RAMIFICATION IN SOME NON-GALOIS EXTENSIONS OF FUNCTION FIELDS

by

ÖZGÜR DENİZ POLAT

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabancı University
Fall 2009

RAMIFICATION IN SOME NONE-GALOIS EXTENSIONS OF FUNCTION FIELDS

APPROVED BY

Prof. Dr. Henning Stichtenoth .....
(Thesis Supervisor)

Prof. Dr. Alev Topuzoğlu .....

Assist. Prof. Dr. Cem Güneri .....

Assoc. Prof. Dr.Özgür Gürbüz .....

Assoc. Prof. Dr.Wilfreid Meidl .....

DATE OF APPROVAL: 05/02/2009

RAMIFICATION IN SOME NON-GALOIS EXTENSIONS OF FUNCTION FIELDS

Özgür Deniz Polat

Mathematics, Master Thesis, 2009

Thesis Supervisor: Prof. Dr. Henning Stichtenoth

Keywords: Function fields, Galois group, ramification index, different exponent.

Abstract

Throughout this thesis, we denote by k an algebraically closed field of characteristic $p > 0$, and $K\ /k$ is a function field over k. We consider extensions $L = K(r)$, where r is a root of one of the following,

$$f(x) = x^p - bx - d \tag{1}$$

$$f(x) = x^p - bx^{p-1} - d \tag{2}$$

with $b, d \in K\ \backslash\{0\}$. For each polynomial listed above, we will describe ramification behavior of places P of K in the extension L/K, i.e. we will determine ramification index and different exponent of the places P' of L lying above P.

FONKSİYON CİSİMLERİNİN GALOIS OLMAYAN BAZI GENİŞLEMELERİNDE DALLANMA DAVRANIŞLARI

Matematik, Yüksek Lisans Tezi, 2009

Tez Danışmanı: Prof. Dr. Henning Stichtenoth

Anahtar Kelimeler: fonksiyon cisimleri, Galois grup, dallanma değeri, fark kuvveti

Özet

Bu tez boyunca k cebirsel olarak kapalı, karakteristiği $p > 0$ olan bir cisim olarak kabul edilmiştir ve K, k üzerinde tanımlı bir fonksiyon cismidir. L, K cisminin aşağıdaki polinomlardan birinin köü tarafından üretilmiş bir cisim genişlemesidir

$$f(x) = x^p - bx - d \tag{1}$$

$$f(x) = x^p - bx^{p-1} - d \tag{2}$$

ve b, d K'nın sıfırdan farklı elemanlarıdır

Yukarıda yer alan her iki polinom içinde K fonksiyon cismine ait maksimal yerel halkaların maksimal özleklerinin L/K daki dallanma davranışlarınıinceleyeceğiz. Bir diğer anlamıyla dallanma değerini ve fark kuvvetini belirleyeceğiz.

Orhan Bey'e

Acknowledgments

I want to thank Prof. Dr. Henning Stichtenoth for changing his decision.

Table of Contents

Introduction

Throughout this thesis, we denote by k an algebraically closed field of characteristic $p > 0$, and $K\ /k$ is a function field over k. We consider extensions $L = K(r)$, where r is a root of one of the following,

$$f(x) = x^p - bx - d \tag{1}$$

$$f(x) = x^p - bx^{p-1} - d \tag{2}$$

with $b, d \in K \setminus \{0\}$. For each polynomial listed above, we will describe ramification behavior of places P of K in the extension L/K, i.e. we will determine ramification index and different exponent of the places P' of L lying above P. This thesis will be organized as follows. In chapter 1, we will give some basic definitions and results which will be frequently used throughout this thesis and recall briefly the case where

$$f(x) = x^n - c \quad \text{with } 0 \neq c \in K \text{ and } p \nmid n \tag{3}$$

$$f(x) = x^p - bx - c \quad \text{with } 0 \neq b \in k \text{ and } c \in K \tag{4}$$

These cases are well-known. In case (3) the extension L/K is a Kummer extension. In case (4) it is an Artin-Schreier extension. In chapter 2, we will consider the polynomial (1). Chapter 3 will be devoted to the investigation of ramification behavior of L/K in case (2).

In case (1) and (2), the extension L/K is in general not Galois. As a first step,we will describe the Galois group of the splitting field F of $f(x)$ over K, and then we will use information about F/K to determine the ramification behavior of places in the extension L/K.

1

Preliminaries

In this chapter, we will give some definitions and facts from the theory of function fields which will be used frequently.

Let L be an algebraic extension of a function field K. Let O_P denote the local ring of K corresponding to the place P of K. A place $P'$of L is said to lie over P, if $O_P \subseteq O_{P'}$, and in this case we write $P' \mid P$. We denote by $\mathbb{P}_K$ the set of all places of K.

Definition 1.1. Let L be an extension of K and P' be a place of L that lies over P. Then there is a positive integer $e(\ P' \mid P) = e$ such that $v_{P'}(x) = e(\ P' \mid P).v_P(x)$ for all $x \in K$. Such e is called ramification index of P' over P. Given a place P of a function field K we denote by K_P the field O_P/P. If $P' \mid P$ in the extension L/K, then the degree $[L_{P'} : K_P]$ is denoted $f(P' \mid P)$.

Theorem 1.2. *Let L be a finite separable extension of K .*

a) Any place P of K has at least one but only finitely many extensions in L. Furthermore if $P_1, ..., P_k$ are all extensions of P in L, then

$$[L : K] = \sum_{i=1}^{k} e(P_i \mid P).f(P_i \mid P) \tag{1.1}$$

Proof. See [5, p.64] □

Now we will give some properties of different exponent and ramification index in a tower of function fields. For the proof see [5, p.62, p.88]

Theorem 1.3. *Let $F \supseteq L \supseteq K$ be a tower of finite separable extensions. If P'' (respectively P', P) are places of F (resp. L, K) with $P'' \supseteq P' \supseteq P$, then the following hold:*

a) $e(P'' \mid P) = e(P'' \mid P') \cdot e(P' \mid P)$

b) $d(P'' \mid P) = e(P'' \mid P') \cdot d(P' \mid P) + d(P'' \mid P')$

Kummer and Artin-Schreier extensions

In this part, we will consider the cases where the polynomial $f(x)$ has the form (3) or (4). In these cases the extension $L = K(r)$ with $f(r) = 0$) is Galois. The following results are well known. See [5, p.110]

Theorem 1.4 (Kummer extensions)**.** *Let $L = K(r)$ where r is a root of the polynomial*

$$f(x) = x^s - c \qquad \text{with } 0 \neq c \in K \text{ and } p \nmid s$$

Let $n = \min\left\{l \geq 1 \mid r^l \in K\right\}$. Then we have

a) The polynomial $\Phi(T) = T^n - r^n$ is the minimal polynomial of r over K. The extension L/K is Galois of degree n and n divides s; its Galois group is cyclic, and all automorphism of L/K are given by $\sigma(r) = \zeta.r$ where ζ is an n-th root of unity.

b) Let $P \in \mathbf{P}_K$ and $P' \in \mathbf{P}_L$ be an extension of P. Then

$$e(P' \mid P) = \frac{n}{r_P} \quad \text{and } d(P' \mid P) = \frac{n}{r_P} - 1$$

where r_P=gcd$(n, v_P(r^n)) > 0$.

Theorem 1.5 (Artin-Schreier extensions)**.** *Let $L = K(r)$ with $f(r) = 0$ where*

$$f(x) = x^p - bx - c \qquad \text{with } 0 \neq b \in k \text{ and } 0 \neq c \in K$$

Assume that $c \neq w^p - bw$ for all $w \in K$. We define an integer m_P by

$$m_P := \begin{cases} m & \text{if there is an element } z \in F \text{ satisfying} \\ & v_P(u - (z^p - z)) = -m < 0 \text{ and } m \not\equiv 0 \bmod p, \\ -1 & \text{if } v_P(u - (z^p - z)) \geq 0 \text{ for some } z \in F. \end{cases}$$

Then we have:

a) L/K is a cyclic Galois extension of degree p.

b) m_P is a well defined integer and P is unramified in L/K iff $m_P = -1$

c) P is totally ramified in L/K iff $m_P > 0$. Denote P' the unique place of L lying over P. Then the different exponent $d(P' \mid P)$ is given by

$$d(P' \mid P) = (p-1) \cdot (m_P + 1)$$

2

On the polynomial $f(x) = x^p - bx - d$

In this chapter we assume that the polynomial $f(x)$ has this form

$$f(x) = x^p - bx - d$$

with $b, d \in K \setminus \{0\}$. As usual $L = K(r)$ with $f(r) = 0$. Let $\overline{K} \supseteq L$ be an algebraic closure of K and choose $b_1 \in \overline{K}$ with

$$b_1^{p-1} - b = 0$$

The extension $K(b_1)/K$ is a cyclic extension of degree n with $n \mid (p-1)$, by Theorem 1.4. Let $F = K(b_1, r)$. Then we have:

Theorem 2.1. *With notation as above;*

a) $F = K(b_1, r)$ is the splitting field of $f(x)$ over K, hence F/K is Galois.

b) Let $n = [K(b_1) : K]$. Then $n = \min\left\{l \geq 1 \mid b_1^l \in K\right\}$.

Furthermore n divides $p-1$, and $g(x) = x^n - b_1^n \in K[x]$ is the minimal polynomial of b_1 over K.

c) $f(x)$ is reducible over K iff $d = w^p - bw$ for some $w \in K$. If this holds, then

$$Gal(F/K) \simeq C_n$$

where C_n is the cyclic group of $n-th$ roots of unity in $\mathbf{F}_p$

d) Assume that $f(x)$ is irreducible over K. Then

$$Gal(F/K) \simeq C_n \ltimes \mathbf{F}_p$$

and the group structure of $C_n \ltimes \mathbf{F}_p$ is defined by

$$(\zeta_1, \varepsilon_1)(\zeta_2, \varepsilon_2) = (\zeta_1\zeta_2, \varepsilon_2\zeta_1 + \varepsilon_1)$$

Proof. *a)* Assume that $r_1, ..., r_p \in \overline{K}$ are the roots of $f(x)$. Then for $1 \leq i, j \leq p$

$$r_i^p - br_i - d = 0 \tag{2.1}$$

$$r_j^p - br_j - d = 0 \tag{2.2}$$

Hence subtracting (2.2) from (2.1) we obtain that

$$(r_i - r_j)^{p-1} = b \tag{2.3}$$

Let $r_1 = r$ be fixed. Let b_1 be a root of $\Phi(T) = T^{p-1} - b$. We know that the roots of $\Phi(T)$ are $\delta b_1, ..., \delta^{p-1} b_1$ where δ is a primitive $(p-1) - th$ root of unity. Hence by (2.3) we conclude that $r, r + \delta b_1, ..., r + \delta^{p-1} b_1$ are roots of $f(x)$. Therefore, if we denote by F the splitting field of $f(x)$, then $F \subseteq K(r, b_1)$. Conversely since F is the splitting field of $f(x)$, then $r, r_j \in F$ hence $(r - r_j) = \delta b_1 \in F$. So $F \supseteq K(r, b_1)$ and we conclude that $F = K(r, b_1)$.

b) This is clear by Theorem 1.4.

c) First we will show that if $d = w^p - bw$ for some $w \in K$, then $f(x)$ is reducible. To see this look at $f(x)$ Since $d = w^p - bw$, then

$$\begin{aligned} f(x) &= x^p - bx - (w^p - bw) \\ &= (x + w)^p - b(x + w) \\ &= (x + w)((x + w)^{p-1} - b) \end{aligned}$$

Hence $f(x)$ is reducible.

Next we will show that if $f(x)$ is reducible, then there is $w \in K$ such that $w^p - bw = d$. Consider the factorization of $f(x)$ in $K[b_1]$.

$$f(x) = x^p - bx - d = b_1^p [(\frac{x}{b_1})^p - (\frac{x}{b_1}) - \frac{d}{b_1^p}] \tag{2.5}$$

Let $g(x)$ be the following polynomial

$$g(x) = x^p - x - \frac{d}{b_1^p}$$

Hence $\frac{r}{b_1}$ is a root of $g(x)$. On the other hand $K(b_1, \frac{r}{b_1}) = K(b_1, r) = F$. It is clear that $g(x)$ irreducible over $K[b_1]$ iff $f(x)$ is irreducible over $K[b_1]$. Since by assumption $f(x)$ is reducible over $K(b_1)$, then $g(x)$ is also reducible over $K(b_1)$. But we know that if $g(x)$ is reducible, then $g(x)$ has a root in $K(b_1)$, hence all roots of $g(x)$ are in $K(b_1)$. Therefore $K(r, b_1) = K(b_1)$. Now we have two cases: Either $K(r)$ is contained properly in $K(b_1)$, or $K(b_1) = K(r)$

Consider the first case. To obtain a contradiction assume that $f(x)$ has no root in K. So $[K(r) : K] \geq 2$. Since $K(r)$ is contained in $K(b_1)$ which is a cyclic extension of K, $K(r)/K$ is a normal extension. So by (a) $r + wb_1$ must be contained in $K(r)$ for some $w \in \mathbf{F}_p^*$. Hence b_1 must be contained in $K(r)$ which contradict the assumption that $K(r)$ is contained in $K(b_1)$ properly.

Now assume that $K(b_1) = K(r)$. First we claim that for any $w \in \mathbf{F}_p^*$ either $K(r + wb_1) = K(r)$ or $K(r + wb_1) = K$. To see this recall that $r + wb_1$ are roots of $f(x)$ and

$K(b_1)$ is the splitting field of $f(x)$. Hence $K(r+wb_1) \subseteq K(b_1) = K(r)$. If $K(r+wb_1) \neq K$ then the degree of the minimal polynomial $h(x)$ of $r + wb_1$ is greater than 1, and since $K(b_1)/K$ is cyclic, $K(r + wb_1)/K$ is a normal extension. Therefore $r + \delta b_1$ must be also in $K(r + wb_1)$ for some $\delta \in \mathbf{F}_p^*$, so b_1 must be in $K(r + wb_1)$. Now we obtain that if $K(r+wb_1) \neq K$, then $K(r+wb_1) = K(r)$. It follows that if $t(x) \in K[x]$ divides $f(x)$, then the degree of $t(x)$ is either n or 1. Since by assumption $f(x)$ is reducible with degree p, we conclude that there exist a root of $f(x)$ in K.

We know by Theorem 1.4 that $K[b_1]/K$ is a Kummer extension and its Galois group is isomorphic to C_n.

d) Now we will show that if $f(x)$ is irreducible then $Gal(F/K)$ is isomorphic to $C_n \ltimes \mathbf{F}_p$

Let G be the Galois group $Gal(F/K)$ and H be the subgroup of G that fixes $K(b_1)$. So $H = Gal(F/K(b_1))$. Since $K(b_1)/K$ is a normal extension and $[F : K(b_1)] = p$, by fundamental theorem of Galois theory H is a normal subgroup of G with order p. Note that $|H|$ and $|G/H|$ are prime to each other, hence by Hall theorem [1, p.113] H has a complement in G i.e. there is a subgroup N of G such that $N \cap H = 1$ and $G = NH$. Furthermore $N \simeq G/H$. But we know by the fundamental theorem of Galois theory $G/H \simeq Gal(K(b_1)/K)$. Hence we obtain that

$$G \simeq Gal(K(b_1)/K) \ltimes Gal(F/K(b_1))$$

Now $N \cap H = 1$ implies that every element $g \in G$ can be considered as a pair $g = (\sigma_i, \psi_j)$ where $\sigma_i \in Gal(K(b_1)/K)$ and $\psi_j \in Gal(F/K(b_1))$. By theorem 1.5 we know that $\sigma_i(b) = \zeta b$ where ζ is $n-th$ root of unity and by Theorem 1.5 $\psi_j(\frac{r}{b_1}) = \frac{r}{b_1} + \varepsilon_s$ for some $\varepsilon_s \in \mathbf{F}_p$. But since $\psi_j \in Gal(F/K(b_1))$, it fixes b_1

$$\psi_j(\frac{r}{b_1}) = \frac{\psi_j(r)}{\psi_j(b_1)} = \frac{\psi_j(r)}{b_1} = \frac{r + b_1\varepsilon_s}{b_1}$$

Therefore $\psi(r) = r + b_1\varepsilon_s$. Clearly $g(b_1) = \sigma_i(b_1)$, and $g(r) = \psi_j(r)$. Let σ and ψ be generators of the cyclic groups, $Gal(K(b_1)/K)$ and $Gal(F/K(b_1))$ respectively. If $\sigma(b_1) = \zeta b_1$ and $\psi(r) = r + \varepsilon b_1$, $\varepsilon \in \mathbf{F}_p$ then $\sigma^i(b_1) = \zeta^i b_1$ for $0 \leq i \leq n$ and $\psi^j(r) = r + j \cdot \varepsilon b_1$, for $1 \leq j \leq p$. Consider for a fixed i, the map:

$$\sigma_*^i : Gal(F/K(b_1)) \longrightarrow Gal(F/K(b_1))$$

$$\sigma_*^i(\psi^j)(r) := r + j.\varepsilon\sigma^i(b_1)$$

We want to show that this is an automorphism of $Gal(F/K(b_1))$. First note that this is a group homomorphism. Because

$$\sigma_*^i(\psi^j \cdot \psi^k)(r) = \sigma_*^i(\psi^{j+k})(r) = r + (j + k) \cdot \varepsilon\sigma^i(b_1)$$

$$= r + j \cdot \varepsilon\sigma^i(b_1) + k \cdot \varepsilon\sigma^i(b_1)$$

Note that ψ^j ψ^k fix $\varepsilon\sigma^i(b_1) \in K(b_1)$. So

$$\sigma_*^i(\psi^j \cdot \psi^k)(r) = \sigma_*^i(\psi^j) \cdot \sigma_*^i(\psi^k)(r).$$

Also $\sigma_*^i(Id)(r) = r + 0 \cdot \sigma^i(b_1) = Id(r)$. Since $Gal(F/K(b_1))$ has order p, σ_*^i are automorphisms of $Gal(F/K(b_1))$ for $1 \leq i \leq n$. Using this we can compute multiplication of two elements of G.

$$(\sigma^i, \psi^j)(\sigma^k, \psi^l)(b_1) = (\sigma^i, \psi^j)\sigma^k(b_1) = \sigma^i\sigma^k(b_1)$$

and

$$(\sigma^i, \psi^j)(\sigma^k, \psi^l)(r) = (\sigma^i, \psi^j)\psi^l(r) = (\sigma^i, \psi^j)(r + l.w.b_1) = \psi^j(r) + \sigma^i(l.w.b_1)$$

$$= r + j \cdot wb_1 + l \cdot w \cdot \sigma^i(b_1) = \psi^j(\sigma_*^i(\psi^l))(r)$$

Therefore we obtain that $(\sigma^i, \psi^j)(\sigma^k, \psi^l) = (\sigma^i\sigma^k, \psi^j(\sigma_*^i(\psi^l))$. □

Definition 2.2. A transitive permutation group in which only the identity fixes more than one letter, but the subgroup fixing one element is nontrivial, is called Frobenius group.

Remark 2.3. Assume that $f(x)$ is irreducible. Let X be the set of the roots of $f(x)$. Note that $Gal(F/K)$ acts on X transitively. Note also that the subgroup $Gal(F/K\,(b_1))$ of $Gal(F/K)$ acts on X transitively. On the other hand $Gal(F/K(r))$ fixes r by Theorem 2.1. Hence we can conclude that $Gal(F/K)$ has a nontrivial subgroup that fixes one letter. Now we claim that only identity fixes more then one letter. Let $\sigma \in Gal(F/K)$ be an element that fixes more than one root of $f\,(x)$. For simplicity assume that r and $r + wb_1$ is fixed by σ, *i.e.* $\sigma(r) = r$ and $\sigma(r + wb_1) = r + wb_1$. Now we obtain the following:

$$r + wb_1 = \sigma(r + wb_1) = \sigma(r) + w\sigma(b_1)$$

By the above equality we conclude that σ fixes also b_1. Therefore σ must be the identity.

Theorem 2.4. *Let G be Frobenius group and let H be a subgroup of G that fixes one letter. Then the following hold:*

a) The subset of G consisting of the identity together with those elements which fix no letters forms a normal subgroup K of G of order $\mid G : H \mid$.

b) $G = H.K$ and $H \cap K = 1$.

c) $H \cap gHg^{-1} = Id$ for $g \notin H$ and $N_G(H) = H$.

d) $|H|$ divides $|K| - 1$

Proof. See [2, p. 38] □

Definition 2.5. Let π be a set of primes. A group G is called $\pi-$group, if the order of G is divisible only by primes in π. A subgroup H of G is called an S_π- subgroup of G provided that H is a $\pi-$group and the index $G : H$ is divisible by no primes in π.

Theorem 2.6. *Let G be a solvable group. Then*

a) G possesses an S_π- subgroup for any set of primes π

b) Any two S_π- subgroups of G are conjugate

c) Any $\pi-$subgroup of G is contained in an S_π- subgroup.

Proof. See [2, p. 231] □

Theorem 2.7. *Let H be a normal subgroup of a group G. If both H and G/H are solvable, then G is solvable.*

Proof. See [2, p.23] □

Remark 2.8. Note that $G = Gal(F/K)$ is solvable. To see this recall that $Gal(F/K(b_1))$ is normal in G with cyclic group of order p, hence it is solvable. On the other hand $G/Gal(F/K(b_1))$ is a cyclic group of order n. We know that abelian groups are solvable. Therefore by Theorem 2.5 we conclude that G is solvable.

Proposition 2.9. *Let $f(x)$ be as above and assume that $f(x)$ is irreducible. Let P be a ramified place of K in L/K. Then P is totally ramified in L.*

Proof. Assume that P is not totally ramified in L. Let P' be an extension of P in L such that $e(P' \mid P) > 1$. By assumption P is ramified in L so there exist such P'. Let $Q_1, .., Q_s$ be the places of F that lie over P'. Since F/L is Galois with extension degree n, then $e(Q_i \mid P')$ divides n. Note that $e(Q_i \mid P') = e(Q_j \mid P')$ for $1 \leq i, j \leq s$. Clearly $Q_1, .., Q_s$ lies over P in F/K with ramification index

$$e(Q_i \mid P) = e(Q_i \mid P') \cdot e(P' \mid P)$$

On the other hand, since F/K is Galois, $e(Q_i \mid P)$ must divide $[F : K]{=}n \cdot p$. By assumption P is not totally ramified in L. Hence $e(Q_i \mid P)$ must divides n. Let $G_T(Q_i \mid P)$ denote the inertia group of Q_i over P. It can be shown that

$$e(Q_i \mid P) = |G_T(Q_i \mid P)|$$

see details [5, p.119].

Recall that k is algebraically closed. So $f_i = [\mathbf{F}_{Q_i} : \mathbf{F}_P] = 1$ for $1 \leq i \leq s$. By Theorem III.8.2 in [5, p.119],

$$f_i = |G_Z(Q_i \mid P)| \,/\, |G_T(Q_i \mid P)| \tag{2.3}$$

Hence the decomposition group of Q_i over P is the inertia group of Q_i over P. Now we fix one of them, say Q_1. Let T be the fixed field of $G_Z(Q_1 \mid P)$. We claim that T contains L. To prove this claim, we need to show that

$$G_Z(Q_1 \mid P) \subseteq Gal(F/L) \tag{2.4}$$

Since the fixed field of $Gal(F/L)$ is L and (2.4) implies that $T \supseteq L$. It can be shown that $e(Q_1 \mid P) = e(Q_1 \mid Q_T)$ where Q_T is the restriction of Q_1 to T. For details see [5, p.119]. Since Q_T lies over P, $e(Q_T \mid P)$ must be 1 by Theorem 1.3. In particular $e(P' \mid P) = 1$, contradicting the assumption that $e(P' \mid P) > 1$.

To show (2.4), we use the fact that $G = Gal(F/K)$ is a Frobenius group. By Remark 2.6, G is a solvable group. So any subgroup of G with order prime to p should be a subgroup of a conjugate of $Gal(F/L)$ by Theorem 2.4. Recall that

$$G_Z(Q_1 \mid P') \subseteq Gal(F/L) \tag{2.5}$$

and

$$G_Z(Q_1 \mid P') \subseteq G_Z(Q_1 \mid P) \tag{2.6}$$

Assume that $G_Z(Q_1 \mid P') \neq 1$. Since $|G_Z(Q_1 \mid P)|$ is prime to p, $G_Z(Q_1 \mid P)$ is contained in a conjugate of $Gal(F/L)$. But (2.5) and (2.6) imply that

$$G_Z(Q_1 \mid P) \cap Gal(F/L) \neq 1$$

So we conclude that $G_Z(Q_1 \mid P) \subseteq Gal(F/L)$, and the result follows.

Now we assume that $G_Z(Q_1 \mid P') = 1$. In this case $Gal(F/L)$ does not fix $Q_1, ..., Q_s$ i.e. $G_Z(Q_i \mid P') \cap Gal(F/L) = 1$ for $1 \leq i \leq s$. We also conclude that

$$G_Z(Q_1 \mid P) \cap Gal(F/L) = 1$$

Hence $G_Z(Q_1 \mid P)$ is contained in a conjugate of $Gal(F/L)$,i.e. $G_Z(Q_1 \mid P) \subseteq \sigma Gal(F/L)\sigma^{-1}$ for some $\sigma \in H$. Let $\sigma^i(Q_1) \restriction_L$denote the restriction of $\sigma^i(Q_1)$ to the field L. Now we claim that $\sigma^i(Q_1) \restriction_L \neq \sigma^j(Q_1) \restriction_L$ unless $i = j$.

First we will show that $\sigma(Q_1) \restriction_L \neq P'$. Since $G_Z(Q_1 \mid P) \subseteq \sigma^{-1}Gal(F/L)\sigma$ there is an element $\varphi \neq 1$ in $Gal(F/L)$ such that $\sigma^{-1}\varphi\sigma(Q_1) = Q_1$. So

$$\varphi(\sigma(Q_1)) = \sigma(Q_1)$$

If $\sigma(Q_1) \restriction_L = P'$, then $\sigma(Q_1) = Q_h$ for some $h \in \{1, .., s\}$, hence φ fixes Q_h which contradicts the fact that $Gal(F/L) \cap G_Z(Q_h \mid P') = 1$. Therefore $\sigma(Q_1) \restriction_L \neq P'$. On the other hand if $\sigma^i(Q_1) \restriction_L = \sigma^j(Q_1) \restriction_L$, and $i > j$ then $\sigma^{i-j} \in G_Z(\sigma^j(Q_1)/\sigma^j(Q_1) \restriction_L)$. But $\sigma \in H$. So σ^{i-j} is also a generator of H with order p i.e. $H \subseteq G_Z(\sigma^j(Q_1) \mid \sigma^j(Q_1) \restriction_L)$. This contradicts the fact that $|G_Z(\sigma^j(Q_1)/\sigma^j(Q_1) \restriction_L)|$ is prime to p. Thus we obtain that $\sigma^i(Q_1) \restriction_L \neq \sigma^j(Q_1) \restriction_L$, so there are p distinct places of L that lie over P. This contradicts the fact that P is ramified in L. □

Remark 2.10. Assume that there exists a place P of K such that $v_P(d)$ is prime to p and $(p-1) \cdot v_P(d) < p \cdot v_P(b)$. Then $f(x)$ is irreducible. To establish this claim, let r be a root of this polynomial and consider the field $K(r)$. Let P' be an extension of P in $K(r)$. Since $f(r) = 0$ and

$$r^p - br = d,$$

then by triangle inequality

$$\min\{p.v_{P'}(r), v_{P'}(r) + v_{P'}(b)\} \leq v_{P'}(r^p + br) = v_{P'}(d). \tag{2.7}$$

Now first assume that

$$p.v_{P'}(r) = v_{P'}(b) + v_{P'}(r) \tag{2.8.}$$

Hence

$$(p-1) \cdot v_{P'}(r) = v_{P'}(b) \tag{2.9}$$

and by (2.7)

$$p \cdot v_{P'}(r) \leq v_{P'}(d) \tag{2.10}$$

Combining (2.9) with our assumption that $(p-1) \cdot v_P(d) < p \cdot v_P(b)$, we obtain the following:

$$(p-1) \cdot v_{P'}(d) < p \cdot v_{P'}(b) \Longrightarrow (p-1) \cdot v_{P'}(d) < p \cdot (p-1) \cdot v_{P'}(r)$$

So we conclude that

$$p \cdot v_{P'}(r) > v_{P'}(d)$$

Hence by (2.10), we obtain the equality $p \cdot v_{P'}(r) = v_{P'}(d) = e \cdot v_P(d)$. Since $\gcd(v_P(d), p) = 1$, we conclude that $e = p$. On the other hand $e \leq [K(r) : K] \leq p$, so $[K(r) : K] = p$ and $f(x)$ is irreducible.

For the second case, assume that (2.8) does not hold. By strict triangle inequality, $v_{P'}(d) = \min\{p.v_{P'}(r), v_{P'}(r) + v_{P'}(b)\}$. We claim that if P satisfies the condition that $(p-1) \cdot v_P(d) < p \cdot v_P(b)$, then

$$\min\{p \cdot v_{P'}(r), v_{P'}(r) + v_{P'}(b)\} = p \cdot v_{P'}(r)$$

Assume the contrary, i.e.

$$v_{P'}(r) + v_{P'}(b) = v_{P'}(d). \tag{2.11}$$

Then $p \cdot v_{P'}(r) < v_{P'}(r) + v_{P'}(b)$, hence,

$$(p-1)v_{P'}(r) < v_{P'}(b) \tag{2.12}$$

Multiplying (2.11) with $p-1$, we obtain that

$$(p-1) \cdot v_{P'}(r) + (p-1) \cdot v_{P'}(b) = (p-1) \cdot v_{P'}(d)$$

But since e is positive, by using (2.12), we conclude that

$$p \cdot v_P(b) < (p-1) \cdot v_P(d),$$

which contradicts our assumption. Therefore $p \cdot v_{P'}(r) = v_{P'}(d)$ and the result follows from the previous case.

Theorem 2.11. *Let notation be as above and P be a place of K. Then the following hold:*

a) Assume that $(p-1)\cdot v_P(d) \geq p\cdot v_P(b)$. Then P is unramified in L/K.

b) Assume that $(p-1)\cdot v_P(d) < p\cdot v_P(b)$ and $p \nmid v_P(d)$. Then P is ramified in L/K and

$$d(P'/P) = (p\cdot v_P(b) - (p-1)\cdot v_P(d)) + (p-1)$$

Proof. a) We have shown in Theorem 2.1 (a) that the splitting field of $f(x)$ over $K(b_1)$ is $F = K(b_1, r_1)$ where r_1 is a root of the irreducible polynomial $g(x)$.

$$g(x) = x^p - x - \frac{d}{b_1^p}$$

So F is an Artin−Schreier extension of $K(b_1)$. Let P be a place of K and Q be an extension of P in F. Let Q_1 be the restriction of Q to the field $K(b_1)$. Let m_{Q_1} be defined as in Theorem 1.5. We will show that if $m_{Q_1} = -1$, then P is unramified in L. By Theorem 1.5, Q_1 is unramified in F iff $m_{Q_1} = -1$. Note that if $v_{Q_1}(\frac{d}{b_1^p}) \geq 0$, then $m_{Q_1} = -1$. Now assume that $m_{Q_1} = -1$. Then $e(Q \mid Q_1) = 1$. Using Theorem 1.5, we can write :

$$e(Q \mid P) = e(Q \mid P').e(P' \mid P) = e(Q \mid Q_1).e(Q_1 \mid P)$$

Hence, we obtain that

$$e(Q \mid P) = e(Q \mid P').e(P' \mid P) \tag{2.13}$$

But since Q_1 is a place of $K(b_1)$ lying over P, and $K(b_1)$ is a Galois extension, $e(Q_1 \mid P)$ must divide $[K(b_1) : K] = n$. By (2.13) we conclude that $e(P' \mid P)$ must divide n. But we have shown in Proposition 2.7 that if P is a ramified place of K in L/K, then P must be totally ramified with ramification index p. Since p is prime to n, $e(P' \mid P)$ must be 1. Hence if $m_{Q_1} = -1$, then P is unramified.

Clearly if $v_{Q_1}(\frac{d}{b_1^p}) \geq 0$ then $m_{Q_1} = -1$. Finally, we will show that if $(p-1)\cdot v_P(d)$ $\geq p\cdot v_P(b)$, then $v_{Q_1}(\frac{d}{b_1^p}) \geq 0$. Let e_0 denote $e(Q_1|P)$. Now we will compute $v_{Q_1}(\frac{d}{b_1^p})$

$$v_{Q_1}(\frac{d}{b_1^p}) = v_{Q_1}(d) - p\cdot v_{Q_1}(b_1). \tag{2.14}$$

On the other hand since

$$b_1^{p-1} = b,$$

then

$$(p-1)\cdot v_{Q_1}(b_1) = v_{Q_1}(b) = e_0\cdot v_P(b)$$

implies that

$$v_{Q_1}(b_1) = \frac{e_0}{p-1}\cdot v_P(b) \tag{2.15}$$

Hence, combining (2.14) and (2.15), we obtain that

$$v_{Q_1}(\frac{d}{b_1^p}) = \frac{e_0}{p-1}((p-1)\cdot v_P(d) - p\cdot v_P(d)) \tag{2.16}$$

Therefore by (2.16) we conclude that, if $(p-1)\cdot v_P(d)-p\cdot v_P(b)\geq 0$ then $v_{Q_1}(\frac{d}{b_1^p})\geq 0.b)$ Let P be a place of K that satisfies the condition

$$(p-1)v_P(d) < pv_P(b) < 0.$$

Let Q denote an extension of P in F. Again we denote Q_1 (respectively P') the restriction of Q to the field $K(b_1)$ (respectively to L). Let e_o be as in a). We know by Theorem 1.5 that $e(Q \mid Q_1) = p$ iff $m_{Q_1} > 0$. Again by Theorem 1.5

$$d(Q \mid Q_1) = (p-1)(m_{Q_1}+1) \tag{2.18}$$

Using Proposition 1.2, we can compute $d(P' \mid P)$ using the two equations below.

$$d(Q \mid P) = e(Q \mid P') \cdot d(P' \mid P) + d(Q \mid P') \tag{2.19}$$

$$d(Q \mid P) = e(Q \mid Q_1) \cdot d(Q_1 \mid P) + d(Q \mid Q_1)$$

So

$$e_0 \cdot d(P'|P) + e_0 - 1 = p \cdot (e_o - 1) + (m_{Q_1}+1) \cdot (p-1)$$

$$e_0 \cdot d(P'|P) = (p-1) \cdot (e_o - 1) + (m_{Q_1}+1) \cdot (p-1)$$

Since

$$m_{Q_1} = \frac{e_0}{p-1}(p \cdot v_P(b) - (p-1) \cdot v_P(d)),$$

$$e_0 d(P'|P) = (p-1) \cdot (e_o - 1) + \ e_0((p \cdot v_P(b) - (p-1) \cdot v_P(d)) + p - 1.$$

So we obtain that

$$d(P'|P) = (p-1) + p \cdot v_P(b) - (p-1) \cdot v_P(d)$$

□

3

On the polynomial $f(x) = x^p - bx^{p-1} - d$

In this chapter we assume that the polynomial has this form

$$f(x) = x^p - bx^{p-1} - d$$

where $b, d \in K \setminus \{0\}$. As usual $L = K(r)$ with $f(r) = 0$. Let $\overline{K} \supseteq L$ be the algebraic closure of K and choose $c \in \overline{K}$ with

$$c^{p-1} - \frac{b}{d} = 0$$

The extension $K(c)/K$ is a cyclic extension of degree n where $n = \min l | c^l \in K\}$. Let $F = K(c, r)$.

Lemma 3.1. *Assume that $f(x)$ is irreducible . Then the irreducible polynomial of r^{-1} is*

$$\widetilde{f}(x) = x^p - \frac{b}{d}x - \frac{1}{d}$$

Proof. Let r is a root of $f(x)$. Then

$$r^p - br^{p-1} - d = 0. \tag{3.1}$$

Multiplying (3.1) with $\frac{1}{r^p}$, we obtain that

$$\frac{r^p}{r^p} - \frac{br^{p-1}}{r^p} - \frac{d}{r^p} = 1 - \frac{b}{r} - \frac{d}{r^p} = 0. \tag{3.2}$$

Again multiplying (3.2) with $\frac{1}{d}$, we obtain that

$$(\frac{1}{r})^p - \frac{b}{d}(\frac{1}{r}) - \frac{1}{d} = 0.$$

Since $K(r) = K(r^{-1})$ and by assumption $[K(r) : K] = p$, we conclude that $\widetilde{f}$ is the irreducible polynomial of r^{-1}. □

Corollary 3.2. *Let notation be as above, and assume that $f(x)$ is irreducible. Then the splitting field of $\widetilde{f}(x)$ is F. The Galois group $Gal(F/K)$ is isomorphic to $C_n \ltimes \mathbf{F}_p$*

Proof. Clearly $K(r^{-1}, c) = K(r, c)$. By theorem 2.1, the splitting field of $\widetilde{f}(x)$ is $K(r^{-1}, c)$. Since the splitting field of $f(x)$ and $\widetilde{f}(x)$ are the same, we conclude that F is the splitting field of $f(x)$. Again by Theorem 2.1 $Gal(F/K)$ is isomorphic to $C_n \ltimes \mathbf{F}_p$ □

Remark 3.3. Assume that there is a place P of K such that $v_P(d)$ is prime to p and $v_P(d) < pv_P(b)$. Then $f(x)$ is irreducible. To see this, first note that $f(x)$ is irreducible if and only if $\widetilde{f}(x)$ is irreducible. Subtracting $pv_P(d)$ from both sides of the above inequality, we obtain:

$$v_P(d) - pv_P(d) < pv_P(b) - pv_P(d) \tag{3.3}$$
$$(1-p)v_P(d) < pv_P(\frac{b}{d})$$

Hence P satisfies also the inequality below:

$$(p-1)v_P(\frac{1}{d}) < pv_P(\frac{b}{d}) \tag{3.4}$$

By Remark 2.3 we know that if there is a place P of K such that $(p-1)v_P(\frac{1}{d}) < pv_P(\frac{b}{d})$, then $\widetilde{f}(x)$ is irreducible. Therefore $f(x)$ is irreducible.

Corollary 3.4. *Let notation be as above and P be a place of K. Then the following hold:*

a) Assume that $v_P(d) \geq pv_P(b)$, then P is unramified in L/K.

b) Assume that $p \nmid v_P(d)$and $v_P(d) < pv_P(b)$. Then P is ramified and if P' is the unique place of L that lies over P,

$$d(P'|P) = p - 1 + p \cdot v_P(b) - v_P(d)$$

Proof. We know by Theorem 1.9, if r^{-1} is a root of $\widetilde{f}(x) = x^p - \frac{b}{d}x - \frac{1}{d}$, then for any place P of K that satisfies the condition :

$$(p-1)v_P(\frac{1}{d}) > pv_P(\frac{b}{d})$$

is unramified in $K(r^{-1})/K$. Since $K(r) = K(r^{-1})$ we conclude that if $(p-1)v_P(\frac{1}{d}) > pv_P(\frac{b}{d})$,then P is unramified in L/K. But

$$\begin{aligned}(p-1)v_P(\frac{1}{d}) &> pv_P(\frac{b}{d}) \Rightarrow (1-p)v_P(d) > pv_P(b) - pv_P(d) \\ &\Rightarrow v_P(d) > pv_P(b)\end{aligned}$$

So the result follows.

b) By Remark 3.3, we know that $v_P(d) < p \cdot v_P(b)$ implies that

$$(p-1)v_P\left(\frac{1}{d}\right) < p \cdot v_P\left(\frac{b}{d}\right) \tag{3.4}$$

By Theorem 1.1, if $v_P(\frac{1}{d})$ is prime to p and P satisfies (3.4), then P is totally ramified in $K[r^{-1}]/K$ with the different exponent

$$\begin{aligned} d(P'|P) &= (p-1) + p \cdot v_P\left(\frac{b}{d}\right) - (p-1)v_P\left(\frac{1}{d}\right) \\ &= (p-1) + p \cdot v_P(b) - v_P(d). \end{aligned}$$

□

Bibliography

[1] A.Bluher, On $x^{q+1} + ax + b$ *Finite field and Appl.* **10** (2004) 285-305.

[2] D. Gorenstein, Finite Groups, *American Mathematicial Society*, (2007).

[3] M.L Madan, R.C Valentini, A Hauptsatz of L.E.Dickson and Artin-Schreier extensions, *J.Reine Angew.Math*, **318** (1980) 156-177.

[4] S.Lang, Algebra, *Addison-Wesley Pub. Co.* (2002).

[5] H. Stichtenoth, Algebraic Function Fields and Codes, *Springer, Berlin*,(2008).