse, we obtain

Proposition 7.3 (Hasse [6]). *Let K/k be a cyclic extension of degree p such that $K \subseteq k(\Lambda_{P^\beta})$ for some $\beta \in \mathbb{N}$, $P \in R_T^+$. Then there exists $y \in K$ such that $K = k(y)$ with $\wp y = y^p - y = h(T) \in k$ with $h(T) = \frac{g(T)}{P(T)^\lambda}$ with $g(T) \in R_T$, $\gcd(P(T), g(T)) = 1$, $\deg g \leq \deg P^\lambda = \lambda \deg P$, $\lambda > 0$ and $\gcd(\lambda, p) = 1$.*

The conductor of the extension K/k is $P^{\lambda+1}$. □

From Proposition 7.3 and Schmid's results [24] on the arithmetic generation of p–cyclic extensions based on Witt vectors, we obtain

Corollary 7.4 (Schmid [24]). *Let K/k be a cyclic extension of degree p^n with $K \subseteq k(\Lambda_{P^\alpha})$ for some $\alpha \in \mathbb{N}$. Then there exists $\vec{y}$ such that $K = k(\vec{y})$ with $\wp \vec{y} = \vec{y}^p \overset{\bullet}{-}$*

$\vec{y}=\vec{\beta}\in W_n(k)$ where $\beta_i(T)=\frac{g_i(T)}{P(T)^{\lambda_i}}$ with $g_i(T)\in R_T$, $\lambda_i\geq 0$ and if $\lambda_i>0$ then $\gcd(g_i(T),P(T)=1$ *and* $\gcd(\lambda_i,p)=1$. *Finally* $\lambda_1>0$. □

From the norm residue symbol obtained by Schmid [22] for cyclic extensions of degree p, generalized by Witt [30], Schmid himself [24] obtained the following invariants to compute the conductor of a p–cyclic extension K/k:

Let $K=k(\vec{y})$ be such that $\wp\vec{y}=\vec{y}^p\overset{\bullet}{-}\vec{y}=\vec{\beta}\in W_n(k)$, $\big(\beta_i\big)=\frac{\mathfrak{c}_i}{\mathfrak{p}^{\lambda_i}}$ with $\lambda_i\geq 0$ and if $\lambda_i>0$, then $\gcd(\mathfrak{c}_i,\mathfrak{p})=1$ and $\gcd(\lambda_i,p)=1$ where $\mathfrak{p}$ is the prime divisor associated to P.

Let $M_n:=\max\limits_{1\leq i\leq n}\{p^{n-i}\lambda_i\}$. Note that $M_i=\max\{pM_{i-1},\lambda_i\}$, $M_1<M_2<\cdots<M_n$. Then

Theorem 7.5 (Schmid [24]). *With the above conditions we have that the local conductor of K/k is*

$$\mathfrak{f}_K=P^{M_n+1}. \qquad \square$$

Corollary 7.6. *Let K/k be a cyclic extension of degree p^n with $K\subseteq k(\Lambda_{P^\alpha})$ for some $\alpha\in\mathbb{N}$. Then $M_n+1\leq\alpha$.* □

8 The Kronecker–Weber–Hayes Theorem

In this section we discuss another proof of Hayes' result. The detailed proofs of the results of this section can be found in [18, 19, 20]. Let $k_{(T)}:=\bigcup_{M\in R_T}k(\Lambda_M)$, $\mathbb{F}_\infty:=\bigcup_{m\in\mathbb{N}}\mathbb{F}_{q^m}$, $k_\infty:=L_{(T')}^{G_0'}$ where $L_{(T')}:=\bigcup_{n=1}^{\infty}k(\Lambda_{T^{-n}})$ and $G_0'\cong\mathbb{F}_q^*$ is the inertia group of the zero divisor of T in $L_{(T')}$.

Theorem 8.1 (Kronecker–Weber–Hilbert–Hayes). *The maximal abelian extension of $k=\mathbb{F}_q(T)$ is $A=k_{(T)}\mathbb{F}_\infty k_\infty$.*

To prove Theorem 8.1 it suffices to prove that any finite abelian extension of k is contained in $k_N\mathbb{F}_{q^m}k_n$ for some $N\in R_T$, $m,n\in\mathbb{N}$ and where the field k_n is given by $k_n:=\big(\bigcup_{r=1}^{n+1}k(\Lambda_{T^{-r}})\big)^{G_0'}=k(\Lambda_{T^{-n-1}})^{G_0'}$. Theorem 8.1 will be a consequence of the following theorem.

Theorem 8.2. (a).- *If K/k is a finite tamely ramified abelian extension such that $P_1,\ldots,P_r\in R_T$ and possibly $\mathfrak{p}_\infty$ are the ramified primes, then*

$$K\subseteq\mathbb{F}_{q^m}k(\Lambda_{P_1\cdots P_r})\quad\textit{for some}\quad m\in\mathbb{N}.$$

(b).- *If K/k is a cyclic extension of degree p^n where $P\in R_T^+$ is the only ramified prime and it is totally ramified and $\mathfrak{p}_\infty$ is fully decomposed, then $K\subseteq k(\Lambda_{P^\alpha})$ for some $\alpha\in\mathbb{N}$.*

(c).- *If K/k is a cyclic extension of degree p^n where $P \in R_T^+$ is the only ramified prime, not necessarily fully ramified, we have $K \subseteq \mathbb{F}_{q^m} k(\Lambda_{P^\alpha})$ for some $m, \alpha \in \mathbb{N}$.* □

Let K/k be a finite abelian extension. Let $G := \text{Gal}(K/k) \cong C_{n_1} \times \cdots \times C_{n_l} \times C_{p^{a_1}} \times \cdots \times C_{p^{a_h}}$ where $\gcd(n_i, p) = 1$, $1 \leq i \leq l$ and $a_i \in \mathbb{N}$, $1 \leq j \leq h$. Let $K_i \subseteq L$ be such that $\text{Gal}(K_i/k) \cong C_{n_i}$, $1 \leq i \leq l$ and let $R_j \subseteq K$ be such that $\text{Gal}(R_j/k) \cong C_{p^{a_j}}$, $1 \leq j \leq h$. To prove Theorem 8.1 it suffices to show that each K_i and each R_j are contained in $k(\Lambda_N)\mathbb{F}_{q^m} k_n$ for some $N \in R_T$, $m, n \in \mathbb{N}$.

To obtain Theorem 8.1 from Theorem 8.2, first we give the following result.

Theorem 8.3. *Let K/k be a cyclic extension of degree p^n where $P_1, \ldots, P_r \in R_T^+$ and possibly $\mathfrak{p}_\infty$, are the ramified prime divisors. Then $K = k(\vec{y})$ where*

$$\vec{y}^p \overset{\bullet}{-} \vec{y} = \vec{\beta} = \vec{\delta}_1 \overset{\bullet}{+} \cdots \overset{\bullet}{+} \vec{\delta}_r \overset{\bullet}{+} \vec{\mu},$$

with $\beta_1^p - \beta_1 \notin \wp(k)$, $\delta_{ij} = \frac{Q_{ij}}{P_i^{e_{ij}}}$, $e_{ij} \geq 0$, $Q_{ij} \in R_T$ and if $e_{ij} > 0$, then $p \nmid e_{ij}$, $\gcd(Q_{ij}, P_i) = 1$ and $\deg(Q_{ij}) < \deg(P_i^{e_{ij}})$, and $\mu_j = f_j(T) \in R_T$ with $p \nmid \deg f_j$ when $f_j \notin \mathbb{F}_q$.

Sketch of proof: See [13]. The proof of Theorem 8.3 is as follows. Consider a cyclic extension $K = k(\vec{y})$, $\wp\vec{y} = \vec{y}^p \overset{\bullet}{-} \vec{y} = \vec{\beta} \in W_n(k)$, $\vec{y} \in W_n(K)$ a Witt vector of length n in K. We decompose each component β_j in partial fractions as usual, we then consider the ghost components $\big(\beta^{(1)}, \ldots, \beta^{(n)}\big)$. From (7.1) follows that they have a decomposition of the form

$$\beta^{(j)} = \sum_{i=1}^{r} \frac{Q'_{ij}}{P_i^{e'_{ij}}} + f'_j(T) \text{ for all } 1 \leq j \leq n.$$

We then write

$$\big(\beta^{(1)}, \ldots, \beta^{(n)}\big) = \big(\gamma_1^{(1)}, \ldots, \gamma_1^{(n)}\big) + \cdots + \big(\gamma_r^{(1)}, \ldots, \gamma_r^{(n)}\big) + \big(\xi^{(1)}, \ldots, \xi^{(n)}\big)$$

with $\gamma_i^{(j)} = \frac{Q'_{ij}}{P_i^{e'_{ij}}}$, $\quad 1 \leq i \leq r, 1 \leq j \leq n$ and $\xi^{(j)} = f'_j(T)$.

Now we return to the regular components. The second simplification is no other than Corollary 7.4. □

With the decomposition given in Theorem 8.3, we obtain

Proposition 8.4. *If part* (b) *of Theorem* 8.2 *holds, then if $K = k(\vec{y})$ where $\wp\vec{y} = \vec{y}^p \overset{\bullet}{-} \vec{y} = \vec{\beta}$ with $\beta = \big(\beta_1, \ldots, \beta_n \mid \beta^{(1)}, \ldots, \beta^{(n)}\big)$, β_i in the normal form (Theorem* 8.3*), $\beta_1, \ldots, \beta_r \in \mathbb{F}_q$, $\beta_{r+1} \notin \mathbb{F}_q$, we have $K \subseteq \mathbb{F}_{q^{p^n}} k(\Lambda_{P^\alpha})$ for some $\alpha \in \mathbb{N}$.* □

Therefore Theorem 8.2 (c) is an immediate consequence of Theorem 8.2 (b) and Proposition 8.4. According to the decomposition provided by Theorem 8.3, if $R_i = k(\vec{\delta_i})$ and $R' = k(\vec{\mu})$, it follows from Theorem 8.2 (a) and (b) and from Proposition 8.4 that $R_i \subseteq \mathbb{F}_{q^{m_i}} k(\Lambda_{P_i^{\alpha_i}})$ for some α_i, m_i, $1 \leq i \leq r$ and $R' \subseteq \mathbb{F}_{q^m} k_n$ for some $m, n \in \mathbb{N}$. Thus $M \subseteq k(\Lambda_N)\mathbb{F}_{q^m} k_n$ for some $N \in R_T$ and $n, m \in \mathbb{N}$ and Theorem 8.1 follows.

To prove part (a) of Theorem 8.2, first we observe

Proposition 8.5. *Let $P \in R_T^+$ be a tamely ramified in K/k. If e is the ramification index of P in K, we have $e|q^d - 1$ where $d = \deg P$.* □

The proof of Proposition 8.5 is similar to that of the classical case, that is, to a part of the proof of Proposition 2.1.

The next step is to prove the analogue of Proposition 2.1. Here we consider a tamely ramified abelian extension K/k where $P_1, \ldots, P_r$ are the finite prime divisors ramified in K/k. Let $P \in \{P_1, \ldots, P_r\}$ and with ramification index e. We consider $k \subseteq E \subseteq k(\Lambda_P)$ with $[E : k] = e$. In E/k the prime divisor P has ramification e. Consider the composite KE.

$$\begin{tikzcd}
K \arrow[r, dash] \arrow[d, dash] & KE \arrow[d, dash] \\
k \arrow[r, dash] & E
\end{tikzcd}$$

From Abhyankar's Lemma we obtain that the ramification of P in KE/k is e, so if we consider H, the inertia group of P in KE/k and $R := (KE)^H$. Then P is unramified in R/k. Then it can be proved that $K \subseteq Rk(\Lambda_P)$.

Continuing with this process r times we obtain that $K \subseteq R_0 k(\Lambda_{P_1 \cdots P_r})$ and where R_0/k is an extension such that the only possible ramified prime is $\mathfrak{p}_\infty$. Part (a) of Theorem 8.2 is consequence of

Proposition 8.6. *Let K/k be an abelian extension where at most a prime divisor $\mathfrak{p}_0$ of degree one is ramified and it is tamely ramified. Then K/k is an extension of constants.* □

Wild ramification is the key fact that distinguishes the positive characteristic case from the classical one in the proof of the Kronecker–Weber Theorem. In the classical case, the proof was based on the fact that for $p \geq 3$, there is only one cyclic extension of degree p over $\mathbb{Q}$ where p is the only ramified prime. The case $p = 2$ is slightly harder since there are three quadratic extensions where 2 is the only finite prime ramified.

In the function field case the situation is different. Fix a monic irreducible polynomial $P \in R_T^+$ of degree d. Consider the Galois extension $k(\Lambda_{P^2})/k$ and let $G_{P^2} = \mathrm{Gal}(k(\Lambda_{P^2})/k)$. We have that G_{P^2} is isomorphic to the direct product of $D_{P,P^2} =$

$\mathrm{Gal}(k(\Lambda_{P^2})/k(\Lambda_P))$ with $H := \mathrm{Gal}(k(\Lambda_P)/k) \cong C_{q^d-1}$.

$$\begin{tikzcd}
F \arrow[r, dash, "H"] \arrow[d, dash, "D_{P,P^2}"'] & k(\Lambda_{P^2}) \arrow[d, dash, "D_{P,P^2}"] \\
k \arrow[r, dash, "H"'] & k(\Lambda_P)
\end{tikzcd}$$

If $F := k(\Lambda_{P^2})^H$, then $\mathrm{Gal}(F/k) \cong D_{P,P^2}$. Note that $D_{P,P^2} \cong \{A \bmod P^2 \mid A \in R_T, A \equiv 1 \bmod P\}$ is an elementary abelian p–group so that $D_{P,P^2} \cong C_p^u$ where $u = sd$, $q = p^s$. In F/k the only ramified prime is P, it is wildly ramified and u can be chosen as large as we want. This is one of the reasons that the proof of the classical case using ramification groups seems not to be applicable here.

Let $P \in R_T^+$, $\alpha \in \mathbb{N}$ and let $d := \deg P$. First we compute how many cyclic extensions of degree p^n are contained in $k(\Lambda_{P^\alpha})$. Note that $\mathfrak{p}_\infty$ is fully decomposed in K/k where K is any of these extensions. We have the exact sequence

$$1 \longrightarrow D_{P,P^\alpha} \longrightarrow \big(R_T/(P^\alpha)\big)^* \xrightarrow{\varphi} \big(R_T/(P)\big)^* \longrightarrow 1$$

where

$$\begin{array}{rcl} \varphi\colon \big(R_T/(P^\alpha)\big)^* & \to & \big(R_T/(P)\big)^* \\ A \bmod P^\alpha & \mapsto & A \bmod P \end{array}, \quad D_{P,P^\alpha} = \{N \bmod P^\alpha \mid N \equiv 1 \bmod P\}.$$

We may consider $D_{P,P^\alpha} = \{1 + hP \mid h \in R_T, \deg h < \deg P^\alpha = d\alpha\}$. To compute the number of elements of order p^n in D_{P,P^α} we just have to consider the elements $1 + hP$ such that

$$(1+hP)^{p^n} \equiv 1 \bmod P^\alpha \quad \text{but} \quad (1+hP)^{p^{n-1}} \not\equiv 1 \mod P^\alpha. \tag{8.1}$$

If we write $A = 1 + gP^{1+\gamma}$ with $\gcd(g,P) = 1$ and $\deg g < d(\alpha - \gamma - 1)$, then A satisfies (8.1) precisely for γ satisfying

$$\left\lceil \frac{\alpha}{p^n} \right\rceil - 1 \leq \gamma < \left\lceil \frac{\alpha}{p^{n-1}} \right\rceil - 1 \tag{8.2}$$

where $\lceil x \rceil$ denotes the *ceiling function*, that is, $\lceil x \rceil$ is the minimum integer larger than or equal to x. For each γ satisfying (8.2) there exist $\Phi(P^{\alpha-\gamma-1)}$ different polynomials g with $\gcd(g,P) = 1$ and $\deg g < d(\alpha - \gamma - 1)$, that is, $\deg(gP^{1+\gamma}) < \deg P^\alpha$. Recall that $\Phi(P^{\alpha-\gamma-1}) = \big|\big(R_T/(P^{\alpha-\gamma-1})\big)^*\big|$.

Therefore we obtain that the number of elements of order p^n in $\mathrm{Gal}(k(\Lambda_{P^\alpha})/k)$ is equal to

$$q^{d(\alpha - \lceil \frac{\alpha}{p^{n-1}} \rceil)} \Big(q^{d(\lceil \frac{\alpha}{p^{n-1}} \rceil - \lceil \frac{\alpha}{p^n} \rceil)} - 1\Big).$$

Since each cyclic group of order p^n has $\varphi(p^n) = p^{n-1}(p-1)$ different generators, we obtain

Proposition 8.7. *Let $v_n(\alpha)$ be the number of cyclic groups of order p^n contained in $\big(R_T/(P^\alpha)\big)^*$. Then*

$$v_n(\alpha) = \frac{q^{d(\alpha - \lceil \frac{\alpha}{p^{n-1}} \rceil)}\big(q^{d(\lceil \frac{\alpha}{p^{n-1}} \rceil - \lceil \frac{\alpha}{p^n} \rceil)} - 1\big)}{p^{n-1}(p-1)}. \qquad \square$$

Now we describe the behavior of $\mathfrak{p}_\infty$ in an Artin–Schreier extension K/k.

Proposition 8.8. *Let $K := k(y)$ where $y^p - y = \alpha \in k$ with the normalized equation*

$$y^p - y = \alpha = \sum_{i=1}^{r} \frac{Q_i}{P_i^{e_i}} + f(T) = \frac{Q}{P_1^{e_1} \cdots P_r^{e_r}} + f(T),$$

where $P_i \in R_T^+$, $Q_i \in R_T$, $\gcd(P_i, Q_i) = 1$, $e_i > 0$, $p \nmid e_i$, $\deg Q_i < \deg P_i^{e_i}$, $1 \leq i \leq r$, $f(T) \in R_T$, with $p \nmid \deg f$ when $f(T) \notin \mathbb{F}_q$.

The finite primes ramified in K/k are precisely $P_1, \ldots, P_r$. The prime $\mathfrak{p}_\infty$ is

(a).- *decomposed if $f(T) = 0$.*

(b).- *inert if $f(T) \in \mathbb{F}_q$ and $f(T) \notin \wp(\mathbb{F}_q) := \{a^p - a \mid a \in \mathbb{F}_q\}$.*

(c).- *ramified if $f(T) \notin \mathbb{F}_q$ (thus $p \nmid \deg f$).* □

Note that any $K \subseteq k(\Lambda_{P^\alpha})$ has conductor $\mathfrak{f}_K$ a divisor of P^α. Next, using the Theory of Artin–Schreier, we compute the number of cyclic extensions K of k of degree p such that P is the only ramified prime, $\mathfrak{p}_\infty$ decomposes and the conductor $\mathfrak{f}_K$ divides P^α. From Proposition 8.8 follows that any such extension, written in normal form, is given by an equation

$$\wp y = y^p - y = \frac{Q}{P^\lambda}, \quad \lambda > 0, \quad p \nmid \lambda, \quad \deg Q < \deg P^\lambda$$

and the conductor is $\mathfrak{f}_K = P^{\lambda+1}$, so that $\lambda \leq \alpha - 1$.

Now given another equation $\wp z = z^p - z = a$ written also in normal form and such that $k(y) = k(z)$, satisfies that $a = j\frac{Q}{P^\gamma} + \wp c$ with $j \in \{1, \ldots, p-1\}$ and $c = \frac{h}{P^\gamma}$ with $p\gamma < \lambda$. From these considerations, one may deduce that the number of different cyclic extensions K/k of degree p such that the conductor K is $\mathfrak{f}_K = P^{\lambda+1}$ is equal to $\frac{1}{p-1}\Phi(P^{\lambda - \left[\frac{\lambda}{p}\right]})$ where $[x]$ denotes the *integer* function. So, the number of these extensions with conductor a divisor of P^α is $\frac{\omega(\alpha)}{p-1}$ where

$$\omega(\alpha) = \sum_{\lambda=1}^{\alpha-1} \Phi(P^{\lambda - \left[\frac{\lambda}{p}\right]}). \tag{8.3}$$

Computing (8.3) and comparing with Proposition 8.7 we obtain $\frac{\omega(\alpha)}{p-1} = v_1(\alpha)$.

In other words, every cyclic extension K/k of degree p such that P is the only ramified prime, $\mathfrak{p}_\infty$ decomposes fully in K/k and $\mathfrak{f}_K \mid P^\alpha$ is contained in $k(\Lambda_{P^\alpha})$. Therefore the Kronecker–Weber Theorem holds in this case.

Now we proceed with the cyclic case of degree p^n. In other words, we want to prove that any cyclic extensions of degree p^n of conductor a divisor P^α and where $\mathfrak{p}_\infty$ decomposes fully, is contained in $k(\Lambda_{P^\alpha})$.

The proof is by induction on n. The case $n = 1$ is the case of Artin–Schreier extensions. We assume that any cyclic extension K_{n-1} of degree p^{n-1}, $n \geq 2$ with P the only ramified prime and with $\mathfrak{p}_\infty$ fully decomposed in K_{n-1} and such that $\mathfrak{f}_{K_{n-1}} \mid P^\delta$ is contained in $k(\Lambda_{P^\delta})$, $\delta \in \mathbb{N}$.

We consider K_n a cyclic extension of k of degree p^n such that P is the only ramified prime, P is fully ramified, $\mathfrak{p}_\infty$ is fully decomposed and $\mathfrak{f}_{K_n} \mid P^\alpha$. Let K_{n-1} be the subfield of K_n of degree p^{n-1} over k. Let K_n/k be generated by the Witt vector $\vec{\beta} = (\beta_1, \ldots, \beta_n)$, that is, $K_n = k(\vec{y})$ with $\wp\vec{y} = \vec{y}^p \overset{\bullet}{-} \vec{y} = \vec{\beta}$ and $\vec{\beta}$ written is the normal form described by Schmid. Then K_{n-1}/k is given by the Witt vector $\vec{\beta}' = (\beta_1, \ldots, \beta_{n-1})$.

Let $\vec{\lambda} = (\lambda_1, \ldots, \lambda_{n-1}, \lambda_n)$ be the Schmid's vector of invariants, that is, each β_i is given by $\beta_i = \frac{Q_i}{P^{\lambda_i}}$ where $Q_i = 0$, that is, $\beta_i = 0$ or $\gcd(Q_i, P) = 1$, $\deg Q_i < \deg P^{\lambda_i}$, $\lambda_i > 0$ and $\gcd(\lambda_i, p) = 1$. Since P is fully ramified, $\lambda_i > 0$. The next step is to find the number of different extension K_n/K_{n-1} that can be constructed by means of β_n. If $\beta_n \neq 0$, each equation in normal form is given by

$$\wp y_n = y_n^p - y_n = z_{n-1} + \beta_n$$

where z_{n-1} is the element of K_{n-1} obtained by the Witt's generation of K_{n-1} with the vector $\vec{\beta}'$. In fact, formally, z_{n-1} is given by

$$z_{n-1} = \sum_{i=1}^{n-1} \frac{1}{p^{n-1}} \left[y_i^{p^{n-i}} + \beta_i^{p^{n-1}} - \left(y_i + \beta_i + z_{i-1} \right)^{p^{n-i}} \right]$$

with $z_0 = 0$.

As in the case $n = 1$, we have that there exist at most $\Phi(P^{\lambda_n - \left[\frac{\lambda_n}{p}\right]})$ fields K_n with $\lambda_n > 0$. The conductor of K_n is P^{M_n+1} with $M_n = \max\{pM_{n-1}, \lambda_n\}$ and $P^{M_{n-1}+1}$ is the conductor of K_{n-1}. It follows that $pM_{n-1} \leq \alpha - 1$, $\lambda_n \leq \alpha - 1$ and $\mathfrak{f}_{K_{n-1}} \mid P^\delta$ with $\delta = \left[\dfrac{\alpha - 1}{p} \right] + 1$. By the induction hypothesis, the number of such fields K_{n-1} is $v_{n-1}(\delta)$.

Let $t_n(\alpha)$, $n, \alpha \in \mathbb{N}$ be the number of cyclic extensions K_n/k of degree p^n with P the only ramified prime, fully ramified, $\mathfrak{p}_\infty$ fully decomposed and $\mathfrak{f}_{K_n} \mid P^\alpha$. To prove the Kronecker–Weber Theorem it suffices to show $t_n(\alpha) \leq v_n(\alpha)$. We have $t_1(\alpha) = v_1(\alpha) = \frac{\omega(\alpha)}{p-1}$. By induction hypothesis we assume $t_{n-1}(\delta) = v_{n-1}(\delta)$. In general we have $t_n(\alpha) \geq v_n(\alpha)$. Now we obtain by direct computation

$$\frac{v_n(\alpha)}{v_n(\delta)} = \frac{q^{d(\alpha - \lceil \frac{\alpha}{p} \rceil)}}{p}. \tag{8.4}$$

Considering the case $\beta_n = 0$, the number of fields K_n containing a fixed field K_{n-1} obtained in (8.3) is

$$1 + \omega(\alpha) = q^{d(\alpha - \lceil \frac{\alpha}{p} \rceil)}.$$

Finally, with the substitution $y_n \mapsto z := y_n + jy_1$, $j = 0, 1, \ldots, p-1$ in (8.3) we obtain $\wp z = z^p - z = \beta_n + j\beta_1$.

That is, each extension obtained in (8.3) is obtained p times or, equivalently, for each β_n the same extension is obtained with $\beta_n, \beta_n + \beta_1, \ldots, \beta_n + (p-1)\beta_1$. It follows that for each K_{n-1} there are at most $\frac{1+\omega(\alpha)}{p} = \frac{1}{p} q^{d(\alpha - \lceil \frac{\alpha}{p} \rceil)}$ such extensions K_n. From equation (8.4) we obtain

$$t_n(\alpha) \leq t_{n-1}(\delta)\Big(\frac{1}{p} q^{d(\alpha - \lceil \frac{\alpha}{p} \rceil)}\Big) = v_n(\alpha).$$

This proves Theorem 8.2 (b) and Theorem 8.1.

9 Final remarks

The analogue of the Kronecker–Weber Theorem does not hold for number fields other than $\mathbb{Q}$. For instance, if $K := \mathbb{Q}(\sqrt{5})$, then $L := \mathbb{Q}(\sqrt[4]{5})$ is an abelian extension of K but $L/\mathbb{Q}$ is not a normal extension and in particular L is not contained in any $K(\zeta_n)$ since $K(\zeta_n)/\mathbb{Q}$ is an abelian extension.

As we have mentioned, the content of Hilbert's Twelfth Problem is to find an explicit description of the maximal abelian extension of any number field K. This has been achieved only for imaginary quadratic fields at the end of the 1920's. Class field theory gives a full account of abelian extensions of global fields and local fields by means of fields belonging to "*congruence groups*" or "*norm groups*".

In the case of congruence function fields, Hayes described the maximal abelian extension of an arbitrary congruence function field F by means of rank one Drinfeld modules [8, 9]. Thus, we may consider that Hilbert's Twelfth Problem has been solved for function fields. Recently D. Zywina [31] constructed a continuous homomorphism $\rho\colon \text{Gal}(F^{ab}/F) \to C_F$, where F^{ab} is the maximal abelian extension of F and C_F is the idèle class group, whose inverse is the Artin Map of F and as a consequence he obtained an explicit description of F^{ab}.

Bibliography

[1] A. A. Albert, Cyclic fields of degree p^n over F of characteristic p, *Bulletin A.M.S.* **40** (1934), 625–631.

[2] E. Artin and O. Schreier, Otto, Eine Kennzeichnung der reell abgeschlossenen Körper, *Hamburg Abhandlungen* **5** (1926–1927), 225–231.

[3] Carlitz, Leonard, On certain functions connected with polynomials in a Galois field, *Duke Math. J.* **1** (1935), 137–168.

[4] Carlitz, Leonard, A class of polynomials, *Trans. Amer. Math. Soc.* **43** (1938), 167–182.

[5] Cassels, J.W.S. and Fröhlich, Albrecht, Editors, Algebraic Number Theory, Advanced Study Institute, London and New York, Academic Press,1967.

[6] Hasse, Helmut, Theorie der relativ–zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper, *J. Reine Angew. Math.* **172** (1934), 37–54.

[7] Hayes, David R., Explicit class field theory for rational function fields, *Trans. Amer. Math. Soc.* **189** (1974), 77–91.

[8] Hayes, David R., Explicit class field theory in global function fields, *Studies in algebra and number theory, Adv. in Math. Suppl. Stud.,* **6** (1979), Academic Press, New York-London, 173–217.

[9] Hayes, David R., A brief introduction to Drinfel'd modules, The arithmetic of function fields (Columbus, OH, 1991), *Ohio State Univ. Math. Res. Inst. Publ.,* **2** (1992) de Gruyter, Berlin, 1–32.

[10] Hilbert, David, Ein neuer Beweis des Kronecker'schen Fundamentalsatzes über Abelsche Zahlkörper, *Nachr. Ges. Wiss. zu Göttingen* **1** (1896/97), 29–39.

[11] Kronecker, Leopold, Über die algebraisch auflösbaren Gleichungen. *I, Monatsber. Akad. Wiss. zu Berlin* 1853, 356–374; II ibidem 1856, 203–215 = Werke, vol. **4**, Leipzig–Berlin 1929, 3–11, 27–37.

[12] Kronecker, Leopold, Über Abelsche Gleichungen, *Monatsber. Akad. Wiss. zu Berlin* 1877, 845–851 = Werke, vol. **4**, Leipzig–Berlin 1929, 65–71.

[13] Maldonado–Ramírez, Myriam Rosalía, Rzedowski–Calderón Martha and Villa–Salvador Gabriel, Genus fields of abelian extensions of congruence rational function fields, *Finite Fields and Their Applications* **20** (2013), 40–54.

[14] Marcus, Daniel A., Number Fields, Universitext. Springer–Verlag, New York, Heidelberg, 1977.

[15] Neukirch, Jürgen, Algebraic Number Theory, Springer–Verlag, Berlin, Heidelberg, New York, Barcelona, Hong Kong, London, Milan, Paris, Singapore, Tokyo, 1999.

[16] Neumann, Olaf, Two proofs of the Kronecker–Weber theorem "according to Kronecker, and Weber", *J. Reine Angew. Math.* **323** (1981), 105–126.

[17] Niederraiter Harald and Xing Chaoping, Rational points on curves over finite fields: theory and applications, London Mathematical Society Lecture Notes Series **285**, Cambridge University Press, Cambridge 2001.

[18] Salas–Torres, Julio Cesar, Rzedowski–Calderón, Martha and Villa–Salvador, Gabriel Daniel, Tamely ramified extensions and cyclotomic fields in characteristic p, *Palestine Journal of Mathematics* **2** (2013), 1–5.

[19] Salas–Torres, Julio Cesar, Rzedowski–Calderón, Martha and Villa–Salvador, Gabriel Daniel, Artin–Schreier and Cyclotomic Extensions, submitted, arXiv:1306.3716v2.

[20] Salas–Torres, Julio Cesar, Rzedowski–Calderón, Martha and Villa–Salvador, Gabriel Daniel, A combinatorial proof of the Kronecker–Weber Theorem in positive characteristic, submitted, arXiv:1307.3590v1.

[21] Schappacher, Norbert, On the history of Hilbert's twelfth problem: a comedy of errors, Matériaux pour l'histoire des mathématiques au XXe siècle (Nice, 1996), 243–273, *Sémin. Congr.,* **3**, Soc. Math. France, Paris, 1998.

[22] Schmid, Hermann Ludwig, Über das Reziprozitätsgesetz in relativ–zyklischen algebraischen Funktionenkörpern mit endlichem Konstantenkörper, *Math. Z.* **40** (1936), 94–109.

[23] Schmid, Hermann Ludwig, Zyklische algebraische Funktionenkörper vom Grade p^n über endlichem Konstantenkörper der Charakteristik p, *J. Reine Angew. Math.* **175** (1936), 108–123.

[24] Schmid, Hermann Ludwig, Zur Arithmetik der zyklischen p-Körper (1936), *J. Reine Angew. Math.* **176**, 161–167.

[25] Serre, Jean–Pierre, Local Fields, Graduate Texts in Mathematics **67**, New York–Heidelberg–Berlin, Springer–Verlag, (1979).

[26] Villa Salvador, Gabriel Daniel, Topics in the Theory of Algebraic Function Fields, Mathematics: Theory & Applications, Birkhäuser Boston, Inc., Boston, MA, 2006.

[27] Weber, Heinrich, Theorie der Abelschen Zahlkörper. I: Abelsche Körper und Kreiskörper; II: Über die Anzahl der Idealklassen und die Einheiten in den Kreiskörpern, deren Ordnung eine Potenz von 2 ist; III: Der Kroneckersche Satz, *Acta Math.* **8** (1886), 193–263

[28] Weber, Heinrich, Zur Theorie der zyklischen Zahlkörper, *Math. Annalen* **67** (1909), 32–60; Zweite Abhandlung *ibidem* **70** (1911), 459–470.

[29] Witt, Ernst, Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f, *J. Reine Angew. Math.* **174** (1936), 237–245.

[30] Witt, Ernst, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p, *J. Reine Angew. Math.* **176** (1936), 126–140.

[31] Zywina, David, Explicit class field theory for global function fields, *J. Number Theory* **133** (2013), 1062–1078.

Author information

Gabriel D. Villa–Salvador, Departamento de Control Automático
Centro de Investigación y de Estudios Avanzados del I.P.N., México.
E-mail: `gvillasalvador@gmail.com; gvilla@ctrl.cinvestav.mx`