Special Semester on Applications of Algebra and Number Theory

Johann Radon Institute for Computational and Applied Mathematics (RICAM)

Linz, Austria, November 11 – 15, 2013

Analogue of the Kronecker–Weber Theorem in positive characteristic

Gabriel Villa Salvador

Centro de Investigación y de Estudios Avanzados del I.P.N.,
Departamento de Control Automático,
E-mail: gvilla@ctrl.cinvestav.mx

Joint work with Julio Cesar Salas Torres and
Martha Rzedowski Calderón

November 15, 2013

Topic

We may understand by *class field theory* as the study of abelian extensions of global 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 $\mathbb{Q}$.

Introduction

We may understand by *class field theory* as the study of abelian extensions of global 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 [1]. 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.

Number fields

Henrich Weber provided a proof of Kronecker's result in 1886 [3]. Weber's proof was also incomplete but the gap was not noticed up to more than ninety years later by Olaf Neuman [3]. The result is now known as the *Kronecker–Weber Theorem*.

Henrich Weber provided a proof of Kronecker's result in 1886 [3]. Weber's proof was also incomplete but the gap was not noticed up to more than ninety years later by Olaf Neuman [3]. The result is now known as the *Kronecker–Weber Theorem*. David Hilbert gave a new proof of Kronecker's original statement in 1896 [4]. This was the first correct complete proof of the theorem. However, as we mention above, Hilbert was not aware of Weber's gap. Because of this some people call the result the *Kronecker–Weber–Hilbert Theorem*. Hilbert's Twelfth Problem is precisely to extend the Kronecker–Weber Theorem to any base number field.

Congruence function fields

Gabriel Villa Salvador

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 $k = \mathbb{F}_q(T)$.

Congruence function 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 exist 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.

Congruence function fields 2

Leonard Carlitz established an analogue of cyclotomic number fields to the case of function fields. David Hayes [3] developed the ideas of Carlitz and he was able to describe explicitly the maximal abelian extension A of k.

Congruence function fields 2

Gabriel Villa Salvador

Leonard Carlitz established an analogue of cyclotomic number fields to the case of function fields. David Hayes [3] developed the ideas of Carlitz and he was able to describe explicitly the maximal abelian extension A of k. His 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. Hayes' description of A is analogous to the Kronecker–Weber Theorem. Hayes' approach to find A is the use of the Artin–Takagi reciprocity law in class field theory.

Congruence function fields 3

The main purpose of this talk is to present another approach to Hayes' result. The main tools of this description is 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 Ernest Witt and Hermann Ludwig Schmid [2].

Congruence function fields 3

Gabriel Villa Salvador

The main purpose of this talk is to present another approach to Hayes' result. The main tools of this description is 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 Ernest Witt and Hermann Ludwig Schmid [2]. 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 class of cyclic extensions with the number of such extensions contained in A. We find then that these two numbers are the same and from here the result follows.

Cyclotomic function fields 1

We present the basic properties of the Carlitz–Hayes cyclotomic function fieds.

Cyclotomic function fields 1

We present the basic properties of the Carlitz–Hayes cyclotomic function fieds.

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 $\mathbb{Z}$.

Cyclotomic function fields 1

We present the basic properties of the Carlitz–Hayes cyclotomic function fieds.

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 $\mathbb{Z}$.

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

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

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

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

$$\xi(M)(u) = a_d(\varphi + \mu_T)^d(u) + \cdots + a_1(\varphi + \mu_T)(u) + a_0 u$$

where $M(T) = a_d T^d + \cdots a_1 T + a_0$. In this way $\bar{k}$ becomes an R_T–module. The action is denoted as follows: if $M \in R_T$ and $u \in \bar{k}$, $M \circ u = \xi(M)(u) := u^M$.

Cyclotomic function fields 3

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 $\bar{\mathbb{Q}}^*$.

Cyclotomic function fields 3

Gabriel Villa Salvador

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.

Let $k_M := k(\Lambda_M) = k(\lambda_M)$. Then k_M/k is an abelian extension with Galois group $G_M := \mathrm{Gal}(k_M/k) \cong \big(R_T/(M)\big)^*$ the multiplicative group of invertible elements of $R_T/(M)$.

Let $k_M := k(\Lambda_M) = k(\lambda_M)$. Then k_M/k is an abelian extension with Galois group $G_M := \mathrm{Gal}(k_M/k) \cong \big(R_T/(M)\big)^*$ the multiplicative group of invertible elements of $R_T/(M)$. Thus

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

Let $k_M := k(\Lambda_M) = k(\lambda_M)$. Then k_M/k is an abelian extension with Galois group $G_M := \mathrm{Gal}(k_M/k) \cong \big(R_T/(M)\big)^*$ the multiplicative group of invertible elements of $R_T/(M)$. Thus

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

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 $n \in \mathbb{N}$ we have $\Phi(P^n) = q^{nd} - q^{(n-1)d} = q^{(n-1)d}(q^d - 1)$.

The ramification in the extension k_M/k when $M = P^n$ is given by the following result.

Cyclotomic function fields 5

Gabriel Villa Salvador

The ramification in the extension k_M/k when $M = P^n$ is given by the following result.

Theorem

If $M = P^n$ with P an irreducible polynomial in R_T, then P is fully ramified in k_{P^n}/k. We have $\Phi(P^n) = e_P = [k_{P^n} : k] = q^{(n-1)d}(q^d - 1)$, 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_{P^n}/k is a geometric extension, that is, the field of constants of k_{P^n} is $\mathbb{F}_q$ and every subextension $k \subsetneqq K \subseteq k_{P^n}$ is ramified. $\square$

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.

The maximal abelian extension of k

Gabriel Villa Salvador

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.

First component

$\underline{E/k}$: 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.

Second component

$\underline{k_{(T)}/k}$: Now we consider all the Carlitz–Hayes cyclotomic function fields with respect $\mathfrak{p}_\infty$, $k_{(T)} := \bigcup_{M \in R_T} k_M$. We have

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

What is missing?

$\underline{k_\infty/k}$: 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.

What is missing?

$\underline{k_\infty/k}$: 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 for $T' = 1/T$ and we now consider the cyclotomic function fields corresponding to the variable T' instead of T. Namely

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

$k_{(T)}$ and $k_{(T')}$ are not linearly disjoint

We have that $k_{(T')}$ shares much with $k_{(T)}$. For instance, if $q = p^2$, $p > 3$ and $z^p - z = \frac{T^2+T+1}{(T+1)(T+2)}$, then $K := k(z) \subseteq k_{(T)} \cap k_{(T')}$.

Third component

Gabriel Villa Salvador

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 cero divisor of T. The prime $\mathfrak{p}_0$ is now the infinite prime in $k_{(T')}$ and it is tamely ramified with ramification index $q-1$.

Third component

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 cero 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 $G_0' = \mathbb{F}_q^* = \big(R_{T'}/(T')\big)^*$ 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, $k \subsetneq F \subseteq k_\infty$, then $\mathfrak{p}_\infty$ 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.

Why is the maximal abelian extension?

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.

Decomposition of the idele group

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

Decomposition of the idele group

Let $A = k_{(T)} k_\infty E$. The question is why A is the maximal abelian extension of k. First, Hayes constructed a group homomorphism $\psi\colon J_k \to \mathrm{Gal}(A/k)$, where J_k es the idele group of k. Since $k_{(T)}, k_\infty$ and E are pairwise linearly disjoint, we have $\mathrm{Gal}(A/k) \cong G_{(T)} \times G_\infty \times G_E$ 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 was of the following type:

Decomposition of the idele group

Let $A = k_{(T)}k_\infty E$. The question is why A is the maximal abelian extension of k. First, Hayes constructed a group homomorphism $\psi\colon J_k \to \mathrm{Gal}(A/k)$, where J_k es the idele group of k. Since $k_{(T)}, k_\infty$ and E are pairwise linearly disjoint, we have $\mathrm{Gal}(A/k) \cong G_{(T)} \times G_\infty \times G_E$ 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 was of the following type:

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

both algebraically and topologically.

Isomorphisms

The next step in Hayes' construction consisted in proving that there exist natural isomorphisms $\psi_T\colon U_T \to G_{(T)}$ and $\psi_\infty\colon k_{\mathfrak{p}_\infty}^{(1)} \to G_\infty \cong \{f(1/T) \in \mathbb{F}_q[[1/T]] \mid f(0) = 1\}$, both algebraically and topologically. 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.

Isomorphisms

The next step in Hayes' construction consisted in proving that there exist natural isomorphisms $\psi_T\colon U_T \to G_{(T)}$ and $\psi_\infty\colon k_{\mathfrak{p}_\infty}^{(1)} \to G_\infty \cong \{f(1/T) \in \mathbb{F}_q[[1/T]] \mid f(0) = 1\}$, both algebraically and topologically. 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

The next step in Hayes' construction consisted in proving that there exist natural isomorphisms $\psi_T\colon U_T \to G_{(T)}$ and $\psi_\infty\colon k_{\mathfrak{p}_\infty}^{(1)} \to G_\infty \cong \{f(1/T) \in \mathbb{F}_q[[1/T]] \mid f(0) = 1\}$, both algebraically and topologically. 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

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

End of the Hayes' proof

Gabriel Villa Salvador

The final step in Hayes' proof was to show that with these isomorphisms, the Reciprocity Law of Artin–Takagi gives that A is the maximal abelian extension of k.

End of the Hayes' proof

The final step in Hayes' proof was to show that with these isomorphisms, the Reciprocity Law of Artin–Takagi gives that A is the maximal abelian extension of k.

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.

The conductor

Let $K = k(\vec{y})$ be such that $\wp\vec{y} = \vec{y}^p \overset{\bullet}{-} \vec{y} = \vec{\beta} \in W_n(k)$, $(\beta_i) = \frac{\mathfrak{c}_i}{\mathfrak{p}^{\lambda_i}}$ 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 $M_n := \max_{1 \leq i \leq n} \{p^{n-i}\lambda_i\}$. Note that $M_i = \max\{pM_{i-1}, \lambda_i\}$, $M_1 < M_2 < \cdots < M_n$. Then

The conductor according to Schmid

Gabriel Villa Salvador

Introduction

Cyclotomic function fields

The maximal abelian extension of the rational function field

The proof of David Hayes

Witt vectors and the conductor

The Kronecker–Weber–Hayes Theorem

Bibliography

Theorem (Schmid [2])

With the above conditions we have that the conductor of K/k is

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

The conductor according to Schmid

Theorem (Schmid [2])

With the above conditions we have that the conductor of K/k is

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

□

Corollary

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 $M_n + 1 \leq \alpha$. □

To prove the Kronecker–Weber–Hayes Theorem 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 $k_n := \left(\bigcup_{r=1}^{n+1} k(\lambda_{T^{-r}})\right)^{G_0'} = k(\lambda_{T^{-n-1}})^{G_0'}$.

The Kronecker–Weber–Hayes Theorem

To prove the Kronecker–Weber–Hayes Theorem 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 $k_n:=\left(\bigcup_{r=1}^{n+1}k(\lambda_{T^{-r}})\right)^{G_0'}=k(\lambda_{T^{-n-1}})^{G_0'}$.
It suffices to prove this when the abelian extension is cyclic of order either relatively prime to p or of order p^u for some $u\in\mathbb{N}$.

The Kronecker–Weber–Hayes Theorem

To prove the Kronecker–Weber–Hayes Theorem 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 $k_n := \big(\bigcup_{r=1}^{n+1} k(\lambda_{T^{-r}})\big)^{G_0'} = k(\lambda_{T^{-n-1}})^{G_0'}$.
It suffices to prove this when the abelian extension is cyclic of order either relatively prime to p or of order p^u for some $u \in \mathbb{N}$.
The Kronecker–Weber Theorem will be a consequence of the following facts.

Reduction steps

- (a) If K/k is a finite tamely ramified abelian extension where $P_1, \ldots, P_r \in R_T^+$ and possibly $\mathfrak{p}_\infty$ are the ramified primes, then

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

Reduction steps

- (a) If K/k is a finite tamely ramified abelian extension where $P_1, \ldots, P_r \in R_T^+$ and possibly $\mathfrak{p}_\infty$ are the ramified primes, then

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

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

Reduction steps

- (a) If K/k is a finite tamely ramified abelian extension where $P_1,\ldots,P_r \in R_T^+$ and possibly $\mathfrak{p}_\infty$ are the ramified primes, then
$$K \subseteq \mathbb{F}_{q^m} k(\Lambda_{P_1\cdots P_r}) \quad \text{for some} \quad m \in \mathbb{N}.$$
- (b) If K/k is a cyclic extension of degree p^n where $P \in R_T^+$ is the only ramified prime, P 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, then $K \subseteq \mathbb{F}_{q^{p^m}} k(\Lambda_{P^\alpha})$ for some $m, \alpha \in \mathbb{N}$.

Reduction steps

- (a) If K/k is a finite tamely ramified abelian extension where $P_1, \ldots, P_r \in R_T^+$ and possibly $\mathfrak{p}_\infty$ are the ramified primes, then
$$K \subseteq \mathbb{F}_{q^m} k(\Lambda_{P_1 \cdots P_r}) \quad \text{for some} \quad m \in \mathbb{N}.$$
- (b) If K/k is a cyclic extension of degree p^n where $P \in R_T^+$ is the only ramified prime, P 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, then $K \subseteq \mathbb{F}_{q^{p^m}} k(\Lambda_{P^\alpha})$ for some $m, \alpha \in \mathbb{N}$.
- (d) Similarly for $\mathfrak{p}_\infty$, that is, if K/k is a cyclic extension of degree p^n and $\mathfrak{p}_\infty$ is the only ramified prime, then $K \subseteq \mathbb{F}_{q^{p^m}} k_\alpha$ for some $m, \alpha \in \mathbb{N}$.

Gabriel Villa Salvador

For the part (a), first we observe

Tame ramification

For the part (a), first we observe

Proposición

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

Gabriel Villa Salvador

Tame ramification

For the part (a), first we observe

Proposición

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

Gabriel Villa Salvador

For the part (a), first we observe

Proposición

Let $P \in R_T^+$ *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 this proposition is similar to that of the classical case.

Tame ramification 2

Now 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.

Tame ramification 2

Now 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.

$$\begin{tikzcd}
K \arrow[rr, dash] \arrow[dd, dash] & & KE \arrow[dd, dash] \\
& R \arrow[ur, dash, "H"] & \\
k \arrow[ur, dash] \arrow[rr, dash] & & E
\end{tikzcd}$$

Tame ramification 2

Now 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.

$$\begin{tikzcd}
K \arrow[rr, dash] \arrow[dd, dash] & & KE \arrow[dd, dash] \\
& R \arrow[ur, dash, "H"] & \\
k \arrow[ur, dash] \arrow[rr, dash] & & E
\end{tikzcd}$$

From Abyankar'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) is consequence of

Proof of the tame ramification

Continuing with this process r times we obtain that $K \subseteq R_0k(\Lambda_{P_1 \cdots P_r})$ and where R_0/k is an extension such that the only possible ramified prime is $\mathfrak{p}_\infty$. Part (a) is consequence of

Proposición

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

Key fact: wild ramification

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 is based in 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.

Number fields vs function fields 1

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 $k(\Lambda_{P^2})/k$. Then $\mathrm{Gal}(k(\Lambda_{P^2})/k) = G_{P^2}$. We have that G_{P^2} is isomorphic to the direct product of $\mathrm{Gal}(k(\Lambda_{P^2})/k) = D_{P,P^2}$ with $H := \mathrm{Gal}(k(\Lambda_P)/k) \cong C_{q^d-1}$.

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

Number fields vs function fields 2

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 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.

Gabriel Villa Salvador

Main reduction step 1

We now study wild ramification. Thus, we have to show that if L/k is a cyclic extension of degree p^n for some $n \in \mathbb{N}$ we have to show that $L \subseteq \mathbb{F}_{q^{p^n}} k_{P^\alpha} k_m$ for some $\alpha, m \in \mathbb{N}$.
The main simplification is given next on Witt generation of cyclic extensions where we separate the ramification prime by prime.

Main reduction step 2

Theorem

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 $f_j \notin \mathbb{F}_q$. $\square$

What remains to prove

Cases (c) and (d) follow from (b) and the above theorem, so the Kronecker–Weber Theorem will follow if we prove:

What remains to prove

Cases (c) and (d) follow from (b) and the above theorem, so the Kronecker–Weber Theorem will follow if we prove:

"Every cyclic extension K/k of degree p^n where $P \in R_T^+$ is the only ramified prime, P is fully ramified and $\mathfrak{p}_\infty$ is fully decomposed, satisfies that $K \subseteq k_{P^\beta} = k(\Lambda_{P^\beta})$ for some $\beta \in \mathbb{N}$."

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.

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

$$q^{d(\alpha - \lceil \frac{\alpha}{P^{n-1}} \rceil)} \left(q^{d(\lceil \frac{\alpha}{p^{n-1}} \rceil - \lceil \frac{\alpha}{p^n} \rceil)} - 1 \right). \tag{6.1}$$

Subgroups of order p^n in G_{P^α}

As a consequence we obtain

Proposición

The number $v_n(\alpha)$ of cyclic groups of order p^n contained in $\big(R_T/(P^\alpha)\big)^*$ is

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

□

Artin–Schreier extensions

Note that any $K \subseteq k(\Lambda_{P^\alpha})$ has conductor $\mathfrak{f}_K$ a divisor of P^α. Next, we compute the number of cyclic extensions K of k of degree p using the Theory of Artin–Schreier, such that P is the only ramified prime, $\mathfrak{p}_\infty$ decomposes and the conductor $\mathfrak{f}_K$ divides P^α. 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 $\lambda \leq \alpha - 1$.

Number of Artin–Schreier extensions with given conductor and in normal form

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

Number of Artin–Schreier extensions with given conductor and in normal form

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

$$\omega(\alpha) = \sum_{\substack{\lambda=1 \\ \gcd(\lambda,p)=1}}^{\alpha-1} \Phi(P^{\lambda - \left[\frac{\lambda}{p}\right]}). \tag{6.2}$$

Number of Artin–Schreier extensions with given conductor and in normal form

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

$$\omega(\alpha) = \sum_{\substack{\lambda=1 \\ \gcd(\lambda,p)=1}}^{\alpha-1} \Phi(P^{\lambda-\left[\frac{\lambda}{p}\right]}). \tag{6.2}$$

Computing (6.2) and comparing with last proposition we obtain $\frac{\omega(\alpha)}{p-1} = v_1(\alpha)$.

Gabriel Villa Salvador

In other words, every cyclic extensions 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.

Case $n = 1$

In other words, every cyclic extensions 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 $k(\Lambda_{P^\alpha})$.

Case $n = 1$

In other words, every cyclic extensions 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 on induction on n. The case $n = 1$ is the case of Artin–Schreier extensions.

Induction hypothesis

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 $\vec{\beta} = (\beta_1, \dots, \beta_n)$, that is, $K_n = k(\vec{y})$ with $\wp\vec{y} = \vec{y}^p - \vec{y} = \vec{\beta}$ and $\vec{\beta}$ written is the normal form described by Schmid. Then K_{n-1}/k is given by the Witt vector $\vec{\beta}' = (\beta_1, \dots, \beta_{n-1})$.

Case $n-1$

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

$$\beta_i = \frac{Q_i}{P^{\lambda_i}} \quad \text{where} \quad Q_i = 0, \quad \text{that is,} \quad \beta_i = 0 \quad \text{or}$$
$$\gcd(Q_i, P) = 1, \quad \deg Q_i < \deg P^{\lambda_i},$$
$$\lambda_i > 0 \quad \text{and} \quad \gcd(\lambda_i, p) = 1.$$

Case $n-1$

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

$$\beta_i = \frac{Q_i}{P^{\lambda_i}} \quad \text{where} \quad Q_i = 0, \quad \text{that is,} \quad \beta_i = 0 \quad \text{or}$$
$$\gcd(Q_i, P) = 1, \quad \deg Q_i < \deg P^{\lambda_i},$$
$$\lambda_i > 0 \quad \text{and} \quad \gcd(\lambda_i, p) = 1.$$

Since P is fully ramified, $\lambda_1 > 0$. The next step is to find the number of different extensions 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

Witt equation

$$\wp y_n = y_n^p - y_n = z_{n-1} + \beta_n \tag{6.3}$$

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 $z_0 = 0$.

Case $n-1$ second part

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}.

Case $n-1$ second part

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

$$pM_{n-1} \leq \alpha - 1, \quad \lambda_n \leq \alpha - 1 \quad \text{and}$$
$$\mathfrak{f}_{K_{n-1}} \mid P^{\delta} \quad \text{with} \quad \delta = \left[\frac{\alpha-1}{p}\right] + 1.$$

By the induction hypothesis, the number of such fields K_{n-1} is $v_{n-1}(\delta)$.

Case n

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

Case n

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

$$\frac{v_n(\alpha)}{v_n(\delta)} = \frac{q^{d(\alpha - \lceil \frac{\alpha}{p} \rceil)}}{p}. \tag{6.4}$$

Repetitions

Considering the case $\beta_n = 0$, the number of fields K_n containing a fixed field K_{n-1} obtained in (6.2) 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 (6.2) we obtain

Repetitions

Considering the case $\beta_n = 0$, the number of fields K_n containing a fixed field K_{n-1} obtained in (6.2) is

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

Finally, with the substitution $y_n \mapsto z := y_n + jy_1$, $j = 0, 1, \ldots, p-1$ in (6.2) we obtain

$$\wp z = z^p - z = \beta_n + j\beta_1.$$

The miracle

That is, each extension obtained in (6.2) 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 $\frac{1+\omega(\alpha)}{p} = \frac{1}{p} q^{d(\alpha - \lceil \frac{\alpha}{p} \rceil)}$ of such extensions K_n. From equation (6.4) we obtain

The miracle

That is, each extension obtained in (6.2) 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 $\frac{1+\omega(\alpha)}{p} = \frac{1}{p} q^{d(\alpha - \lceil \frac{\alpha}{p} \rceil)}$ of such extensions K_n. From equation (6.4) we obtain

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

The miracle

That is, each extension obtained in (6.2) 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 $\frac{1+\omega(\alpha)}{p} = \frac{1}{p} q^{d(\alpha - \left\lceil \frac{\alpha}{p} \right\rceil)}$ of such extensions K_n. From equation (6.4) we obtain

$$\begin{aligned} t_n(\alpha) &\leq t_{n-1}(\delta)\left(\frac{1}{p} q^{d(\alpha - \left\lceil \frac{\alpha}{p} \right\rceil)}\right) \\ &= v_{n-1}(\delta)\left(\frac{1}{p} q^{d(\alpha - \left\lceil \frac{\alpha}{p} \right\rceil)}\right) = v_n(\alpha). \end{aligned}$$

This proves part (b) and the Theorem of Kronecker–Weber.

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

References

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

Carlitz, Leonard, *A class of polynomials*, Trans. Amer. Math. Soc. **43** (1938), 137–168.

References

- Carlitz, Leonard, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. **1** (1935), 137–168.
- Carlitz, Leonard, *A class of polynomials*, Trans. Amer. Math. Soc. **43** (1938), 137–168.
- Hayes, David R., *Explicit Class Field Theory for Rational Function Fields*, Trans. Amer. Math. Soc. **189** (1974), 77–91.

References

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

Carlitz, Leonard, *A class of polynomials*, Trans. Amer. Math. Soc. **43** (1938), 137–168.

Hayes, David R., *Explicit Class Field Theory for Rational Function Fields*, Trans. Amer. Math. Soc. **189** (1974), 77–91.

Hilbert, David, *Ein neuer Beweis des Kronecker'schen Fundamentalsatzes über Abel'sche Zahlkörper*, Nachr. Ges. Wiss. zu Gottingen **1** (1896/97), 29–39.

References 2

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.

References 2

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

References 2

- 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.
- Kronecker, Leopold, *Über Abelsche Gleichungen*, Monatsber. Akad. Wiss. zu Berlin 1877, 845–851 = Werke, vol. **4**, Leipzig–Berlin 1929, 65–71.
- Neumann, Olaf, *Two proofs of the Kronecker–Weber theorem "according to Kronecker, and Weber"*, J. Reine Angew. Math. **323** (1981), 105–126.

References 3

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.

References 3

- 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.
- Salas–Torres, Julio Cesar, Rzedowski–Calderón, Martha and Villa–Salvador, Gabriel Daniel, *Artin–Schreier and Cyclotomic Extensions*, to appear in JP Journal of Algebra, Number Theory and Applications.

References 4

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

References 4

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

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

References 4

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

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

Weber, Henrich, *Theorie der Abel'schen Zahlkörper. I: Abel'sche Korper und Kreiskörper; II: Über die Anzahl der Idealklassen und die Einheiten in den Kreiskorpern, deren Ordnung eine Potenz von 2 ist; III: Der Kronecker'sche Satz*, Acta math. **8** (1886), 193–263

WEBER, HENRICH, *Zur Theorie der zyklischen Zahlkörper*, Math. Annalen **67** (1909), 32–60; Zweite Abhandlung ibidem **70** (1911), 459–470.

References 5

- Weber, Henrich, *Zur Theorie der zyklischen Zahlkörper*, Math. Annalen **67** (1909), 32–60; Zweite Abhandlung ibidem **70** (1911), 459–470.
- Villa Salvador, Gabriel Daniel, Topics in the theory of algebraic function fields, Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, 2006.