DECOMPOSITION OF PRIMES IN NON-GALOIS EXTENSIONS

by

ÖZGÜR DENİZ POLAT

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

Sabancı University
Fall 2013

DECOMPOSITION OF PRIMES IN NON-GALOIS EXTENTIONS

APPROVED BY:

Prof. Dr. Henning Stichtenoth

(Thesis Supervisor)

Prof. Dr. Alev Topuzoğlu

Prof. Dr. İlhan İkeda

A.Bassa

Asst. Prof. Dr. Alp Bassa

Assoc. Prof. Dr. Erkay Savaş

DATE OF APPROVAL: 13/01/2014

DECOMPOSITION OF PRIMES IN NON-GALOIS EXTENSIONS

Özgür Deniz Polat

Mathematics, PhD Thesis, 2013

Thesis Supervisor: Prof. Dr. Henning Stichtenoth

Keywords: Non-Galois extension, global field, prime, Galois group, double coset space, finite group of Lie type, Weyl group, length function, inertia degree, ramification index.

Abstract

In this thesis we consider the following question: Given a finite separable non-Galois extension F/K of a global field K, how a prime P of K decomposes in the field F.

In the first part, we study the Galois extension M/K where M is the Galois closure of F/K and action of Galois group G of M/K over the set of primes of F lying over a prime P in K. We obtain a one to one correspondence between the double coset space of G with respect to certain subgroups of G (depending on P and F) and the set of primes of F lying over P. Under this correspondence ramification indices and inertia degrees are explicitly determined.

Then we investigate the case where G is a finite group of Lie type and F is the intermediate field corresponding to a parabolic subgroup of G. We obtain that the number of primes of F lying over an unramified place with given residue degree can be given as polynomials in a power of the characteristic of the variety G. This polynomials depend on the length function on the certain subgroups of the Weyl group of G.

ASALLARIN SONLU CİSİM GENİŞLEMELERİNDE ÇARPANLARINA AYRILIŞI

Özgür Deniz Polat

Matematik, Doktora Tezi, 2013

Tez Danışmanı: Prof. Dr. Henning Stichtenoth

Anahtar Kelimeler: Galois olmayan genişleme, cisim, asal, Galois grup, çift koset uzayı, sonlu Lie grupları, Weyl grup, ramifikasyon derecesi, kalan derecesi

Özet

Bu tezde şu sorunun cevabını araştırdık. Verilen bir K cisminin Galois olmayan F genişlemesinde K' ın bir asalı, F'de nasıl çarpanlarına ayrılır?

İlk bölümde F/K genişlemesinin Galois kapanışı olan M cismi ve bu cismin K üzerindeki Galois grubunun K'daki herhangi bir P asalının F cismindeki asal çarpanları üzerindeki aksiyonunu inceledik. Böylelikle G'in belirli altgruplarına göre belirlenmiş çift koset uzayıyla (P ve F tarafından belirlenen) P'in F'deki asal çarpanlarından oluşan küme arasında birebir bir fonksiyon bulduk. Bu fonksiyonun görüntüsü altında P'in her bir asal çarpanı için ramifikasyon ve kalan derecelerini açıkça belirledik.

Daha sonra G'in sonlu bir Lie grup olduğu ve F'inde G'in parabolik bir altgrubuna karşılık geldiği durumu inceledik. Bu koşullar altında K'in F üzerinde ramifikasyonun olmadığı P asalları için, kalan derecesinin belli bir sayı olduğu asal çarpanlarının sayısının bir polinom şeklinde verildiğini belirledik. Bu polinom G'in üzerinde tanımlı olduğu cismin karakteristiğinin bir gücü olarak verilir ve G'in Weyl grubu üzerindeki uzunluk fonksiyonunun bu grubun belli altgrupları üzerindeki görüntüsü tarafından belirlenir.

To my grandfather and my brother Ulaş

Acknowledgments

I am grateful to everybody.

Table of Contents

CHAPTER 1

Introduction

In this thesis we are interested in the following question: Given a finite seperable extension of function fields F/K, what we can say about the decomposition of a place P of K in F? Though all results hold for any finite seperable extension of global fields, we consider K as a function field over the constant field $\mathbb{F}$.

Our motivation comes from a very interesting article of Bluher. In her work, Bluher has shown that if $\mathbb{F}_q \subseteq \mathbb{F}$, the number of roots of $\widetilde{h}(x) = x^{q+1} + ax + b$ in the field $\mathbb{F}$, $a, b \in \mathbb{F}$ is either $0, 1, 2$ or $q+1$. Her result can be interpreted in the theory of function fields as follows. If $\mathbb{F}_q \subseteq \mathbb{F}$, then in the extension $\mathbb{F}(x)/\mathbb{F}(\widetilde{h}(x))$, there are either $0, 1, 2$ or $q+1$ rational places of $\mathbb{F}(x)$ lying over the rational place P_α of $\mathbb{F}(h(x))$. In a series of papers, Abhyankar has constructed explicit polynomials $h(x)$ over $\mathbb{F}_q$ such that $\mathbb{F}(x)/\mathbb{F}(h(x))$ has Galois closure M whose Galois group $Gal(M/\mathbb{F}(h(x)))$ is a classical group defined over $\mathbb{F}_q$. In particular he has shown that when $h_n(x) = x^{\langle n-1\rangle} + x + 1$ where $\langle n-1\rangle = q^{n-1} + q^{n-2} + ... + 1$, then $Gal(M/\mathbb{F}(h_n(x))$ is isomorphic to $PGL(n, q)$ (see [1]).

In her paper, Bluher has shown that the splitting field M of $\widetilde{h}(x)$ has Galois group $G = Gal(M/\mathbb{F}(\widetilde{h}(x)))$ which is a subgroup of $PGL(2, q)$. Her method is the following: She has labeled the roots of $\widetilde{h}(x)$ as points of the projective line $\mathbb{P}^1(\mathbb{F}_q)$. Then she has constructed an action of $PGL(2, q)$ on the set of roots $S = \{r_{v_1}, ..., r_{v_{q+1}} |\ v_i \in \mathbb{P}^1(\mathbb{F}_q)\}$ of $\widetilde{h}(x)$ and this action of $PGL(2, q)$ on S is similar as on $\mathbb{P}^1(\mathbb{F}_q)$. Namely $\sigma(r_v) = r_{\sigma(v)}$ for $\sigma \in \mathbb{P}^1(\mathbb{F}_q)$ and $v \in \mathbb{P}^1(\mathbb{F}_q)$. Then he has analyzed this extension in detail and has given the result.

We have started to study any finite separable extension F of K with $Gal(M/K) \simeq PGL(2, q)$ where M is the Galois clousure of F/K. We also assume that $\mathbb{F}$ is finite. First we deal with the decomposition of unramified places P of K in F. By fundamental theorem of Galois theory the extension M/F is a Galois extension and $H = Gal(M/F)$ is a subgroup of G. Our method is to use the transitive action of G on the places R of M lying over P. We know that the restriction Q of each R to the field F is a place

Q of F lying over P and again the action of H on the places R of M lying over Q is transitive.

On the other hand, the subgroups $D := D(R|P) \subseteq G$ (respectively $D(R|Q) \subseteq H$) fixing R are cyclic by our assumption that P is unramified. By Dickson's theorem (see Theorem 2.3.12) we know all subgroups of G and their structures. We know also the number of fixed points of each element $g \in PGL(2, q)$ when acting on $\mathbb{P}^1(\mathbb{F}_q)$. Then we have observed that for any unramified place P in F/K the number of places Q of F with residue degree $f(Q|P) = 1$ is either $0, 1, 2$ or $q + 1$. After that, we have enabled to formulate the general case, i.e for any G and any place P of K we have a correspondence between the places Q of F lying over P and the double coset space $H \backslash G/D$. Furthermore we also determined ramification index $e(Q|P)$ and residue degree $f(Q|P)$ for each Q under this correspondence.

In Chapter two, first we discuss this correspondence (Theorem 2.1.4). Then since in a finite separable extension F/K there are only finitely many ramified places, we focus on the decomposition of an unramified place P in a non-Galois extension F/K. In the Galois extension M/K, each unramified place P determines a conjucagy class in G. This conjugacy class is called Artin class of P in M/K. Then using the Cheboterev Density Theorem, we have shown that the decomposition of P in F/K strongly depends on the Artin class of P in M/K and the subgroup H. In Section 2.3, we give another proof of Bluher's result using these arguments (Theorem 2.3.18). Indeed we do not just give the number of roots of $\widetilde{h}(x)$ but also give the number of irreducible factors m_i of $\widetilde{h}(x)$ of degree i over the field $\mathbb{F}$.

By the Classification Theorem of finite simple groups, we know the importance of finite groups of Lie type. In fact, almost all finite simple groups are in these classes. Therefore we have concentrated on these groups and we have investigated the decomposition of places in this extensions. Our viewpoint is to consider these groups as algebraic groups over finite fields reformulated by in terms of Frobenius endomorphisms (see Appendix, Section 2). This reformulation is given by Steinberg as follows: Let $\mathbf{G}$ be an algebraic group defined over $\overline{\mathbb{F}}_p$, and let $\mathbf{F}$ be a Frobenius endomorphism on $\mathbf{G}$. Then the subgroup $\mathbf{G}^{\mathbf{F}}$ of $\mathbf{G}$ fixed by $\mathbf{F}$ is a finite group of Lie type and all these groups arise in this way. The endomorphism $\mathbf{F}$ conveys the algebraic group structure of $\mathbf{G}$ to $\mathbf{G}^{\mathbf{F}}$. Let $\mathbf{W}$ be the Weyl group of $\mathbf{G}$. The action of $\mathbf{F}$ on $\mathbf{G}$ gives rise to an automorphism ϕ on $\mathbf{W}$.

It is well known that the identity component $C_{\mathbf{G}}(s)^0$ of the centralizer of a semisimple element $s \in \mathbf{G}$ is a connected reductive group. When s is $\mathbf{F}$-rational, then $C_{\mathbf{G}}(s)^0$ is also $\mathbf{F}$-rational. Therefore $\mathbf{F}$ also acts on the Weyl group $\mathbf{W}(s)$ of $C_{\mathbf{G}}(s)^0$ which is a subgroup of $\mathbf{W}$. This action of $\mathbf{F}$ on $\mathbf{W}(s)$ is closely related to that on $\mathbf{W}$; i.e. $\mathbf{F}$ acts on $\mathbf{W}(s)$ as the automorphism $w \circ \phi$ for some $w \in \mathbf{W}$. The subgroups $\mathbf{W}(s)(w \circ \phi)$ of $\mathbf{W}(s)$ which are fixed by $w \circ \phi$ pointwise, are our main objects. They give polynomials in q which completely determined by the length function l of $\mathbf{W}$ on $\mathbf{W}(s)(w \circ \phi)$. We here note that they are parabolic subgroups of $\mathbf{W}$ in general.

In Chapter 3, first, assuming that $H = N_G(H)$, we have given a method to determine the number m_i of places Q of F with $f(Q|P) = i$ for an unramified place P of K. Then we have assumed that G is a finite group of Lie type and H is a parabolic subgroup of G. If the Artin class of P is a conjugacy class of a semisimple element s, we have shown that the number m_i, for unramified place P can be given by a product of a polynomial in q and a factor, determined explicitly in Section 3.1. In short, the Artin class of P in M/K completely determines these polynomials. When Artin class of P is a conjugacy class of an arbitrary element $g = su$, where s semisimple, u unipotent (see Section 4.1), we also give the exact value of m_i for each i. It is the number of $\mathbf{F}$-rational points of a subvariety of certain homogeneous space, arising from a closed connected subgroup of $C_{\mathbf{G}}(s)^0/$. It can be shown that also in this case, m_i can be given in terms of polynomials determined by a subset of $\mathbf{W}(s)$ and the length function l.

In Section 3.3, we apply our arguments, to decompose the polynomials $h_n(x)$ constructed by Abhyankar.

In the Appendix we recall some facts and definitions from the theory of algebraic groups that we have used throughout this thesis.

CHAPTER 2

Group-theoretical Data Associated to Finite Non-Galois Extensions

2.1. Decomposition of Places in Non-Galois Extensions

The main result of this section (see Theorem 2.1.4 below) relates the ramification behavior of a place in a finite non-Galois extension of function fields with certain group-theoretical data of the Galois group of the Galois closure of this extension.

For the convenience of the reader, we first fix some notation. Denote by

$\mathbb{F}$ a finite field,

$\mathbb{F}_q$ the finite field of cardinality q and characteristic p,

K a function field having $\mathbb{F}$ as its full constant field,

F/K a finite separable field extension,

M/K the Galois closure of the extension F/K,

$G = \mathrm{Gal}(M/K)$ the Galois group of M/K,

$H = \mathrm{Gal}(M/F) \subseteq G$ the Galois group of M/F,

$\mathbb{P}_E$ the set of places of a function field $E/\mathbb{F}$,

$\mathcal{O}_R$ the valuation ring of the place $R \in \mathbb{P}_E$,

E_R the residue class field of the place $R \in \mathbb{P}_E$.

Let L/E be an extension of function fields. For $P \in \mathbb{P}_E$ and $Q \in \mathbb{P}_L$, we use $Q \mid P$ if $P \subseteq Q$. We denote by $e(Q|P)$ and $f(Q|P)$ the ramification index and the relative degree of $Q|P$, respectively.

Proposition 2.1.1 *Let F be a finite extension of K.*

(i) For each $Q \in \mathbb{P}_F$, there is exactly one place $P \in \mathbb{P}_K$ such that $Q|P$.

(ii) Conversely, every place $P \in \mathbb{P}_K$ has at least one, but only finitely many extensions $P' \in \mathbb{P}_F$.

Proof: See [25], Proposition 3.1.7. □

Fix a place $P \in \mathbb{P}_K$, a place $Q \in \mathbb{P}_F$ and a place $R \in \mathbb{P}_M$ such that Q lies over P and R lies over Q. We denote by $Q_1, \ldots, Q_s$ all extensions of P in F and by $R_1, \ldots, R_t$ all extensions of P in M. Without loss of generality, say $Q_1 := Q$ and $R_1 := R$.

The Galois group G acts in a natural way on the set $\{R_1, \ldots, R_t\}$. Define the following sets:

$$D := D(R|P) = \{\sigma \in G \mid \sigma(R) = R\}$$
$$I := I(R|P) = \{\tau \in G | \ \tau(\omega) \equiv \omega \ \mathrm{mod} R, \ \omega \in \mathcal{O}_R\}$$

D and I are the decomposition group and the inertia group of R/P.

We need the following facts related to these subgroups which are significant for the rest of the section.

Proposition 2.1.2 *(i) The Galois group G acts transitively on the set $\{R_1, \ldots, R_t\}$, and hence every place R_j can be written as $R_j = \sigma(R)$ for some $\sigma \in G$.*

(ii) $D(R|P)$ and $I(R|P)$ are subgroups of G of order $e(R|P) \cdot f(R|P)$ and $e(R|P)$, respectively.

Proof: See [25], Theorem 3.8.2.

Proposition 2.1.3 *Suppose that M/K is a Galois extension with the Galois group G and R is a place of M lying over a place P of K. Let $\sigma \in G$. Then $D(\sigma(R)|P) = \sigma D(R|P)\sigma^{-1}$ and $I(\sigma(R)|P) = \sigma I(R|P)\sigma^{-1}$.*

Proof: See [21], Proposition 9.7. □

As an immediate consequence of Proposition 1.1.1 and 1.1.2, each place Q_i, $1 \leq i \leq s$, is the restriction to F of $\sigma(R)$, for some $\sigma \in G$. We write $Q_i = \sigma(R)|_F$.

For $\sigma \in G$ we denote by $H\sigma D$ the double coset of σ with respect to the subgroups $D, H \subseteq G$, i.e.

$$H\sigma D = \{\tau\sigma\rho \mid \tau \in H \text{ and } \rho \in D\} \ .$$

Observe that $H\sigma D = H\sigma' D$ if and only if $\sigma' \in H\sigma D$. The set $H\backslash G/D$ represents the set of all double cosets of G modulo H and D.

Now we can state the main result of this section.

Theorem 2.1.4 *Let F/K be a finite separable extension with the Galois closure M. Fix a place $R \in \mathbb{P}_M$ lying over $P \in \mathbb{P}_K$, and denote by $D(R|P) =: D$ and $I(R|P) =: I$ the decomposition group and the inertia group of R/P, respectively. If H is the subgroup of G corresponding to the field F, then the following hold.*

(i) There is a bijection between the set $\{Q_1, \ldots, Q_s\}$ of all places of F that lie over P, and the set of double cosets of G modulo H and D, $H\backslash G/D$, given by

$$\Phi : Q_i = \sigma(R)|_F \longmapsto H\sigma D \ .$$

(ii) Let Q_i be the place corresponding to the double coset $H\sigma D$. Then we have:

$$e(Q_i|P) \cdot f(Q_i|P) = \frac{|D|}{|\sigma D \sigma^{-1} \cap H|} = \frac{|H\sigma D|}{|H|} \tag{2.1}$$

$$e(Q_i|P) = \frac{|I|}{|\sigma I \sigma^{-1} \cap H|} = \frac{|H\sigma I|}{|H|} \tag{2.2}$$

Proof:

(i) First we show that Φ is well-defined. In fact, suppose that $Q_i = \sigma(R)|_F = \sigma'(R)|_F$. As M/F is Galois and H is the Galois group of M/F, there exists an automorphism $\tau \in H$ such that $\sigma(R) = \tau\sigma'(R)$. Hence $\sigma^{-1}\tau\sigma'(R) = R$ which shows that $\sigma^{-1}\tau\sigma' =: \rho \in D$. We conclude that $\sigma' = \tau^{-1}\sigma\rho \in H\sigma D$ and therefore $H\sigma' D = H\sigma D$.

Next we show that Φ is one-to-one. Suppose that $H\lambda D = H\sigma D$ with $\sigma, \lambda \in G$. This means that $\lambda = \tau\sigma\rho$ for some $\tau \in H$ and $\rho \in D$. It follows that $\lambda(R) = \tau\sigma\rho(R) = \tau\sigma(R)$. Since $\tau \in H$, the places $\lambda(R)$ and $\sigma(R)$ are conjugate over F. Therefore $\lambda(R)|_F = \sigma(R)|_F$, as desired.

The fact that Φ is onto, comes from the definition of Φ : the double coset $H\sigma D$ is the image of the place $\sigma(R)|_F$ under Φ.

(ii) By definition, the decomposition group of $\sigma(R)|Q_i$ is given by

$$D(\sigma(R)|Q_i) = H \cap D(\sigma(R)|P) = H \cap \sigma D \sigma^{-1} \ .$$

By transitivity of ramification indices and residue degrees of places in finite separable extensions $K \subseteq F \subseteq M$, we obtain the following equality.

$$e(Q_i|P) \cdot f(Q_i|P) = \frac{e(\sigma(R)|P) \cdot f(\sigma(R)|P)}{e(\sigma(R)|Q_i) \cdot f(\sigma(R)|Q_i)} = \frac{|D|}{|H \cap \sigma D \sigma^{-1}|} \tag{2.3}$$

In the same way, since

$$I(\sigma(R)|Q_i) = H \cap \sigma I \sigma^{-1},$$

and $e(\sigma(R)|Q_i) \cdot e(Q_i|P) = e(\sigma(R)|P)$ by Proposition 1.1.2(ii), we obtain the equation

$$e(Q_i|P) = \frac{e(\sigma(R)|P)}{e(\sigma(R)|Q_i)} = \frac{|I|}{|H \cap \sigma I \sigma^{-1}|} \tag{2.4}$$

Now we calculate $\frac{|H\sigma D|}{|D|}$ and $\frac{|H\sigma I|}{|I|}$. We fix a complete system of representatives $\rho_1, \cdots, \rho_k$ of left cosets of H modulo its subgroup $H \cap \sigma D \sigma^{-1}$, so $|H| = k \cdot |H \cap \sigma D \sigma^{-1}|$.

Claim 1: $H\sigma D$ is the disjoint union of the left cosets $\rho_1 \sigma D, \cdots, \rho_k \sigma D$ of G modulo D, hence $|H\sigma D| = k \cdot |D|$.

Claim 2: $H\sigma I$ is the disjoint union of the left cosets $\rho_1 \sigma I, \cdots, \rho_k \sigma I$ of G modulo I, hence $|H\sigma I| = k \cdot |I|$.

Assuming the Claim 1 is true, we obtain the following equations.

$$\frac{|D|}{|H \cap \sigma D \sigma^{-1}|} = \frac{|D| \cdot k}{|H|} = \frac{|D|}{|H|} \cdot \frac{|H\sigma D|}{|D|} = \frac{|H\sigma D|}{|H|} \tag{2.5}$$

In the same way assuming claim 2 we obtain

$$\frac{|I|}{|H \cap \sigma I \sigma^{-1}|} = \frac{|I| \cdot k}{|H|} = \frac{|I|}{|H|} \cdot \frac{|H\sigma I|}{|I|} = \frac{|H\sigma I|}{|H|} \tag{2.6}$$

Equations (1.1) and (1.2) and Equation 2.6 yield the statement of our theorem.

Proof of the Claims: We will only prove claim 1. The proof of claim 2 is the same as the proof of claim 1. Clearly, the double coset $H\sigma D$ is the union of all left cosets $\rho\sigma D$ with $\rho \in H$. For given $\rho \in H$, let ρ_ℓ be the representative of the coset $\rho(H \cap \sigma D \sigma^{-1})$, then $\rho = \rho_\ell \epsilon$ with $\epsilon \in \sigma D \sigma^{-1}$. Write $\epsilon = \sigma \delta \sigma^{-1}$ with $\delta \in D$, then $\rho \sigma D = \rho_\ell \epsilon \sigma D = \rho_\ell \sigma \delta \sigma^{-1} \sigma D = \rho_\ell \sigma D$. This shows that

$$H\sigma D = \bigcup_{\ell=1}^{k} \rho_\ell \sigma D,$$

and it remains to show that the cosets $\rho_\ell \sigma D$ $(1 \leq \ell \leq k)$ are pairwise distinct.

Assume that $\rho_m \sigma D = \rho_\ell \sigma D$. Then $\rho_m \sigma = \rho_\ell \sigma \delta$ for some $\delta \in D$ and therefore $\rho_\ell^{-1} \rho_m = \sigma \delta \sigma^{-1} \in H \cap \sigma D \sigma^{-1}$. This implies that $m = \ell$ and finishes the proof of the claim. □

Corollary 2.1.5 *Let notation be as above. Then* $e(Q_i|P)f(Q_i|P) = 1$ *if and only if* $\sigma D \sigma^{-1} \subseteq H$*, where* Q_i *corresponds to* $H\sigma D$*. In particular, if* P *is rational and* $\sigma D\sigma^{-1} \subseteq H$*, then* Q_i *is rational.*

Proof: This is clear by Theorem 1.1.3 (ii). □

Definition 2.1.1 *Let* F/K *be a finite function field extension of degree* l*. To any unramified place* $P \in \mathbb{P}_K$*, we attach an* l*-tuple* $\mathcal{A}_P = \{A_1, ..., A_l\} \in \mathbb{N}^l$ *with the property there are exactly* A_i *places* $\widetilde{Q}$ *of* F *lying over* P *with* $f(\widetilde{Q}|P) = i$*. We call the* l*-tuple* $\mathcal{A}_P$ *the splitting type of* P*.*

Since the extension F/K is finite, the cardinality of the set

$$\mathcal{A}_{F/K} = \{\mathcal{A}_P| \;\; P \text{ is unramified in } \mathbb{P}_K\} \subset \mathbb{N}^l$$

is finite. Indeed it is bounded above by the number of partitions of l. Now we want to determine the cardinality of $\mathcal{A}_{F/K}$. But first we need the following results.

Theorem 2.1.6 *Let* M/K *be a Galois extension and* R *be a place of* M *lying over a place* P *of* K*. Then the extension* M_R/K_P *is a Galois extension with cyclic Galois group* $Gal(M_R/K_P)$*. There is a natural homomorphism from* $D(R/P)$ *onto* $Gal(M_R/K_P)$ *with kernel* $I(R/P)$*. Hence the inertia group* $I(R|P)$ *is a normal subgroup of* $D(R|P)$*. In particular, if* P *is unramified, then* $D(R|P)$ *is a cyclic group.*

Proof: See [25], Theorem 3.8.2. □

When P is unramified, we have an isomorphism $D(R|P) \cong Gal(M_R/K_P)$ by Theorem 2.1.6. If m is the cardinality of K_P, then the group $Gal(M_R/K_P)$ is generated by ϕ_P which is defined by $\phi_P(x) = x^m$ for $x \in M_R$. Then there is unique element $\sigma_R \in D(R|P)$ which corresponds to the element ϕ_P under this isomorphism. We call σ_R the Frobenius automorphism of R for the extension M/K. By Proposition 2.1.3 and Theorem 2.1.6, we see that as R varies over the places above P in M, the Frobenius automorphisms σ_R fill out a conjugacy class in G. Therefore in a Galois extension M/K, to each unramified place P in K we attach a conjugacy class in G . This conjugacy class is called the Artin conjugacy class of P. Any element of this class is called a Frobenius element of P.

Theorem 2.1.7 *(Tchebotarev Density Theorem) Let* M/K *be a Galois extension of function fields with Galois group* G*. Let* $\mathcal{C}$ *be a conjugacy class in* G*. Let* $\mathcal{S}$ *be the set of unramified places of* K *in* F/K *whose Frobenius elements are in* $\mathcal{C}$*. Then the Dirichlet density of* $\mathcal{S}$ *is* $\frac{|\mathcal{C}|}{|G|}$*.*

Proof: For the proof see [21], Theorem 9.13A □

One of the important consequences of the Tchebotarev Density Theorem is that every conjugacy class $\mathcal{C}$ is the set of Frobenius elements for infinitely many unramified places of K.

Corollary 2.1.8 *Let F/K be as above, and M be its Galois closure with Galois group $G = Gal(M/K)$. Let $H \subset G$ be such that $M^H = F$. Denote by $\mathcal{C}_G$ the set of all distinct conjugacy classes in G. Let $\mathcal{C} \in \mathcal{C}_G$ and choose $g \in \mathcal{C}$. Let A_i be the number of double cosets $H\sigma\langle g\rangle$ with $\frac{|H\sigma\langle g\rangle|}{|H|} = i$. Then there is a one to one correspondence between $\mathcal{C}_G$ and $\mathcal{A}_{F/K}$, which is defined as follows:*

$$\mathcal{C}_G \to \mathcal{A}_{F/K}$$

$$\mathcal{C} \mapsto (A_1, \ldots, A_l)$$

Proof: Observe that the number A_i is independent of the choice of $g \in \mathcal{C}$. To see this, let g' be another element in $\mathcal{C}$. Then g' is a conjugate of g by an element $\lambda \in G$. Now for each representative $\rho \in H\sigma\langle g\rangle$, we obtain that $H\rho\langle g\rangle = H\sigma\lambda\langle g'\rangle\lambda^{-1}$. Therefore each double coset $H\sigma\lambda\langle g'\rangle$ of G modulo H and $\langle g'\rangle$ is a translation of $H\sigma\langle g\rangle$ by λ. Furthermore, since i is the number of distinct right cosets of H in $H\sigma\langle g\rangle$, then the number of right coset of H in $H\sigma\lambda\langle g'\rangle$ is also i. Hence we conclude that the number A_i is independent of the choice of $g \in \mathcal{C}$. Set $\mathcal{A}_{\mathcal{C}} = (A_1, ...A_l)$. Now we want to show that $\{A_{\mathcal{C}}|\ \mathcal{C} \in \mathcal{C}_G\} = \mathcal{A}_{F/K}$. By Theorem 2.1.4, if $\mathcal{C}$ is the Artin class of $P \in \mathbb{P}_K$ in M/K, then $\mathcal{A}_{\mathcal{C}} = (A_1, ...A_l)$ is the splitting type of P in F/K. Hence every element of $\mathcal{A}_{F/K}$ is of the form $A_{\mathcal{C}}$ for some $\mathcal{C} \in \mathcal{C}_G$. On the other hand by Tchebotarev Density Theorem we know that every conjugacy class $\mathcal{C}$ occurs as the Artin conjugacy class for infinitely many places of K. Hence we obtain the desired result. □

Notation: We denote by $\mathcal{A}_{\mathcal{C}}(i)$ the i-th coordinate A_i of $\mathcal{A}_{\mathcal{C}}$.

□

2.2. Decomposition of polynomials over $\mathbb{F}$

Let $h(x) = x^k + a_{k-1}x^{k-1} + ... + a_o \in \mathbb{F}[x]$. Then $h(x)$ induces as a function over $\mathbb{F}$. We can extend $h(x)$ as a rational function on the projective line $\mathbf{P}^1(\mathbb{F})$ by sending ∞ to ∞. Then $h(x)$ gives rise to an extension of rational function fields $\mathbb{F}(x)/\mathbb{F}(z)$, where $z = h(x)$. The following proposition gives the basic idea how to use the theory of function fields to decompose $h(x)$ in the field $\mathbb{F}$.

Proposition 2.2.9 *Let P_α be the rational place of $\mathbb{F}(z)$ that corresponds to $z-\alpha$ where $\alpha \in \mathbb{F}$. Assume that $h(x)-\alpha$ decomposes over $\mathbb{F}$ as*

$$h(x)-\alpha = \prod_{i=1}^{s} h_i(x)^{n_i} \ ,$$

where $h_i(x)$'s are pairwise distinct, monic, irreducible polynomials of degree ≥ 1. Then $Q_{h_i(x)} \in \mathbb{P}_{\mathbb{F}(x)}$ are the only places of $\mathbb{F}(x)$ lying over P_α and we have $e(Q_{h_i(x)}|P_\alpha) = n_i$ and $f(Q_{h_i(x)}|P_\alpha) = \deg(h_i(x))$, for $i = 1, \ldots, s$.

Proof: Let $(y)_0^{\mathbb{F}(x)}$ resp. $(y)_0^{\mathbb{F}(z)}$ denote the zero divisor of $y \in \mathbb{F}(z)$ in $\mathrm{Div}(\mathbb{F}(x))$ resp. in $\mathrm{Div}(\mathbb{F}(z))$. By assumption $h(x)-\alpha = \prod_{i=1}^{s} h_i(x)^{n_i}$. Hence $(h(x)-\alpha)_0^{\mathbb{F}(z)} = P_\alpha$ and $(h(x)-\alpha)_0^{\mathbb{F}(x)} = \sum_{i=1}^{s} n_i Q_{h_i(x)}$. For a place $P \in \mathbb{P}_{\mathbb{F}(z)}$, consider its conorm (with respect to the extension $\mathbb{F}(x)/\mathbb{F}(z)$) defined as

$$Con_{\mathbb{F}(x)/\mathbb{F}(z)}(P) = \sum_{P'|P} e(P'|P) \cdot P'$$

where the sum runs over all places of $\mathbb{F}(x)$ lying over P. The conorm map is extended to a homomorphism from $\mathrm{Div}(\mathbb{F}(z))$ to $\mathrm{Div}(\mathbb{F}(x))$ by setting

$$\mathrm{Con}_{\mathbb{F}(x)/\mathbb{F}(z)}(\sum n_P \cdot P) = \sum n_P \cdot \mathrm{Con}_{\mathbb{F}(x)/\mathbb{F}(z)}(P).$$

By [25] Proposition 3.1.9, $\mathrm{Con}_{\mathbb{F}(x)/\mathbb{F}(z)}(y)_0^{\mathbb{F}(z)} = (y)_0^{\mathbb{F}(x)}$ for $0 \neq y \in \mathbb{F}(z)$. Therefore the places $Q_{h_i(x)}$ are the only places of $\mathbb{F}(x)$ lying over P_α with $e(Q_{h_i(x)}|P) = n_i$. Conversely, let $Q_1, ...Q_s$ be the all places of $\mathbb{F}(x)$ that lie over P_α with $e(Q_i|P_\alpha)$ is equal to n_i. Since $(z-\alpha)_0^{\mathbb{F}(z)} = P_\alpha$, then

$$\mathrm{Con}_{\mathbb{F}(x)/\mathbb{F}(z)}(z-\alpha)_0^{\mathbb{F}(x)} = \sum_{Q_i|P_\alpha} n_i \cdot Q_i = (h(x)-\alpha)_0^{\mathbb{F}(x)}.$$

Now we obtain that if $h_i(x)$ is the irreducible polynomial that corresponds to Q_i for each $1 \leq i \leq s$, then $h(x)-\alpha$ is the product $\prod_{i=1}^{s} h_i(x)^{n_i}$. □

Applying Theorem 2.1.4 to the extension $\mathbb{F}(x)/\mathbb{F}(h(x))$, we obtain the following result.

Theorem 2.2.10 *Let $h(x)$ be a polynomial with coefficients in $\mathbb{F}$. Denote by M the Galois closure of $\mathbb{F}(x)/\mathbb{F}(h(x))$ with Galois group $G = Gal(M/\mathbb{F}(h(x)))$ and by H the subgroup corresponding to $\mathbb{F}(x)$. Let P_α be the rational place of $\mathbb{F}(h(x))$ corresponding to $z-\alpha$ and R be any place of M lying over P with the decomposition group D and the inertia group I. Then the following hold.*

(i) $h(x)-\alpha$ is a product of exactly $|H\backslash G/D|$ distinct irreducible polynomials in $\mathbb{F}$, and each irreducible polynomial corresponds to a double coset $H\sigma_i D$.

(ii) If $h_i(x)$ corresponds to $H\sigma_i D$, then the multiplicity m_i of $h_i(x)$ is the number of left cosets of H in $H\sigma_i I$ and the degree of $h_i(x)$ is $\frac{s_i}{m_i}$, where s_i denotes the number of left cosets of H in $H\sigma_i D$.

Now we want to determine the number of roots of $h(x) - \alpha$ in $\mathbb{F}$

Corollary 2.2.11 *Let notation be as above and assume that $h(x) - \alpha$ is a square free polynomial with coefficients in $\mathbb{F}$. Let k be the number of roots of $h(x) - \alpha$ in $\mathbb{F}$. Then $k \in \{\mathcal{A}_{\mathcal{C}}(1) | \; \mathcal{C} \in \mathcal{C}_G\}$. Moreover, if we denote by k_i the number of irreducible factors of degree i of $h(x) - \alpha$ in $\mathbb{F}$, then $k_i \in \{\mathcal{A}_{\mathcal{C}}(i) | \; \mathcal{C} \in \mathcal{C}_G\}$.*

Proof: Consider the extension $\mathbb{F}(x)/\mathbb{F}(z)$ with the Galois closure M. By Proposition 2.2.9, the decomposition of the place $P_\alpha \in \mathbb{P}_{\mathbb{F}(h(x))}$ corresponding to $z - \alpha$ is determined by the decomposition of $h(x) - \alpha$ in $\mathbb{F}(x)$. Since $h(x) - \alpha$ is square free, P is unramified. By Corollary 2.1.8, $\mathcal{A}_P$ is of the form $\mathcal{A}_{\mathcal{C}}$ for some $\mathcal{C} \in \mathcal{C}_G$. Since $\mathcal{A}_{\mathcal{C}}(i)$ is defined as the number of places $\widetilde{Q}$ of F over P with $f(\widetilde{Q}|P) = i$ the result follows. □

2.3. The Decomposition of $x^{q+1} + x - \alpha$

Let $q = p^a$ and $\mathbb{F}_q \subseteq \mathbb{F}$. In this section, we consider the extension $\mathbb{F}(x)/\mathbb{F}(h(x))$ where $h(x) = x^{q+1} + x \in \mathbb{F}[x]$. The irreducible polynomial of x over $\mathbb{F}(h(x))$ is $G(T) = T^{q+1} + T - h(x)$.

In [1] Proposition 5.2, Abhyankar showed that if M is the Galois closure of the extension $\mathbb{F}(x)/\mathbb{F}(h(x))$, then $Gal(M/\mathbb{F}(h(x)) \cong PGL(2, q)$. The more general form $\tilde{G}(T) = T^{q+1} + \gamma T + \beta$ with coefficients in any field L containing $\mathbb{F}_q$ was studied by Bluher in [2]. The polynomial $\tilde{G}(T)$ also gives the group $PGL(2, q)$ as the Galois group of corresponding extension. Moreover, she obtained more detailed information about the possible number of roots of $\tilde{G}(T)$ in L.

This section is devoted to find the possible decompositions of $h(x) - \alpha$ in $\mathbb{F}$ for all $\alpha \in \mathbb{F}$. Write $h(x) = z$. Let $P_\alpha \in \mathbb{P}_{\mathbb{F}(z)}$ be the rational place of $\mathbb{F}(z)$ corresponding to the irreducible polynomial $z - \alpha$.

In [1], p.3 line 16, Abhyankar remarked that the extension $\mathbb{F}(x)/\mathbb{F}(z)$ gives an unramified covering of the (once) punctured affine line over $\mathbb{F}_q$ (punctured at $z = 0$). So we conclude that there is no ramification for the rational places $P \in \mathbb{P}_{\mathbb{F}(z)}$ other than P_∞ and P_0. Therefore by Theorem 2.1.6 we conclude that for any rational place P_α with $\alpha \notin \{\infty, 0\}$ the decomposition group is $D(R|P_\alpha) \cong \mathrm{Gal}(M_R/F_P)$. Recall that it is a cyclic group.

In Section 1.1, we have seen that the splitting type of a place P in the extension $\mathbb{F}(x)/\mathbb{F}(h(x))$ depends on the Galois group $PGL(2, q)$, the Artin conjugacy class of P in $PGL(2, q)$ and the subgroup H of $PGL(2, q)$ whose fixed field is $\mathbb{F}(x)$. So we will investigate cyclic subgroups of $PGL(2, q)$ to determine $D(R|P)$. Actually all the subgroups of $PGL(2, q)$ and their structures are known. Below we list all of them.

Notation: We denote by S_l and A_l the symmetric group and the alternating group of degree l. D_s is the dihedral group of order $2s$.

Theorem 2.3.12 *(Dickson's Theorem) $PGL(2, p^a)$ has only the following subgroups:*

(i) elementary abelian p-groups of order p^f with $f \leq a$;

(ii) cyclic groups of order k with $k|(p^a \pm 1)$;

(iii) D_s with $s|(p^a \pm 1)$;

(iv) A_4 *for* $p > 2$ *or* $p = 2$ *and* $a \equiv 0 \pmod{2}$*;*

(v) S_4 *for* $p > 2$*;*

(vi) A_5 *for* $p = 5$ *or* $p^{2a} - 1 \equiv 0 \pmod{5}$*;*

(vii) semidirect products of elementary abelian p*-groups of order* p^f *with cyclic groups of order* k *with* $f \leq a$*,* $k|(p^f - 1)$ *and* $k|(p^a - 1)$*;*

(viii) $PSL(2, p^f)$ *and* $PGL(2, p^f)$ *with* $f|a$*.*

Proof: See [26], Theorem 3. □

By Theorem 2.3.12, we conclude that there are only 3 types of cyclic subgroups of $PGL(2, q)$. If σ generates one of them, then the order of σ is either p or it must divide $q \pm 1$.

It is well known that $PGL(2, q)$ acts 3- transitively on $\mathbf{P}^1(\mathbb{F}_q)$, the projective line over $\mathbb{F}_q$. Another important property of the action of $PGL(2, q)$ on $\mathbf{P}^1(\mathbb{F}_q)$ is that only identity fixes three elements of $\mathbf{P}^1(\mathbb{F}_q)$. Now we give properties of subgroups of $PGL(2, q)$ fixing a point in $\mathbf{P}^1(\mathbb{F}_q)$.

(i) The stabilizer $B_v \subseteq PGL(2, q)$ of a point $v \in \mathbf{P}^1(q)$ has order $q \cdot (q-1)$. Any two of such groups are conjugate and there are exactly $q+1$ such groups in $PGL(2, q)$. Note that these subgroups correspond to (vii) of Theorem 2.3.12.

(ii) The group $T_{u,v}$, which is the intersection of B_u and B_v, is a cyclic group of order $q - 1$. Any two subgroups of this type are conjugate in $PGL(2, q)$, and if they are distinct, their intersection is trivial.

The subgroups B_v are important in our context, because they are conjugate to the subgroup H of $PGL(2, q)$ corresponding to the intermediate field $\mathbb{F}_{q^m}(x)$. Indeed

$$|Gal(M/\mathbb{F}_{q^m}(z))| = |PGL(2, q)| = q \cdot (q - 1) \cdot (q + 1)$$

and

$$[\mathbb{F}_{q^m}(x) : \mathbb{F}_{q^m}(z)] = q + 1 \ .$$

So the order of H must be $q \cdot (q - 1)$. On the other hand, by Theorem 2.3.12 the subgroups of $PGL(2, q)$ having this order are semidirect products of elementary abelian p-groups and cyclic groups of order $q - 1$. The subgroups B_u have this order and we remarked above that these subgroups of $PGL(2, q)$ are all conjugate and there are exactly $q + 1$ subgroups of this order. Hence H must be one of them. We conclude that $H = B_u$ for some $u \in \mathbf{P}^1(\mathbb{F}_q)$.

The following Theorem gives the number of fixed points of $g \in PGL(2, q)$ arising from the action of $PGL(2, q)$ on $\mathbf{P}^1(\mathbb{F}_q)$.

Theorem 2.3.13 *Let g be a nontrivial element in $PGL(2,q)$ of order $d \neq 2$ and k be the number of fixed points of g. Then one of the following holds.*

(i) $d = p$ and $k = 1$;

(ii) $d|(q+1)$ and $k = 0$;

(iii) $d|(q-1)$ and $k = 2$.

Proof: See [3], Theorem 1. □

Now we consider the case $d = 2$ when p is odd. For odd p, $PGL(2,q)$ contains two classes of involutions. The centralizer of an involution is a dihedral group of order either $2(q+1)$ or $2(q-1)$. See [16], Lemma A.3. Let $g \in PGL(2,q)$ be an involution whose centralizer is a dihedral group $D_{2(q+1)}$. We want to show that g does not fix any element of $\mathbf{P}^1(\mathbb{F}_q)$. Let $\omega \in D_{2(q+1)}$ be a generator of the cyclic subgroup of $D_{2(q+1)}$ of order $q+1$. By Theorem 2.3.13, ω does not fix any element in $\mathbf{P}^1(\mathbb{F}_q)$. But ω is in the centralizer of g. Therefore if g fixes an element u, then $\omega^i g (\omega^i)^{-1}(u) = g(u) = u$, hence g also fixes $(\omega^i)^{-1}(u)$ for each i. Since all $(\omega^i)^{-1}(u)$ are distinct, we conclude that g fixes $q+1$ elements. It is well known that in $PGL(2,q)$ only the identity element fixes more than three elements. Hence g does not fix any element. Similarly if g is an involution of $PGL(2,q)$ with centralizer $D_{2(q-1)}$, it can be shown that g fixes 2 points of $\mathbf{P}^1(\mathbb{F}_q)$. Indeed let $\omega \in D_{2(q-1)}$ be a generator of the cyclic subgroup of $D_{2(q-1)}$ of order $q-1$. We know by Theorem 2.3.13 that ω fixes two elements u_i (for $i = 1,2$) of $\mathbf{P}^1(\mathbb{F}_q)$. Since ω is in the centralizer of g, then $g\omega g^{-1}(u_i) = \omega(u_i) = u_i$, and g fixes $\omega^{-1}(u_i)$ for $(i = 1,2)$. We conclude that g fixes two elements of $\mathbf{P}^1(\mathbb{F}_q)$.

Let $\langle g \rangle$ denote the subgroup of $PGL(2,q)$ generated by the element g, and $H = B_u$ for some $u \in \mathbf{P}^1(\mathbb{F}_q)$. To determine the decomposition of P_α in $\mathbb{F}(x)/\mathbb{F}(z)$ by applying Theorem 2.1.4, we first need to count the number of double cosets $H\sigma\langle g \rangle$ of G modulo H and $\langle g \rangle$, for one of three types of g mentioned in Theorem 2.3.13.

Remark 2.3.1 *Let G be any group with subgroups H, N and let $H\backslash G$ be the set of right cosets of H in G. Then N acts on the set $H\backslash G$ as given below.*

$$H\backslash G \times N \to H\backslash G$$

$$(H\sigma, k) \mapsto H\sigma k$$

Then each orbit of N on the set $H\backslash G$ gives a double coset $H\sigma N$ for some $H\sigma$ in the orbit. Since double cosets are disjoint, for each subgroup N of G, the double cosets space $H\backslash G/N$ gives a partition of the set $H\backslash G$. In particular, each double coset $H\sigma N$ corresponds to a subset of $H\backslash G$.

Lemma 2.3.14 *Let H be a subgroup of G, $g \in G$ of order n and $\sigma \in G$. Let i be the least positive integer such that g^i is contained in $\sigma^{-1}H\sigma$. Then the number of right cosets of H in the double coset $H\sigma\langle g\rangle$ is equal to i.*

Proof: Clearly, the cosets $H\sigma, H\sigma g, ..., H\sigma g^{i-1}$ are contained in $H\sigma\langle g\rangle$. We claim that they are pairwise distinct.In fact, assume that $H\sigma g^j = H\sigma g^k$ for some $0 \le j < k < i$. Then $H\sigma g^{k-j} = H\sigma$, so $g^{k-j} \in \sigma^{-1}H\sigma$. Since $k - j < i$, we obtain a contradiction to the choice of i.
Now we will show that $H\sigma g^{li+k} = H\sigma g^k$ for some integers k, l with $0 \le k < i$ and $0 \le l$. If $g^i \in \sigma^{-1}H\sigma$, then $g^{il} \in \sigma^{-1}H\sigma$, and hence $g^{il} = \sigma^{-1}h\sigma$ for some $h \in H$. Then

$$H\sigma g^{il}g^k = H\sigma(\sigma^{-1}h\sigma)g^k = H\sigma g^k$$

So there are exactly i right cosets of H in $H\sigma\langle g\rangle$. □

From now on H denotes the subgroup B_u of $PGL(2, q)$ that fixes the point $u \in \mathbf{P}^1(\mathbb{F}_q)$. Recall that there are $q+1$ right cosets of H in $PGL_2(q)$ since the order of H is $q\cdot(q-1)$.

Lemma 2.3.15 *Let $g \in PGL(2, p^n) =: G$ be an element of order p. Then there are exactly $p^{n-1} + 1$ double cosets of G modulo H and $\langle g\rangle$. p^{m-1} double cosets contain exactly p right cosets of H. The remaining one consists of only one coset of H.*

Proof: Since g has order p, by Theorem 2.3.13, g fixes only one point, and so g is contained in B_v for a unique $v \in \mathbf{P}^1$. Let $\sigma \in G$ be such that $\sigma(u) = v$. Then g is contained in $\sigma H\sigma^{-1} = B_v$. So $H\sigma\langle g\rangle$ is the double coset consisting of only the right coset $H\sigma$ by Lemma2.3.14. Since g fixes only one element, it is not contained in any other conjugate $\tau H\tau^{-1} \neq \sigma H\sigma^{-1}$. Therefore the number of right cosets of H in $H\tau\langle g\rangle$ is exactly p, by Lemma 2.3.14. Hence there must be exactly $p^n/p = p^{n-1}$ double cosets $B\sigma\langle g\rangle$ containing p right cosets of H. □

Lemma 2.3.16 *Let $g \in G$ be an element of order k dividing $p - 1$. Then there are $2 + \frac{q-1}{k}$ double cosets of G modulo H and $\langle g\rangle$. Two of these double cosets contain exactly one right coset of H, and $(q-1)/k$ double cosets contain exactly k right cosets of H.*

Proof: By Theorem 2.3.13, g fixes two elements v, w of $\mathbf{P}^1$. So g is contained in $\sigma H\sigma^{-1}$ and $\tilde{\sigma}H\tilde{\sigma}^{-1}$, where $\sigma(u) = v$ and $\tilde{\sigma}(u) = w$. Hence the double cosets $H\sigma\langle g\rangle$ and $H\tilde{\sigma}\langle g\rangle$ consist of only one right coset of H, namely $H\sigma$ and $H\tilde{\sigma}$. Since g fixes only two elements, it is not contained in any other conjugates $\tau H\tau^{-1} \notin \{\sigma H\sigma^{-1}, \tilde{\sigma}H\tilde{\sigma}^{-1}\}$. By Lemma 2.3.14 the remaining double cosets contain exactly k right cosets of H. Hence there are $(q-1)/k$ double cosets which contain k right cosets of H. □

Lemma 2.3.17 *Let $g \in G$ be an element of order k dividing $q+1$. Then there are exactly $(q+1)/k$ double cosets of G modulo H and $\langle g \rangle$, containing k right cosets of H.*

Proof: By Theorem 2.3.13, g does not fix any element in $\mathbf{P}^1$. Hence it is not contained in $\sigma H \sigma^{-1}$ for any $\sigma \in G$. By Lemma 2.3.14, each double coset $H\sigma\langle g \rangle$ contains exactly k right cosets of H. Therefore there are $(q+1)/k$ double cosets of G modulo H and $\langle g \rangle$.

Remark 2.3.2 *In Section 1.1, Theorem 2.1.4(ii) we have seen that if $\widetilde{Q}$ corresponds to the double coset $H\sigma D$, then $e(\widetilde{Q}|P)f(\widetilde{Q}|P) = \frac{|H\sigma D|}{|H|}$. Note that $\frac{|H\sigma D|}{|H|}$ is the number of right cosets of H contained in $H\sigma D$.*

Remark 2.3.2 and Theorem 2.1.4 give the following result.

Theorem 2.3.18 *Let $h(x) - \alpha = x^{q+1} + x - \alpha$ with $\alpha \in \mathbb{F} \setminus \{0\}$. Then $h(x) - \alpha$ is a square-free polynomial and has one of the following decompositions into irreducible factors over $\mathbb{F}$:*

(i) $(x-\beta)\prod_{i \le p^{a-1}} h_i(x)$ *with* $\deg(h_i(x)) = p$;

(ii) $(x-\beta_1)(x-\beta_2)\prod_{i \le \frac{p^a-1}{k}} h_i(x)$ *with* $\deg(h_i(x)) = k > 1$, *and* $k|(q-1)$;

(iii) $\prod_{i \le \frac{q+1}{k}} h_i(x)$ *with* $\deg(h_i(x)) = k > 1$ *and* $k|(q+1)$;

(iv) $\prod_{i \le q+1}(x-\beta_i)$.

Proof: We know by [1], Proposition 5.2, $Gal(M/\mathbb{F}(h(x))) \cong PGL(2,q)$. The subgroup H that corresponds to $\mathbb{F}(x)$ must be B_u for some $u \in \mathbf{P}^1$. Since $h(x) - \alpha$ is square-free, for the place P_α corresponding to $h(x) - \alpha$ and a place R of M lying over P_α the decomposition group $D(R|P_\alpha)$ is cyclic. Let g_α be a generator of $D(R|P_\alpha)$; i.e. $D(R|P_\alpha) = \langle g_\alpha \rangle$. By Theorem 1.1.2 each place $\widetilde{Q}$ of $\mathbb{F}(x)$ lying over P_α corresponds to a double coset of G modulo H and $\langle g_\alpha \rangle$, say $H\sigma\langle g_\alpha \rangle$. Since there is no ramification, by Remark 2.3.2, $f(\widetilde{Q}|P)$ is the number of right cosets of H in $H\sigma\langle g_\alpha \rangle$. On the other hand, $\langle g_\alpha \rangle$ is either one of the types of cyclic subgroups of $PGL(2,q)$ in Theorem 2.3.13 or $\{id\}$. Then the cases (i), (ii) and (iii) come from Lemmas 2.2.13, 2.2.14 and 2.2.15, respectively. $\langle g_\alpha \rangle = \{id\}$ gives the last case. □

If $\alpha = 0$, then $h(x) = x^{q+1} + x = x \cdot (x^q + 1) = x \cdot (x+1)^q$. By Proposition 2.2.9, we conclude that there are two rational places Q_x and Q_{x+1} of $\mathbb{F}(x)$ lying over P_0 with ramification indices $e(Q_x|P_0) = 1$ and $e(Q_{x+1}|P_0) = q$.

Bluher had shown in her article [2] that the number of roots of $g(x)$ is either $0, 1, 2$ or $q+1$. Now we state the same result as a corollary of Theorem 2.3.18:

Corollary 2.3.19 *Let $g(x) = x^{q+1} + x + a$ be in $\mathbb{F}[x]$. Then the number of roots of $g(x)$ in $\mathbb{F}$ is either $0, 1, 2$ or $q + 1$.*

CHAPTER 3

More Results for a Finite Group of Lie Type

In this chapter we will investigate the decomposition of $P \in \mathbb{P}_K$ in the finite extension F/K by assuming that the Galois closure M has the Galois group G over K, which is a finite group of Lie type. We restrict ourselves to the case that $[F : K]$ is prime to $\mathrm{char}(G)$. Also we have the restriction that $D(R|P)$ is a cyclic group. Under these assumptions, we will attach a combinatorial data to the group G.

The first section is devoted to investigate general results under certain conditions on the structure of D and the normalizer of H in G.

3.1. Methods of Counting the Double Cosets of G

Let K be a function field whose constant field $\mathbb{F}$ has cardinality r^s with characteristic r, and let F be a finite separable extension of K. Let M be the Galois closure of the extension F/K, with Galois group G. By H, we denote the Galois group of M/F. Hence F is the fixed field of H. For a place $P \in \mathbb{P}_K$, fix a place $R \in \mathbb{P}_M$ that lies over P. We denote by $D(R|P) = D$ the decomposition group of $R|P$. Section 2.1 contains a preparation to computing the number of double cosets of any group G with respect to two subgroups H and N with the properties that $N_G(H) = H$ and N is cyclic group.

We use the following notations:

$$\mathbb{P}_F^P := \{Q \ : \ Q \in \mathbb{P}_F, \ Q \mid P\}$$
$$\mathbb{P}_F^P(i) := \{Q \ : \ Q \in \mathbb{P}_F^P, \ \ e(Q|P) \cdot f(Q|P) = i\}$$

This section is devoted to determine the cardinalities of $\mathbb{P}_F^P$ and $\mathbb{P}_F^P(i)$.

Remark 3.1.1 *Let H, N be any two subgroups of G. Let $\mathcal{H}$ denote the set of all conjugates of H. There is an action of N on the set $\mathcal{H}$ defined as*

$$N \times \mathcal{H} \to \mathcal{H}$$

$$(x, gAg^{-1}) \mapsto xgAg^{-1}x^{-1}$$

Lemma 3.1.1 *Let notation be as above. Consider the actions of N on the sets $\mathcal{H}$ and the set of right cosets of G modulo H. Then there is a bijection between the set of orbits $\mathfrak{O}_{H\backslash G}$ of N on the set $H\backslash G$ defined in Remark 2.3.1 and the set of orbits $\mathfrak{O}_{\mathcal{H}}$ of N on the set $\mathcal{H}$ defined in Remark 3.1.1. The bijection is given by*

$$\mathfrak{O}_{H\backslash G} \to \mathfrak{O}_{\mathcal{H}}$$

$$orb(Hx) \mapsto orb(x^{-1}Hx)$$

.

Proof: Let $x, y \in G$. We will show that Hx and Hy are in the same orbit of N in the set $\mathfrak{O}_{H\backslash G}$ if and only if $x^{-1}Hx$ and $y^{-1}Hy$ are in the same orbit in the set $\mathfrak{O}_{\mathcal{H}}$. Now assume that Hx and Hy lie in the same orbit. Then there is $n \in N$ such that $Hxn = Hy$. So $xny^{-1} \in H$ and hence $(xny^{-1})^{-1} = yn^{-1}x^{-1} \in H$. This implies that $yn^{-1}x^{-1}Hxny^{-1} = H$ and therefore $y^{-1}Hy = n^{-1}x^{-1}Hxn$. That means that $x^{-1}Hx$ and $y^{-1}Hy$ lie in the same orbit in $\mathfrak{O}_{\mathcal{H}}$.

Conversely, assume that $x^{-1}Hx$ and $y^{-1}Hy$ lie in the same orbit of N in $\mathfrak{O}_{\mathcal{H}}$. Then there is $n \in N$ such that $n^{-1}x^{-1}Hxn = y^{-1}Hy$. So $yn^{-1}x^{-1}Hxny^{-1} = H$. Note that $z = yn^{-1}x^{-1}$ has inverse $z^{-1} = y^{-1}xn$. By our assumption $N_G(H) = H$, so $zHz^{-1} = H$, and $z = yn^{-1}x^{-1} \in H$. Hence $H = Hyn^{-1}x^{-1}$ and it follows that $Hyn^{-1} = Hx$. It means that Hx and Hy lie in the same orbit of in $\mathfrak{O}_{H\backslash G}$. Hence the result follows.

□

Corollary 3.1.2 *Let $\mathcal{O} \in \mathfrak{O}_{H\backslash G}$, and let $\mathcal{O}'$ be the corresponding orbit in $\mathfrak{O}_{\mathcal{H}}$ with respect to the bijection defined in Lemma 3.1.1. Then these two orbits have the same cardinality.*

As remarked in Chapter 2, 2.3.2, the double cosets HwN can be seen as orbits of N arising from the action on the right cosets of H. We can consider the length of the orbit of Hw as the number of right cosets of G in the double coset HwN. Now by Corollary 3.1.2, this length is equal to the length of the orbit of wHw^{-1}, arising from the action of N on the set $\mathcal{H}$.

The following theorem is very useful when computing the number of double cosets.

Theorem 3.1.3 *(Burnside's lemma) Let N be a finite group acting on a finite set X. Then the number of orbits of the action is*

$$\frac{1}{|N|} \cdot \sum_{g \in N} |\mathit{fix}(g)|,$$

where fix(g) denotes the set of $x \in X$ that are fixed by g.

Proof: See [17], Theorem 3. □

Now we fix some notation that will be used in the rest of this section frequently;

$\mu_n(i) := | \{d \ : \ d|n, \ i|d\} |$

$\mathcal{H}(g^i)$:= the set of all conjugates of H containing g^i

$\mathcal{H}^k(g)$:= the set of conjugates H' of H, such that k is the least integer with $g^k \in H'$.

Remark 3.1.2 *Note that by definition $\mathcal{H}(g^i) = \bigsqcup_{k|i} \mathcal{H}^k(g)$, and that $\mathcal{H} = \bigsqcup_k \mathcal{H}^k(g)$.*

Proposition 3.1.4 *Let H be a subgroup of G with $N_G(H) = H$ and let $g \in N$ be of order n. Let* $\mathrm{fix}(g)$ *be the set of fixed points of g, under the action of N on the set $\mathcal{H}$. Then* $\mathrm{fix}(g) = \mathcal{H}(g)$

Proof: Let N act on the set $\mathcal{H}$ by conjugation as in Remark 3.1.1. Then g fixes an element $\tilde{H} \in \mathcal{H}$ if and only if $g\tilde{H}g^{-1} = \tilde{H}$. Since $N_G(H) = H$, then $N_G(\tilde{H}) = \tilde{H}$. Therefore g must be in $\tilde{H}$. So $\mathrm{fix}(g) = \mathcal{H}(g)$. □

Corollary 3.1.5 *Let H be a subgroup of G with $N_G(H) = H$ and let $\langle g \rangle$ denote the subgroup of G generated by the element g of order n. Let $\phi(n)$ denote the Euler ϕ-function. Then the number of double cosets of G modulo H and $\langle g \rangle$ is*

$$\frac{\phi(n)}{n} \cdot |\mathcal{H}(g)| + \sum_{i|n} \sum_{k|i} |\mathcal{H}^k(g)|$$

Proof: By Burnside's Lemma, the number of orbits of the action of $\langle g \rangle$ on the set $\mathcal{H}$ is

$$\frac{1}{|n|} \cdot \sum_{1 \le i \le n} |fix(g^i)|.$$

We can write $\sum_{1 \le i \le n} |fix(g^i)|$ as

$$\sum_{1 \le i \le n} |fix(g^i)| = \sum_{i \nmid n} |fix(g^i)| + \sum_{i|n} |fix(g^i)| \tag{3.1}$$

By Remark 3.1.2, we replace $\mathrm{fix}(g^i)$ with $\bigsqcup_{k|i} \mathcal{H}^k(g)$ for $i|n$. Then we obtain that

$$\textstyle\sum_{1\leq i\leq n}|fix(g^i)| = \sum_{i\nmid n}|fix(g^i)| + \sum_{i|n}\sum_{k|i}|\mathcal{H}^k(g)|$$

When $k|i$, then the set $\mathcal{H}^k(g)$ occurs in fix(g^i) on the right hand side. So $\mathcal{H}^k(g)$ is seen exactly $\mu_n(i)$ times in the right hand sum. Observe that if gcd$(i,n)=1$, then fix$(g^i)=$ fix(g). Hence the first sum of the right hand side is $\phi(n)|\mathcal{H}(g)|$. Multiplying both sides with $\frac{1}{n}$, we obtain desired result. On the other hand, by Lemma 3.1.1 we know that the number of orbits of the action of $\langle g\rangle$ on the set $\mathcal{H}$ is equal to the number of orbits of the action of $\langle g\rangle$ on the set $H\backslash G$. Since the latter orbits are just double cosets $Hw\langle g\rangle$ with $w\in G$, the result follows. □

Proposition 3.1.6 *The number of double cosets of G modulo H and $\langle g\rangle$ that contain exactly i, $i\neq 1$ right cosets of G modulo H is*

$$\frac{\mu_n(i)}{n}\cdot|\mathcal{H}^i(g)|$$

Proof: We know that double cosets of G modulo H and $\langle g\rangle$ are the orbits of $\langle g\rangle$ on $\mathcal{H}$ by Remark 2.3.1. It is clear that the double coset $Hw\langle g\rangle$ corresponds to the orbit of Hw in $\mathfrak{O}_{H\backslash G}$. By Lemma 3.1.1 $Hw\langle g\rangle$ corresponds also to the orbit of $w^{-1}Hw$. By Remark 3.1.2, $w^{-1}Hw\in\mathcal{H}^k(g)$ for some k in the set $\mathfrak{O}_{\mathcal{H}}$. We have seen in Chapter 2, Lemma 2.3.14 that, the number of right cosets of H contained in $Hw\langle g\rangle$ is the least integer i such that g^i is contained wHw^{-1}. So $i=k$. There are exactly $\frac{\mu_n(i)}{n}\cdot|\mathcal{H}^i(g)|$ double cosets of length i by Corollary 3.1.5. Hence we obtain the result. □

Proposition 3.1.7 *The number of double cosets of G modulo H and $\langle g\rangle$ containing just one right coset of G modulo H is $|\mathcal{H}(g)|$.*

Proof: Suppose that gcd$(i,n)=1$, and let xHx^{-1} be any conjugate of H. Then clearly $g\in xHx^{-1}$ if and only if $g^i\in xHx^{-1}$. By Lemma 2.3.14 the number of right cosets of G modulo H that are contained $Hx\langle g\rangle$ is 1. There are exactly $\phi(n)$ integers less than n and that prime to n. On the other hand for $i=1$, $i|k$ for all k with gcd$(k,n)\neq 1$, which means that g is contained in all fix(g^k) for gcd$(k,n)\neq 1$. Hence g occurs in second sum of right hand sum in 3.1 exactly of $n-\phi(n)$ times. When we sum up all of them, and dividing it by the factor n, we obtain the desired result. □

Now we can state the main theorem of this section.

Theorem 3.1.8 *Let F/K be a finite separable extension with Galois closure M. Let G be the Galois group of M/K with subgroup H corresponding to the intermediate field F. Assume that $N_G(H)=H$. Let P be a place of K such that $D(R|P)$ is a cyclic subgroup of G for some $R\in\mathbb{P}_M$ lying over P. If g is a generator of $D(R|P)$ of order* *n, then the cardinality of* $\mathbb{P}_F^P$ *is* $\sum_{i\leq n}|\mathbb{P}_F^P(i)|$ *where* $|\mathbb{P}_F^P(i)|$ *is given by*

$$|\mathbb{P}_F^P(i)| = \begin{cases} |\mathcal{H}(g)| & \textit{, if } i=1 \\ \frac{\mu_n(i)}{n}\cdot|\mathcal{H}^i(g)| & \textit{, if } i|n \\ 0 & \textit{, if } i\nmid n \end{cases}$$

3.2. Further Results for Finite Groups of Lie Type

A consequence of the classification theorem of the finite simple groups is that most finite simple groups are closely related to finite groups of Lie type. We will first explain how a finite group of Lie type arises.

Let $\mathbb{K}$ be the algebraic closure of $\mathbb{F}_p$. The simple algebraic groups over $\mathbb{K}$ were classified by Chevalley and fall into the following families:

classical types :	A_n	B_n	C_n	D_n	
examples :	$SL(n+1,\mathbb{K})$,	$SO(2n+1,\mathbb{K})$,	$Sp(2n,\mathbb{K})$,	$SO(2n,\mathbb{K})$	
exceptional types :	G_2	F_4	E_6	E_7	E_8

Let $\mathbf{G}$ be an algebraic group, and let $\mathbb{F}_q$ denote the field with $q=p^n$ elements. By $\mathbf{G}(\mathbb{F}_q)$ we mean the rational points of the affine variety $\mathbf{G}$ in the field $\mathbb{F}_q$. They are examples of finite groups of Lie types. But not all finite groups of Lie type arise in this way. To unify the description of all finite groups of Lie type, Steinberg [24] studied an arbitrary algebraic group endomorphism $\sigma:\mathbf{G}\to\mathbf{G}$ whose group of fixed points $\mathbf{G}^\sigma$ is finite. The most basic example is the standard Frobenius map relative to q. The resulting finite group of fixed points coincides with the group $\mathbf{G}(\mathbb{F}_q)$.

More complicated endomorphisms are obtained by composing the standard Frobenius map relative to q with a nontrivial graph automorphism π arising from the Dynkin diagram of $\mathbf{G}$. But not all Dynkin diagrams of simple algebraic groups listed above have a non-trivial automorphism. The only simple groups with a nontrivial graph automorphism are those of types A_n, D_n, and E_6.

Also for groups with root system of type G_2, F_4, and B_2, more different endomorphism of $\mathbf{G}$ can be constructed, yielding Suzuki groups in type B_2 with $p=2$ and $q=2^{2n+1}$, and Ree groups in type F_4 and G_2. For type F_4, the prime $p=2$ and for type G_2 the prime $p=3$ yields these types of endomorphisms.

Steinberg's work shows that these are the only possible endomorphisms of $\mathbf{G}$ having a finite fixed point subgroup. We call such an endomorphism of $\mathbf{G}$ a Frobenius map on $\mathbf{G}$ and use the notation $\mathbf{F}$ for a Frobenius map.

Now by a finite group of Lie type we mean a group of the form $\mathbf{G}^{\mathbf{F}}$, where $\mathbf{G}$ is a semisimple algebraic group and where $\mathbf{F}$ is a Frobenius map. Sometimes we will use G as the finite group $\mathbf{G}^{\mathbf{F}}$.

There is another characterization of finite groups of Lie type. G has a BN-pair structure characterized by J. Tits. Indeed any connected algebraic group $\mathbf{G}$ has a BN-pair structure and the BN-pair structure of G is endowed with BN-pair structure of $\mathbf{G}$. (see Appendix). In this section we will use frequently the notions that come from the BN-structure of G.

We fix some notations. $\mathbf{G}$ is a connected reductive algebraic group and $\mathbf{F}$ is a Frobenius map on $\mathbf{G}$. G is the group of fixed points $\mathbf{G}^{\mathbf{F}}$ of $\mathbf{G}$ under $\mathbf{F}$. We denote by $\mathbf{B}$ a Borel subgroup of $\mathbf{G}$ and by $\mathbf{T}$ a maximal torus of $\mathbf{G}$, with normalizer $\mathbf{N}_{\mathbf{G}}(\mathbf{T})$. $\mathbf{W}$ is the Weyl group of the algebraic group $\mathbf{G}$ with respect to $\mathbf{T}$. It is isomorphic to $\mathbf{N}_{\mathbf{G}}(\mathbf{T})/\mathbf{T}$ which is by definition the Weyl group of the BN-pair $\mathbf{G}$ with $B = \mathbf{B}$ and $N = N_{\mathbf{G}}(\mathbf{T})$. See Section 4.2 for related argument.

By a rational subgroup of $\mathbf{G}$ we mean that it is an $\mathbf{F}$-stable subgroup. Let $\mathbf{B}$ be a rational Borel subgroup of $\mathbf{G}$ containing a maximal torus $\mathbf{T}$. It always exists by the Theorem 4.2.1. A rational maximal torus contained in a rational Borel subgroup is called a maximally split torus of G. We will use the notation $\mathbf{T}_o$ for a maximally split torus in $\mathbf{G}$. Then ${\mathbf{T}_o}^{\mathbf{F}}$ is a maximal torus contained in a Borel subgroup $\mathbf{B}^{\mathbf{F}}$ of G.

Here we note that not all rational maximal tori are maximally split tori of $\mathbf{G}$ under $\mathbf{F}$. We also note that all maximally split tori are conjugate in G. If T is a maximally split torus of G contained in B with normalizer $N = N_G(T)$, B and N is of the form $B = \mathbf{B}^{\mathbf{F}}$ and $N = \mathbf{N}_{\mathbf{G}}(\mathbf{T_0})^{\mathbf{F}}$. They form a split BN- structure of G, with Weyl group $W = N/T$.

Let Φ be the root system of $\mathbf{G}$ with respect to $\mathbf{T}_0$. For each $\alpha \in \Phi$ we denote by $\mathbf{U}_\alpha$ the root subgroup of $\mathbf{G}$ defined as the image of the morphism $u_\alpha : \mathbb{G}_a \to \mathbf{G}$, satisfying $tu_\alpha(c)t^{-1} = u_\alpha(\alpha(t)c)$ for all $t \in \mathbf{T}_0$. They are minimal unipotent subgroups of $\mathbf{G}$. Any Borel subgroup containing $\mathbf{T}_0$ is of the form $\mathbf{T}_0 \prod_{\alpha\in\Phi^+} \mathbf{U}_\alpha$ for some positive system Φ^+ in Φ by Theorem 4.1.8.

Let $\mathbf{T}_0$ be a maximally split torus in $\mathbf{G}$. Then $N_{\mathbf{G}}(\mathbf{T}_0)$ is also $\mathbf{F}$-stable. Since $\mathbf{F}$ acts on $N_{\mathbf{G}}(\mathbf{T}_0)$ and $\mathbf{T}_0$, so it also acts on $\mathbf{W} = N_{\mathbf{G}}(\mathbf{T}_0)/\mathbf{T}_0$ by $\mathbf{F}(n\mathbf{T}_0) = \mathbf{F}(n)\mathbf{T}_0$. We denote by $\mathbf{W}^{\mathbf{F}}$ the $\mathbf{F}$-stable subgroup of $\mathbf{W}$.

Let $\mathbf{U}$ be the unipotent radical of $\mathbf{B}$. Since $\mathbf{B}$ is $\mathbf{F}$-stable, $\mathbf{U}$ is also $\mathbf{F}$-stable. As mentioned above, $\mathbf{U} = \prod_{\alpha\in\Phi^+} \mathbf{U}_\alpha$ where Φ^+ is a positive system of roots relative to $\mathbf{B}$. Hence $\mathbf{F}$ permutes the root subgroups $\mathbf{U}_\alpha$ for $\alpha \in \Phi^+$. Therefore there is a permutation ϕ on Φ^+ such that $\mathbf{F}(\mathbf{U}_\alpha) = \mathbf{U}_{\phi(\alpha)}$. Let Δ be the simple system of Φ^+. Observe that since $\phi(\Phi^+) = \Phi^+$, then we have $\phi(\Delta) = \Delta$, hence ϕ gives rise to a permutation of the simple roots. Let I denote the set of simple reflections in $\mathbf{W}$ that generate $\mathbf{W}$ relative to the basis Δ, i.e $I = \{s_\alpha;\ \alpha \in \Delta\}$. Clearly $\mathbf{F}$ permutes also I. The relation of ϕ with the action of $\mathbf{F}$ on the character group $X(\mathbf{T})$ can be found in Section 4.2.

When $\mathbf{F}$ acts on the Weyl group $\mathbf{W}$ as the automorphism ϕ, we prefer to use the notion ϕ-action.
In this section we will investigate the following:

Let F/K be a finite extension of function fields with Galois closure M. We assume that $\mathrm{Gal}(M/K) = G$ is the group of rational points of a reductive algebraic group $\mathbf{G}$ under a Frobenius endomorphism $\mathbf{F}$. Let H be the subgroup of G whose fixed field is F. Our aim is to determine the splitting type of any unramified place P of K in the extension F/K, assuming that H is a parabolic subgroup of G.

To do this we need to determine the number of double cosets of G modulo H and $\langle g\rangle$ for any $g \in G$. First we investigate the properties of single elements of G.

Definition 3.2.1 *Let s be a semisimple element of $\boldsymbol{G}$. If s is $\mathbf{F}$-stable, we say that s is a semisimple element of G. Similarly a rational unipotent element in $\boldsymbol{G}$ is called a unipotent element of G.*

Proposition 3.2.9 *Let g be any element in G.*

(i) There exists unique $s, u \in G$ with s semisimple and u unipotent in G such that $g = us = su$.

(ii) The semisimple elements of G are p'-elements of G, and unipotent elements of G are p- elements of G.

Proof: (i) is the just Jordan decomposition of g (see Theorem 4.1.1). For the proof of (ii) see [9], Proposition 3.18. □

Lemma 3.2.10 *Let $\mathbf{B}$ be a Borel subgroup of $\boldsymbol{G}$ with unipotent radical $\mathbf{U}$.*

(i) $U = \mathbf{U}^{\mathbf{F}}$ is a Sylow p-subgroup of G, and $N_G(U)$ is a Borel subgroup $B = \mathbf{B}^{\mathbf{F}}$ of the group G.

(ii) All Borel subgroups of G are conjugate.

Proof: For the proof of (i), see [19], Corollary 24.11. Now we will consider (ii). We know that Sylow p-subgroups in a finite group are conjugate. Therefore given any two Sylow p-subgroups U_1 and U_2 of G, there is $g \in G$ such that $U_1 = {}^gU_2$ then $B_1 = N_G(U_1) = {}^gN_G(U_2) = {}^gB_2$. Hence the result follows.

By definition, a parabolic subgroup H of BN-pair is a subgroup containing a Borel subgroup. Its structure is defined as follows. Let W be the Weyl group of BN-pair with respect to maximally split torus T contained in the Borel group B. It is a reflection group generated by involutions. Let I' be a set of involutions in W that generate W. A standard parabolic subgroup P_J with respect to B is of the form BW_JB for some $J' \subset I'$. We notice here that $P'_J = \mathbf{P}_J{}^{\mathbf{F}}$ where J is a union of ϕ-orbits on I. See [6], page 63, for related argument. $W_{J'}$ is the subgroup of W generated by the subset $J' \subset I'$, and all conjugate classes of parabolic subgroups of G are parametrized by the subset of I'. Then H is conjugate to a unique standard parabolic subgroup. In particular a Borel subgroup is a parabolic subgroup that is conjugate to the standard parabolic subgroup $BW_{J'}B$ where J is the empty set. See Section 4.2 fore more detailed information.

Proposition 3.2.11 *Let G be a finite group of Lie type. Let H be a parabolic subgroup of G. Then*

(i) $N_G(H) = H$, and any conjugate of H is also a parabolic subgroup of G.

(ii) Any two conjugate parabolic subgroups can not contain the same Borel subgroup of G.

Proof: See [6], Proposition 2.1.6 and [9] Proposition 1.9.

Recall that a subgroup of $\mathbf{G}$ is called a subgroup of maximal rank, if it contains a maximal torus $\mathbf{T}$ of $\mathbf{G}$. The following result is crucial in our context.

Theorem 3.2.12 *Let s be a semisimple element in $\mathbf{G}$. Then the identity component $C_{\mathbf{G}}(s)^0$ of $C_{\mathbf{G}}(s)$ is a connected reductive group. It is also a closed connected subgroup of $\mathbf{G}$ of maximal rank.*

Proof: See [[9], Proposition 2.3].

Since $C_{\mathbf{G}}(s)$ is connected algebraic group of maximal rank, it contains a maximal torus $\mathbf{T}$ of $\mathbf{G}$. Let Φ_s be the root system of $C_{\mathbf{G}}(s)$ with respect to $\mathbf{T}$ and let $\mathbf{W}(s)$ be the Weyl group of Φ_s. If Φ is the root system of $\mathbf{G}$ relative to $\mathbf{T}$, it is a closed subsystem of Φ, hence $\mathbf{W}(s)$ is a subgroup of $\mathbf{W}$. Observe that maximal tori of $C_{\mathbf{G}}(s)$ are the maximal tori of $\mathbf{G}$ containing s. Assume that $s \in \mathbf{G}^{\mathbf{F}}$. Since s is fixed by $\mathbf{F}$, $C_{\mathbf{G}}(s)$ is an $\mathbf{F}$-stable subgroup of $\mathbf{G}$. Furthermore $C_{\mathbf{G}}(s)^{\mathbf{F}} = C_G(s)$. Since $C_{\mathbf{G}}(s)$ is $\mathbf{F}$-rational, it has an $\mathbf{F}$-stable Borel subgroup $\mathbf{B}_s$. Again $C_{\mathbf{G}}(s)^{\mathbf{F}}$ is a finite group of Lie type and therefore it has a finite BN-pair structure BN-pair with $B = \mathbf{B}_s$ with Weyl group

$W(s) = N_{C_{\mathbf{G}}(s)^{\mathbf{F}}}(\mathbf{T}_0)/\mathbf{T}_0)$, where $\mathbf{T}_o$ is a maximally split torus of $C_{\mathbf{G}}(s)^0$ contained in $\mathbf{B}_s$. We note here that, a maximally split torus of $C_{\mathbf{G}}(s)$ is not maximally split torus of $\mathbf{G}$ under a Frobenius map $\mathbf{F}$ in general.

The next proposition gives the relation between the parabolic subgroups of $\mathbf{G}$ and the parabolic subgroups of $C_{\mathbf{G}}(s)$ which will lead to count the rational parabolic subgroups of $\mathbf{G}$ containing s.

Proposition 3.2.13 *Let* $\mathbf{C}$ *be a closed reductive subgroup of* $\mathbf{G}$ *of maximal rank. Then:*

(i) The parabolic subgroups of $\mathbf{C}$ *are of the form* $\mathbf{C} \cap \mathbf{P}$*, where* $\mathbf{P}$ *is a parabolic subgroup containing a maximal torus of* $\mathbf{C}$*. Any parabolic subgroup of* $\mathbf{C}$ *is obtained in this way.*

(ii) If $\mathbf{P}$ *is a parabolic subgroup of* $\boldsymbol{G}$ *containing a maximal torus of* $\mathbf{C}$*, the Levi subgroups of* $\mathbf{P} \cap \mathbf{C}$ *are the* $\mathbf{L} \cap \mathbf{C}$ *where* $\mathbf{L}$ *is a Levi subgroup of* $\mathbf{P}$ *containing a maximal torus of* $\mathbf{C}$*.*

Proof: See [9], Proposition 2.2. □

Lemma 3.2.14 *Let notation be as above. For all* $\alpha \in \Phi$*, and* $w \in \mathbf{W}$

$$ws_\alpha w^{-1} = s_{w(\alpha)}$$

Proof: See [19], Lemma A.4

Lemma 3.2.15 *Let* $\boldsymbol{G}$ *be a reductive algebraic group. Let* $\mathbf{T}$ *be a maximal torus of* $\mathbf{G}$ *contained in* $\mathbf{B}$*. Denote by* $\mathcal{B}_{\mathbf{G}}(\mathbf{T})$ *the set of all Borel subgroups of* $\mathbf{G}$ *containing* $\mathbf{T}$*. Then the Weyl group* $\mathbf{W}$ *of* $\mathbf{G}$ *relative to* $\mathbf{T}$ *acts on* $\mathcal{B}_{\mathbf{G}}(\mathbf{T})$ *simply transitively. In particular the cardinality of the set* $\mathcal{B}_{\mathbf{G}}(\mathbf{T})$ *is* $|\mathbf{W}|$*.*

Proof: By [9],Theorem 0.31, the Borel subgroups containing the maximal torus $\mathbf{T}$ correspond one to one to bases of a root system Φ of $\mathbf{G}$ with respect to $\mathbf{T}$. If Φ^+ is the positive system which is the set of positive integral linear combinations of elements in the basis Δ, the corresponding Borel subgroup is $\mathbf{T}\prod_{\alpha\in\Phi^+}\mathbf{U}_\alpha$. By Proposition 9.4 in [19], for any two bases Δ_1, Δ_2 of Φ, there is a unique $w \in \mathbf{W}$ such that $\Delta_1 = w(\Delta_2)$. This means that $\mathbf{W}$ acts simply transitively on the bases of Φ hence on the set of all positive systems in Φ. The action of $\mathbf{W}$ on $\mathcal{B}_{\mathbf{G}}(\mathbf{T})$ is the following. Let n_w be a representative of w in $N_{\mathbf{G}}(\mathbf{T})/\mathbf{T}$. Then ${}^w\mathbf{B} := n_w\mathbf{B}n_w{}^{-1}$ is different from $\mathbf{B}$. Indeed, by Lemma 3.2.14, $n_w\mathbf{U}_\alpha n_w{}^{-1} = \mathbf{U}_{w(\alpha)}$ for all $\alpha \in \Phi^+$. So ${}^w\mathbf{B} = \mathbf{T}\prod_{\alpha\in w(\Phi^+)}\mathbf{U}_\alpha$. By simply transitivity of $\mathbf{W}$ on the set of of all positive systems in Φ, it follows that $\mathbf{W}$ acts also simply transitively on $\mathcal{B}_{\mathbf{G}}(\mathbf{T})$. □

Lemma 3.2.16 *Let s be a semisimple element of* $\mathbf{G}$*. Let* $\mathbf{B}_s$ *be a Borel subgroup of* $\mathbf{C}_{\mathbf{G}}(s)^o$*. Then the number of Borel subgroups of* $\boldsymbol{G}$ *containing* $\mathbf{B}_s$ *is* $|N_{\mathbf{W}}(\mathbf{W}(s))/\mathbf{W}(s)|$*.*

Proof: Let $\mathbf{T}$ be a maximal torus of $\mathbf{G}$ contained in $\mathbf{B}_s$. Since $\mathbf{B}_s$ is a Borel subgroup of $\mathbf{C}_{\mathbf{G}}(s)$, by 3.2.13, there is a Borel subgroup $\mathbf{B}$ of $\mathbf{G}$ containing $\mathbf{B}_s$. Now we fix $\mathbf{B}$. Let Φ_s be root system of $\mathbf{C}_{\mathbf{G}}(s)$ relative to a maximal torus $\mathbf{T}$ in $\mathbf{B}_s$ and let Φ_s^+ be the positive system in Φ_s with respect to a basis Δ_s corresponding to $\mathbf{B}_s$. Then $\mathbf{B}_s = \mathbf{T} \cdot \prod_{\alpha \in \Phi_s^+} \mathbf{U}_\alpha$. Let Φ^+ be positive system corresponding to $\mathbf{B}$. Since $\mathbf{B}$ contains $\mathbf{B}_s$, ${\Phi_s}^+$ must be contained in Φ^+. Hence the basis Δ of the positive system Φ^+ must contain Δ_s. By Lemma 3.2.15, any two Borel subgroups of $\mathbf{G}$ containing $\mathbf{T}$ are conjugate by element in $\mathbf{W}$. Assume that ${}^v\mathbf{B}$ contains $\mathbf{B}_s$ for some element $v \in \mathbf{W}$. Then v must fix Δ_s. Since Δ_s is a a basis of the root system Φ_s, then W_s is generated by $\{\mathbf{s}_\alpha | \ \alpha \in \Delta_s\}$. By Lemma 3.2.14, $v\mathbf{s}_\alpha v^{-1} = \mathbf{s}_{v(\alpha)}$ for any $\alpha \in \Delta_s$. So v fixes the set Δ_s if and only if v fixes W_s. Hence $v \in N_{\mathbf{W}}(\mathbf{W}_s)$.

Conversely if $v \in N_{\mathbf{W}}(\mathbf{W}(s))/\mathbf{W}(s)$ any coset representatives of $\mathbf{W}(s)$, then ${}^v\mathbf{B}$ contains $v\mathbf{B}_s v^{-1}$. Since $v \in N_{\mathbf{W}}(\mathbf{W}(s))$, $v(\Phi_s^+)$ is of the form ${}^w(\Phi_s^+)$. We replace v by the coset representative vw^{-1}, and obtain that ${}^{vw^{-1}}\mathbf{B}$ contains $\mathbf{B}_s$.

Convention: The Borel subgroups of $\mathbf{P}$ are the Borel subgroups of $\mathbf{G}$ contained in $\mathbf{P}$. Now if $s \in \mathbf{P}$, given a Borel subgroup $\mathbf{B}_s$ of $\mathbf{C}_{\mathbf{G}}(s)^0$, we want to count the number of Borel subgroups of $\mathbf{P}$ containing $\mathbf{B}_s$. To do this, we need the following.

Lemma 3.2.17 *Let* $\mathbf{P}$ *be a parabolic subgroup of* $\mathbf{G}$ *with Levi complement* $\mathbf{L}$ *and unipotent radical* $\mathbf{U}_{\mathbf{P}}$*. Then there is a bijection φ between the Borel subgroups* $\mathbf{B}_{\mathbf{L}}$ *of* $\mathbf{L}$ *and Borel subgroups of* $\mathbf{P}$ *where φ is given by*

$$\varphi : \mathbf{B}_{\mathbf{L}} \to \mathbf{B}_{\mathbf{L}}\mathbf{U}_{\mathbf{P}}.$$

In particular the unipotent radical of a parabolic subgroup $\mathbf{P}$ *is contained in all Borel subgroups of* $\mathbf{G}$ *contained in* $\mathbf{P}$*.*

Proof: See in [11], Springer's article C.5, Section 2.6

Proposition 3.2.18 *Let s be a semisimple element contained in a parabolic subgroup* $\mathbf{P}$*. Then* $\mathbf{C}_{\mathbf{G}}(s)^o \subset \mathbf{P}$*.*

Proof: Let $\mathbf{L} \rtimes \mathbf{U}$ be a Levi decomposition of $\mathbf{P}$ with unipotent radical $\mathbf{U}$ and Levi subgroup $\mathbf{L}$. Since s is semisimple, it lies in a maximal torus in $\mathbf{P}$, hence it lies in a maximal torus of a conjugate of $\mathbf{L}$. Since any Levi complement of $\mathbf{P}$ is conjugate by an element in $\mathbf{U}$ we can assume that s lies in $\mathbf{L}$. We know that every semisimple element of a connected reductive group is contained in a maximal torus of it. Let $\mathbf{T}$ be a maximal torus of $\mathbf{L}$ containing s. Clearly $\mathbf{T}$ is contained in $\mathbf{C}_{\mathbf{G}}(s)^o$. By Proposition 3.2.13 $\mathbf{C}_{\mathbf{G}}(s)^o \cap \mathbf{P}$ is a parabolic subgroup of $\mathbf{C}_{\mathbf{G}}(s)^o$ containing a Borel subgroup $\mathbf{B}_s$. Note also that $\mathbf{P} \cap \mathbf{L}$ is a parabolic subgroup of $\mathbf{L}$ and $\mathbf{B}_s$ is a subgroup of Borel subgroup $\mathbf{B_L}$ of $\mathbf{L}$. If $\Delta_{\mathbf{L}}$ is the simple system contained in the positive system $\Phi^+_{\mathbf{L}}$ that corresponds to $\mathbf{B_L}$, then the simple system Δ_s corresponding to $\mathbf{B}_s$ is contained in Δ. Since $\mathbf{B_L} = \langle \mathbf{T}, \mathbf{U}_\alpha | \ \alpha \in \Phi^+{}_{\mathbf{L}} \rangle$ and $\mathbf{L} = \langle \mathbf{T}, \mathbf{U}_\alpha, \mathbf{U}_{-\alpha} | \ \alpha \in \Phi^+_{\mathbf{L}} \rangle$, then $\mathbf{U}_{-\alpha}$ is contained in $\mathbf{L}$ for all $\alpha \in \Phi^+_{\mathbf{L}}$. In particular $\mathbf{U}_{-\beta}$ is contained in $\mathbf{L}$ for any $\beta \in \Delta_s$. Hence $\mathbf{C_G}(s)^o = \langle \mathbf{T}, \mathbf{U}_\alpha, \mathbf{U}_{-\alpha} | \ \alpha \in \Phi^+_s \rangle$ is contained in $\mathbf{P}$. □

We notice that, except a finite set of semisimple elements in $\mathbf{G}$, $\mathbf{C_G}(s)^0$ is a Levi subgroup of $\mathbf{G}$. Related argument can be found in [9], stated before Lemma 14.11.

The following lemma is another important step to count the number of conjugates of P containing s in G.

Lemma 3.2.19 *Let $\mathbf{B}_s$ be a Borel subgroup of $\mathbf{C_G}(s)^o$. Let $\mathbf{P}$ be a parabolic subgroup of $\mathbf{G}$ conjugate to $\mathbf{B W}_J \mathbf{B}$ for some $J \subset I$. Then the number of Borel subgroups of $\mathbf{P}$ containing $\mathbf{B}_s$ is $|\mathbf{N_{W_J}}(\mathbf{W(s)})/\mathbf{W}(s)|$.*

Proof: Let $\mathbf{T}$ be a maximal torus of $C_{\mathbf{G}}(s)^0$ contained in $\mathbf{B}_s$. By [9] Proposition 1.17, there is unique Levi complement $\mathbf{L}$ of $\mathbf{P}$ containing $\mathbf{T}$. We know that Weyl group of $\mathbf{L}$ with respect to $\mathbf{T}$ is $\mathbf{W_J}$ (see Section 4.1). Recall that $\mathbf{W}_J$ acts simply transitively on the set of Borel subgroups of $\mathbf{L}$ containing $\mathbf{T}$. Hence if $\mathbf{B_L}$ is a Borel subgroup of $\mathbf{L}$ such that $\mathbf{B_L U_P} \cap \mathbf{C_G}(s) = \mathbf{B}_s$, where $\mathbf{B_L U_P}$ as in 3.2.17, then for any $v \in \mathbf{W_L}$, $v(\mathbf{B_L})\mathbf{U} \cap \mathbf{C_G}(\mathbf{s})$ is a Borel subgroup of $\mathbf{C_G}(\mathbf{s})$ containing $\mathbf{T}$. So $\mathbf{W_L}$ acts simply transitively on the set of Borel subgroups of $\mathbf{P}$ that contain $\mathbf{T}$. This action is given by : ${}^v(\mathbf{B_L U}) ={}^v (\mathbf{B_L})\mathbf{U}$. In this way we obtain that $\mathbf{N}(\mathbf{W_L})$ acts on the set of Borel subgroups $\mathbf{P}$ containing $\mathbf{B}_s$. Applying the same idea used in the proof of Lemma 3.2.16, we obtain that the number of Borel subgroups of $\mathbf{P}$ containing $\mathbf{B}_s$ is $|N_{\mathbf{W}_J}(\mathbf{W}(s))/\mathbf{W}(s)|$. □

Now our task will be: given a $\mathbf{F}$-rational Borel subgroup $\mathbf{B}_s$ of $\mathbf{C_G}(s)^0$, to count both the numbers of Borel subgroups of $\mathbf{G}$ and Borel subgroups of $\mathbf{P}$ containing $\mathbf{B}_s$. Although such Borel subgroups are not $\mathbf{F}$-stable, we will see below that they are $w\mathbf{F}$-stable.

We know that there is always a $\mathbf{F}$-stable Borel subgroup $\mathbf{B}$ of $\mathbf{G}$, and any two of them are conjugate by an element in $\mathbf{G^F}$. Let $\mathbf{T}_0$ be a maximally split torus contained in $\mathbf{B}$. Let $\mathbf{W}$ be the Weyl group of $\mathbf{G}$ with respect to $\mathbf{T}_0$. Since $\mathbf{B}$ is fixed by $\mathbf{F}$, it permutes the root subgroups $\mathbf{U}_\alpha$ for $\alpha \in \Phi^+$, hence fixes the basis Δ contained in Φ^+. By Lemma 3.2.14, we conclude that $\mathbf{F}$ permutes the set of simple reflections $I = \{s_\alpha | \ \ \alpha \in \Delta\}$, hence gives rise to an automorphism ϕ on $\mathbf{W}$.

Since Borel subgroups contain the product of root subgroups, $\mathbf{F}$ permutes these root subgroups and gives rise to a permutation of the set $\mathcal{B}_{\mathbf{G}}(\mathbf{T_0})$. This permutation is given as follows: Let $\mathbf{B}'$ be in $\mathcal{B}_{\mathbf{G}}(\mathbf{T_0})$ corresponding to positive system $\Phi'^+ \subset \Phi$, and let Δ' be the simple system in Φ'^+. Since $\mathbf{W}$ acts simple transitively on the set of all simple systems in Φ, there is $v \in \mathbf{W}$ such that $\Delta' = v(\Delta)$. Since ϕ is an automorphism of $\mathbf{W}$, it permutes simple systems in Φ by sending $v(\Delta)$ to $\phi(v)(\Delta)$. Therefore ${\Phi'}^{+} = v(\Phi^{+})$. Now it is clear that $\mathbf{F}$ sends $\mathbf{B}' = \mathbf{T}\prod_{\alpha\in v(\Phi^+)} \mathbf{U}_\alpha$ to $F(\mathbf{B}') = \mathbf{T}\prod_{\alpha\in\phi(v)(\Phi^+)} \mathbf{U}_\alpha$.

Let $\mathbf{T}_0$ be a maximally split torus of $\mathbf{G}$ with respect to $\mathbf{F}$. Since all maximal tori of $\mathbf{G}$ are conjugate , any maximal torus of $\mathbf{G}$ is of the form ${}^{g}\mathbf{T}_0$ for some $g \in \mathbf{G}$. To go further, we need information about the action of $\mathbf{F}$ on the maximal tori of $\mathbf{G}$.

Proposition 3.2.20 *Let $\mathbf{T}_0$ be as above.*

(i) ${}^{g}\mathbf{T}_0$ is $\mathbf{F}$-stable if and only if $g^{-1}\mathbf{F}(g) \in N_{\mathbf{G}}(\mathbf{T}_0)$

(ii) Suppose ${}^{g_1}\mathbf{T}_0 ={}^{g_2} \mathbf{T}_0$. Let w_1 and w_2 be the images of $g_1^{-1}\mathbf{F}(g_1)$ and $g_2^{-1}\mathbf{F}(g_2)$ respectively under the natural map

$$\pi : N_{\mathbf{G}}(\mathbf{T}_0) \to \mathbf{W}$$

Then there is $x \in \mathbf{W}$ such that $w_2 = x^{-1}w_1(\mathbf{F}(x))$

Proof: See [6], Proposition 3.3.1 and Proposition 3.3.2 □

Definition 3.2.2 *We say that w is ϕ-conjugate to w' in $\mathbf{W}$, if there is $x \in \mathbf{W}$ such that $w' = x^{-1}w\phi(x)$. Clearly ϕ-conjugacy is an equivalence relation on $\mathbf{W}$.*

Let $w \in \mathbf{W}$. The set

$$C_{\mathbf{W}}(w\phi) = \{x \in \mathbf{W}; x^{-1}w\phi x = w\}$$

is called ϕ-centralizer of w in $\mathbf{W}$.

Proposition 3.2.21 *The map ${}^{g}\mathbf{T}_0 \to \phi(g^{-1}\mathbf{F}(g))$ determines a bijection between the $\mathbf{G}^{\mathbf{F}}$-classes of $\mathbf{F}$-stable maximal tori of $\boldsymbol{G}$ and the ϕ-conjugacy classes of $\mathbf{W}$.*

Proof: See [19], Proposition 25.1 □

If $\mathbf{T}$ is a rational maximal torus of $\mathbf{G}$ for which the corresponding ϕ-conjugacy class of $\mathbf{W}$ contains w, we say that $\mathbf{T}$ is obtained from the maximally split torus $\mathbf{T}_0$ by twisting with w. We use the notation $\mathbf{T}_w$ for the rational maximal tori that are obtained twisting $\mathbf{T}_0$ with w.

We want to mention the action of $\mathbf{F}$ on $\mathbf{T}_w$ and on the closed connected subgroups of $\mathbf{G}$ containing $\mathbf{T}_w$. This notion has great importance in our text. Since $\mathbf{T}_w$ is obtained twisting $\mathbf{T}_0$ by $w \in \mathbf{W}$, then $\mathbf{T}_w = g\mathbf{T}_0g^{-1}$ and $g^{-1}\mathbf{F}(g) \in N_{\mathbf{G}}(\mathbf{T}_0)$ represents an element which is ϕ-conjugate to w Any element x of $\mathbf{T}_w$ is of the form gtg^{-1} for $t \in \mathbf{T}_0$. $\mathbf{F}$ sends $gtg^{-1} \in \mathbf{T}_w$ to $\mathbf{F}(g)\mathbf{F}(t)\mathbf{F}(g^{-1}) = gg^{-1}\mathbf{F}(g)\mathbf{F}(t)\mathbf{F}(g^{-1})gg^{-1}$. Since $g^{-1}\mathbf{F}(g) := w$, $\mathbf{F}(gtg^{-1}) = gw\mathbf{F}(t)w^{-1}g^{-1}$. So it acts on $\mathbf{T}_w$ like $w\mathbf{F}$ acts on $\mathbf{T}_0$.

Let s be a rational element of $\mathbf{G}$. Then $C_{\mathbf{G}}(s)^0$ is an $\mathbf{F}$-stable connected reductive group. In general, as we noted above, maximally split tori of $C_{\mathbf{G}}(s)^0$ under $\mathbf{F}$ are not maximally split tori of $\mathbf{G}$. Let ϕ be the outer automorphism arising the action of $\mathbf{F}$ on the Weyl group of $\mathbf{G}$. If $\mathbf{T}_w$ is a maximally split torus of $C_{\mathbf{G}}(s)^0$, then again $N_{\mathbf{G}}(\mathbf{T}_w)/\mathbf{T}_w \simeq \mathbf{W}$, but the action of $\mathbf{F}$ on the Weyl group $\mathbf{W}$ with respect to $\mathbf{T}_w$ becomes $w \circ \phi$. For example if $\mathbf{B}_s$ is a $\underline{\text{rational Borel subgroup of } C_{\mathbf{G}}(s)^0 \text{ under } \mathbf{F}}$, then $\mathbf{B}_s$ is an $w\mathbf{F}$-rational subgroup of $\mathbf{G}$. An argument discussing this concept can be found in the proof of Proposition 4.3 in [9].

Let $\mathbf{T}_0$, $\mathbf{T}_s$ be maximally split tori of $\mathbf{G}$ and $C_{\mathbf{G}}(s)^0$ respectively. Then $\mathbf{T}_s$ is obtained by twisting $\mathbf{T}_0$ by w for some $w \in \mathbf{W}$.

Proposition 3.2.22 *Let $\mathbf{T}_0$ be a maximally split torus of $\boldsymbol{G}$. Let $\mathbf{T}_s$ be a maximally split torus of $C_{\mathbf{G}}(s)^0$ obtained twisting $\mathbf{T}_0$ by an element $w \in \mathbf{W}$. Then ${\mathbf{W}_s}^{\mathbf{F}} = C_{\mathbf{W}(s)}(w\phi)$.*

Proof: We know that the Weyl group of $C_{\mathbf{G}}(s)^0$ is isomorphic to $N_{C_{\mathbf{G}}(s)^0}(\mathbf{T}_w)/\mathbf{T}_w$. By Proposition 23.2 in [19], $(N_{C_{\mathbf{G}}(s)^0}(\mathbf{T}_w)/\mathbf{T}_w)^{\mathbf{F}} \simeq C_{C_{\mathbf{G}}(s)^0}(\mathbf{T}_w)/{\mathbf{T}_w}^{\mathbf{F}}$ and it is isomorphic to $C_{\mathbf{W}(s)}(w\phi)$ by Proposition 25.3 of [19]. □

Corollary 3.2.23 *Let s be a rational point of $\mathbf{G}$ under a Frobenius map $\mathbf{F}$. Let $\mathbf{B}_s$ be a $\mathbf{F}$-rational Borel subgroup of $\mathbf{C}_{\mathbf{G}}(s)^o$ containing maximally split torus $\mathbf{T}_w$ obtained twisting a maximally split torus $\mathbf{T}_0$ of $\boldsymbol{G}$ by $w \in \mathbf{W}$. Let $\mathbf{P}$ be a $\mathbf{F}$-rational parabolic subgroup conjugate to a standard parabolic subgroup $\mathbf{B}\mathbf{W}_J\mathbf{B}$ for some rational Borel subgroup $\mathbf{B}$. Assume that s is contained in a $\mathbf{F}$-rational parabolic subgroup $\mathbf{P}$. Then*

(i) the number of $w\mathbf{F}$-rational Borel subgroups of $\mathbf{G}$ containing $\mathbf{B}_s$ is

$$|C_{N_{\mathbf{W}}(\mathbf{W}(s))}(w\phi)/\mathbf{C}_{\mathbf{W}(s)}(w\phi)|$$

(ii) the number of $w\mathbf{F}$-rational Borel subgroups of $\mathbf{P}$ containing $\mathbf{B}_s$ is

$$|C_{N_{\mathbf{W}_J}(\mathbf{W}(s))}(w\phi)/\mathbf{C}_{\mathbf{W}(s)}(w\phi)|$$

Proof: (i) Let $\mathbf{T}_w$ be a maximally split torus contained in $\mathbf{B}_s$. First we want to show that there is $w\mathbf{F}$-stable Borel subgroup $\mathbf{B}$ of $\mathbf{G}$ containing $\mathbf{B}_s$. By assumption $\mathbf{T}_w = g\mathbf{T}_0 g^{-1}$ for some $g \in \mathbf{G}$ where $g^{-1}\mathbf{F}(g) \in N_{\mathbf{G}}(\mathbf{T}_0)$ is

representative of $w \in \mathbf{W}$. Let $\mathbf{B}$ be a $\mathbf{F}$-rational Borel subgroup of $\mathbf{G}$ containing $\mathbf{T}_0$. Then $g\mathbf{B}g^{-1}$ is a Borel subgroup of $\mathbf{G}$ containing the maximal torus $\mathbf{T}_w$. By 3.2.13, the intersection of $g\mathbf{B}g^{-1}$ with $C_{\mathbf{G}}(s)^0$ is a $\underline{\text{rational}}$ Borel subgroup $\mathbf{B}_k$ of $C_{\mathbf{G}}(s)^0$ because it contains the maximally split torus $\mathbf{T}_w$. So there is $v \in \mathbf{W}(s)^{\mathbf{F}}$ such that ${}^v\mathbf{B}_k = \mathbf{B}_s$. Now the Borel group $g^{-1}v\mathbf{B}v^{-1}g$ clearly lies over $\mathbf{B}_s$. Now we want to show that $g^{-1}v\mathbf{B}v^{-1}g$ is $w\mathbf{F}$-stable. Indeed $w\mathbf{F}(g^{-1}v\mathbf{B}v^{-1}g) = w\mathbf{F}(g^{-1}v\mathbf{B}v^{-1}g)w^{-1} = w(\mathbf{F}(g^{-1})\mathbf{F}(v)\mathbf{F}(\mathbf{B})\mathbf{F}(v^{-1})\mathbf{F}(g))w^{-1}$.

But $\mathbf{B}$ and v are $\mathbf{F}$-stable and $w := g^{-1}\mathbf{F}(g)$, we obtain that $w\mathbf{F}(g^{-1}v\mathbf{B}v^{-1}g) = g^{-1}v\mathbf{B}v^{-1}g$. So $g^{-1}v\mathbf{B}v^{-1}g$ is $w\mathbf{F}-$stable.

We know that $\mathbf{W}(s)$ acts simply transitively on the Borel subgroups of $C_G(s)^0$ containing $\mathbf{T}_w$. So any of them is conjugate to $\mathbf{B}_s$ by a unique $v \in \mathbf{W}(s)$. It is clear that ${}^v\mathbf{B}_s$ is rational if and only if $v \in W^{\mathbf{F}}$. Hence $W^{\mathbf{F}}$ acts on the rational Borel subgroups of $C_{\mathbf{G}}(s)^0$ containing $\mathbf{T}_w$ simply transitively. On the other hand, by Lemma 3.2.16, we know that $N_{\mathbf{W}}(\mathbf{W}(s))/\mathbf{W}(s)$ acts simply transitively on the set of Borel subgroups of $\mathbf{G}$ containing $\mathbf{B}_s$. So every Borel subgroup containing $\mathbf{B}_s$ is of the form ${}^v\mathbf{B}'$ for v a representative in $N_{\mathbf{W}(W(s)^{\mathbf{F}})}$. It is clear that ${}^v\mathbf{B}'$ is $w\mathbf{F}$- rational if and only if $w\mathbf{F}({}^v\mathbf{B}') = {}^v\mathbf{B}'$. Observe that since $\mathbf{B}'$ is $w\mathbf{F}$ stable, $\mathbf{F}(\mathbf{B}') = {}^{w^{-1}}\mathbf{B}$. Since $w\mathbf{F}({}^v\mathbf{B}') = {}^{w\mathbf{F}(v)}\mathbf{F}(\mathbf{B}')$, we obtain that $w\mathbf{F}({}^v\mathbf{B}') = {}^{w\mathbf{F}(v)w^{-1}}\mathbf{B}'$. Therefore ${}^v\mathbf{B}'$ is $w\mathbf{F}$-stable if and only if $w\mathbf{F}(v)w^{-1} = v$, which means that $v \in C_{N_{\mathbf{W}}(\mathbf{W}(s))}(w\phi)$.
To prove (ii) first we note that if s is contained in $\mathbf{P}$, then w is ϕ-conjugate to some element in W_J. This follows from by [6], Proposition 6.5.2. Therefore if $\mathbf{B}'$ is a $\mathbf{F}$-rational Borel subgroup contained in $\mathbf{P}$, then $w^{-1}\mathbf{B}'$ also lies in $\mathbf{P}$. Consider the Borel subgroup $\mathbf{B}'$. Then by Lemma 3.2.17, we know that it is of the form $\mathbf{B}'_L\mathbf{U}_{\mathbf{P}}$ where $\mathbf{U}_{\mathbf{P}}$ is the unipotent radical of $\mathbf{P}$ and $\mathbf{B}'_L$ is a Borel subgroup of a Levi complement $\mathbf{L}$ of $\mathbf{P}$. Note that by assumption $\mathbf{B}'$ is $\mathbf{F}$-rational. Hence $\mathbf{B}'_L$ is also $\mathbf{F}$- rational. We know that $N_{\mathbf{W}_J}(\mathbf{W}(s))/\mathbf{W}(s)$ acts simply transitively on Borel subgroups of $\mathbf{P}$ containing $\mathbf{B}_s$ by sending $\mathbf{B}'_L\mathbf{U}_{\mathbf{P}}$ to ${}^v\mathbf{B}'_L\mathbf{U}_{\mathbf{P}}$. Then applying the same arguments in the proof of (i), we obtain that ${}^v\mathbf{B}'_L\mathbf{U}_{\mathbf{P}}$ is $w\mathbf{F}$-rational if and only if $v \in C_{N_{\mathbf{W}_J}(\mathbf{W}(s))}(w\phi)$. Hence we obtain that the number of $w\mathbf{F}$-rational Borel subgroups containing $\mathbf{B}_s$ is $|C_{N_{\mathbf{W}_J}(\mathbf{W}(s))}(w\phi)/\mathbf{C}_{\mathbf{W}(s)}(w\phi)|$.

□

Let l be the length function on $\mathbf{W}$. Recall that for a fixed basis $\Delta \subset \Phi$ and a the positive system Φ^+ containing Δ, it is defined as

$$l(w) = |\{\beta \in \Phi^+ | \ w(\beta) \in \Phi^-\}|.$$

Since $\mathbf{W}$ is a Coxeter group, for a fixed generating set $I = \{s_\alpha | \ \alpha \in \Delta\}$ the length of $w \in \mathbf{W}$ can be given also as follows: If $w = s_1...s_k$, $s_i \in I$, is a reduced expression of w, then $l(w) = k$.

Proposition 3.2.24 *Let $\mathbf{G}$ be a connected reductive group with a maximal split torus $\mathbf{T}_0$ contained in a rational Borel subgroup under a Frobenius endomorphism $\mathbf{F}$. Let $\mathbf{W}$ be the Weyl group of $\boldsymbol{G}$ with respect to $\mathbf{T}_0$. Then*

$$|\mathbf{G}^{\mathbf{F}}| = q^{|\Phi^+|}|\mathbf{T}_0^{\mathbf{F}}| \sum_{v \in \mathbf{W}^{\mathbf{F}}} q^{l(v)}$$

In particular the number of rational Borel subgroups of $\mathbf{G}^{\mathbf{F}}$ is given by $\sum_{w \in \mathbf{W}^{\mathbf{F}}} q^{l(w)}$.

Proof: For the proof of the equation see [9], Proposition 3.18. The order of a Borel subgroup of $\mathbf{G}^{\mathbf{F}} = G$ is $q^{|\Phi^+|}.|\mathbf{T_0}^{\mathbf{F}}|$ by the proof of [9], Proposition 3.18. Let $\mathbf{B}^{\mathbf{F}} = B$. We know that $N_G(B) = B$ and all Borel subgroups are conjugate in G. So $\sum_{w \in \mathbf{W}^{\mathbf{F}}} q^{l(w)}$ gives the number of Borel subgroups of $\mathbf{G}^{\mathbf{F}}$.

Proposition 3.2.25 *Let notation be as above and let H be a parabolic subgroup of G which is conjugate to the standard parabolic subgroup $\mathbf{P}_J$ for some $J \subset I$. If s is contained in at least one conjugate of H, then the number of conjugates of P containing s is given by*

$$|C_{N_W(\mathbf{W}(s))}(w\phi)|/|C_{N_{\mathbf{W}_J}(\mathbf{W}(s))}(w\phi)| \sum_{w \in W(s)^{\mathbf{F}}} q^{l(w)}$$

.

Proof: Let $\mathcal{H}$ be the set of all $\mathbf{F}$-rational conjugates of $\mathbf{H}$ in $\mathbf{G}$. Observe that given a rational Borel subgroup $\mathbf{B}$ of $\mathbf{G}$, there is unique element $\mathbf{Q}$ in $\mathcal{H}$ containing $\mathbf{B}$, hence containing ${}^{w^{-1}}\mathbf{B}$. In fact, by Proposition 3.2.11 two conjugate parabolic subgroups can not contain the same Borel subgroup of $\mathbf{G}$. It follows that each rational Borel subgroup $\mathbf{B}_s$ of $C_{\mathbf{G}}(s)^0$ determines a unique $\mathbf{Q} \in \mathcal{H}$. Indeed if $s \in \mathbf{Q}$, by Proposition 3.2.13, the intersection $\mathbf{Q} \cap \mathbf{C_G}(s)^0$ is a parabolic subgroup of $\mathbf{C_G}(s)^0$ hence contains a rational Borel subgroup $\mathbf{B}_s$ of $\mathbf{C_G}(s)^0$. Conversely, given any rational Borel subgroup $\mathbf{B}_s$ of $C_{\mathbf{G}}(s)^0$, any parabolic subgroup of $\mathbf{G}$ containing $\mathbf{B}_s$ contains a $w\mathbf{F}$-rational Borel subgroup $\mathbf{B}$ of $\mathbf{G}$ containing $\mathbf{B}_s$, and any such $\mathbf{B}$ containing $\mathbf{B}_s$ determine a unique parabolic subgroup in $\mathcal{H}$ containing it. □

Let $\mathcal{H}^{\mathbf{F}}_{\mathbf{s}}$ be the subset $\{\mathbf{Q} \in \mathcal{H}| \quad \int \in \mathbf{Q}\}$ of $\mathcal{H}$. Then $\mathcal{H}^{\mathbf{F}}_{\mathbf{s}}$ is the set of parabolic subgroups of G that conjugate to H containing s.

To determine the cardinality of the set $\mathcal{H}^{\mathbf{F}}_{\mathbf{s}}$ it is enough to count the $w\mathbf{F}$-rational Borel subgroups of $\mathbf{G}$ containing a rational Borel subgroup $\mathbf{C_G}(s)^o$. Note that in this way we count each parabolic subgroups in $\mathcal{H}^{\mathbf{F}}_{\mathbf{s}}$ n times, where n denotes the number of $w\mathbf{F}$-rational Borel subgroup of $\mathbf{P}$ containing a fixed Borel subgroup $\mathbf{B}_s$ of $\mathbf{C_G}(s)^0$. Observe that n is the same for all parabolic subgroups containing s. By Proposition 3.2.24, we know that the number of Borel subgroups of $\mathbf{C_G}(s)^{0\mathbf{F}}$ is

$$\sum_{w \in \mathbf{W}(s)^{\mathbf{F}}} q^{l(w)}$$

For each rational $\mathbf{B}_s$ in $C_{\mathbf{G}}(s)^0$, there are exactly $|C_{N_{\mathbf{W}}(\mathbf{W}(s))}(w\phi)/C_{\mathbf{W}}(s)(w\phi)|$. $w\mathbf{F}$-rational Borel subgroups of G containing $\mathbf{B}_s$. So the number of all $w\mathbf{F}$-Borel subgroups of G containing a Borel subgroup of $C_{\mathbf{G}}(s)^0$ is

$$\frac{|C_{N_{\mathbf{W}}(\mathbf{W}(s))}(w\phi)|}{|C_{\mathbf{W}(s)}(w\phi)|} \sum_{v \in \mathbf{W}(s)^{\mathbf{F}}} q^{l(v)}$$

Each parabolic subgroup $Q \in \mathcal{H}_{\mathbf{s}}^{\mathbf{F}}$ contains exactly $|C_{N_{\mathbf{W}_J}(\mathbf{W}(s)}(\phi)/C_{\mathbf{W}(s)}(\phi)|$ $w\mathbf{F}$-rational Borel subgroups of G containing $\mathbf{B}_s$. Hence we conclude that the cardinality of the set $\mathcal{H}_{\mathbf{s}}^{\mathbf{F}}$ is

$$\frac{|C_{N_{\mathbf{W}}(\mathbf{W}(s))}(w\phi)|}{|C_{N_{\mathbf{W}_J}(\mathbf{W}(s))}(w\phi)|} \sum_{v \in \mathbf{W}(s)^{\mathbf{F}}} q^{l(v)}.$$

□

Let ϕ be as above. Recall that by Proposition 4.2.20 , the action of $\mathbf{F}$ on the character group $\mathbf{X}(\mathbf{T})$ of $\mathbf{G}$ with respect to the maximal torus $\mathbf{T}$ is $q\phi$ for some p-power q. Let

Corollary 3.2.26 *Let notation be as above and let F/K be an extension of function fields with Galois closure M. Assume that $Gal(M/K) = G$ is a finite group of Lie type which is the group of fixed points of a connected algebraic group $\boldsymbol{G}$ under a Frobenius map $\mathbf{F}$ whose action on character group $\mathbf{X}(\mathbf{T_0})$ is $q\phi$ for some maximally split torus $\mathbf{T}_0$. Assume that F is the fixed field of a parabolic subgroup H which is conjugate to $H = \mathbf{B}\mathbf{W}_J\mathbf{B}^{\mathbf{F}}$ for some $J \subset I$ where I is the set of involutions that generate W. Let P be an unramified place of K, and let $s \in G$ be a Frobenius element of P in M/K, which is semisimple element of order n. Let $\mathbf{T}_w$ be a maximally split torus of $C_G(s)^0$ that is obtained twisting $\mathbf{T}_0$ by $w \in \mathbf{W}$. Then the number m_i of places $\widetilde{Q}$ of F lying over P with $f(\widetilde{Q}|P) = i$ is given by*

$$m_i = \frac{\mu_n(i)}{n} \cdot \frac{C_{N_{\mathbf{W}}(\mathbf{W}(s^i))}(w\phi)}{C_{N_{\mathbf{W}_J}(\mathbf{W}(s^i))}(w\phi)} \sum_{v \in \mathbf{W}(s^i)^{\mathbf{F}}} q^{l(v)}$$

Proof: The number of conjugate of H containing s^i is

$$\frac{C_{N_{\mathbf{W}}(\mathbf{W}(s^i))}(\phi)}{C_{N_{\mathbf{W}_J}(\mathbf{W}(s^i))}(\phi)} \sum_{v \in W(s^i)^{\mathbf{F}}} q^{l(v)}$$

by Proposition 3.2.25. Applying Theorem 3.1.8 we obtain desired result. □

Now we want to determine m_i for the case that a Frobenius element g of P is arbitrary. By Proposition 3.2.9, $g = su = us$ where u is a unipotent element and s is a semisimple element. To count the number of parabolic subgroups that are conjugate to a fixed parabolic of G and containing g, we need the following:

Proposition 3.2.27 *If $g = su$ is the Jordan decomposition of an element of $\boldsymbol{G}$, then $g \in C_{\boldsymbol{G}}(s)^0$.*

Proof: See [9], Proposition 2.5.

Proposition 3.2.28 *Let $\boldsymbol{G}$ be a connected algebraic group defined over $\mathbb{F}_p$. Then any $\mathbf{F}$-rational unipotent element is contained in a $\mathbf{F}$-rational Borel subgroup.*

Proof: See [9], Corollary 3.20.

Let g be an element in G. Since g is rational then both s and u are rational. Rationality of s implies that $C_{\mathbf{G}}(s)^0$ is a rational subgroup of $\mathbf{G}$. Recall that s is contained in all maximal tori of $C_{\mathbf{G}}(s)^0$. In particular, it is contained in all maximally split tori of $C_{\mathbf{G}}(s)^0$. It follows that s is contained in all Borel subgroups of $C_{\mathbf{G}}(s)^0$. On the other hand, since u is a rational element of $C_{\mathbf{G}}(s)^0$, it is contained in some Borel subgroup+ of $C_{\mathbf{G}}(s)^0$. We conclude that g is contained in all Borel subgroups of $C_{\mathbf{G}}(s)^0$ containing u. Let $\mathbf{P}$ be a parabolic subgroup of $\mathbf{G}$. Then g is contained in $\mathbf{P}$ if and only if there is a Borel subgroup of $\mathbf{G}$ contained in $\mathbf{P}$ whose intersection with $C_{\mathbf{G}}(s)^0$ is a Borel subgroup of $C_{\mathbf{G}}(s)^0$ containing u. Denote by $\mathcal{B}_u$ the set of rational Borel subgroups of $C_{\mathbf{G}}(s)^0$ containing u. Combining these with previous results, we obtain the following :

Corollary 3.2.29 *Let notation be as above. Let $g = su$ be a rational element of $\boldsymbol{G}$ under a Frobenius map $\mathbf{F}$. Let H be a parabolic subgroup of G which is conjugate to the standard parabolic subgroup $\mathbf{P}_J{}^{\mathbf{F}}$ for some $J \subset I$. Then the number of rational parabolic subgroups of $\boldsymbol{G}$ that $\boldsymbol{G}^{\mathbf{F}}$ conjugate to $\mathbf{H}$ and containing g is*

$$|C_{N_{\mathbf{W}}\mathbf{W}(s)}(w\phi)|/|C_{N_{\mathbf{W}_J}(\mathbf{W}(s))}(w\phi)| \cdot |\mathcal{B}_u|$$

Corollary 3.2.30 *Let notation be as in Corollary 3.2.26 and let F/K be an extension of function fields with Galois closure M. Let P be an unramified place of K, and let $su = g \in G$ be a Frobenuis element of P of order n in the extension M/K. Then the number m_i of places $\widetilde{Q}$ of M lying over P with $f(\widetilde{Q}|N) = i$ is given by*

$$m_i = \frac{\mu_n(i)}{n} \cdot |C_{N_{\mathbf{W}}(\mathbf{W}(s^i))}(\phi)|/|C_{N_{\mathbf{W}_J}(\mathbf{W}(s^i))}(\phi) \cdot |\mathcal{B}_{u^i}|.$$

Remark 3.2.3 *When P is ramified and $D(R|P)$ is a cyclic group generated by $g = su$, then we can deduce that the number m_i of places $\widetilde{Q}$ of F with $e(\widetilde{Q}|P)f(\widetilde{Q}|P) = i$ is*

$$m_i = \frac{\mu_n(i)}{n} \cdot |C_{N_{\mathbf{W}}(\mathbf{W}(s^i))}(\phi)|/|C_{N_{\mathbf{W}_J}(\mathbf{W}(s^i))}(\phi) \cdot |\mathcal{B}_{u^i}|.$$

We have seen that, for any $g \in G$, the number of parabolic subgroups of G that contain $g = su$, depends on the combinatorial data of the centralizer $C_G(s)^0$ of the semisimple element s. This data consists of the number of Borel subgroup that contains u and the Weyl group $W(s)$ of $C_G(s)$. When $u = 1$ we know the exact value. If two subgroups C_1, C_2 of G are conjugate in G, then the data that they convey will be the same. Now we are interested in the set of conjugacy classes of centralizers of semisimple elements in G.

In literature there are two important works on conjugacy classes of centralizers of semisimple elements in a finite group of Lie type. Deriziotis gives the criteria for a closed connected reductive subgroup of $\mathbf{G}$ to be a centralizer of semisimple elements, in terms of root system of G in the articles [7] and [8]. He also gives the parametrization of these classes in terms of subset of the root system of G inherited from $\mathbf{G}$. Carter gives all conjugacy classes of centralizer of semisimple elements in a finite group of Lie type for classical types A_n, B_n, C_n and D_n explicitly. He also computed their orders. See [5].

Now we state the following Theorem which gives the conjugacy classes of centralizer of semisimple elements in G:

Theorem 3.2.31 $\mathbf{G}$ *is simple linear algebraic group defined over* $\mathbb{F}_p$*. Let* $G = \mathbf{G}^{\mathbf{F}}$ *be finite group of Lie type with a Frobenius endomorphism* $\mathbf{F}$*. Let* $\widetilde{\Delta} = \Delta \cup \{-\alpha_0\}$ *where* Δ *is a basis for a root system* Φ *of* $\boldsymbol{G}$ *with respect to a maximal torus* $\mathbf{T}$ *and* α_0 *be highest root. Let* $\mathbf{W}_J$ *be the Weyl group of the subsytem* Φ_J *of* Φ *generated by* $J \subset \widetilde{\Delta}$*. Then* G*-conjugacy classes of centralizers of semisimple elements are parametrized by* $(J, [v])$ *where* J *is a subset of* $\widetilde{\Delta}$ *and* $[v]$ *is a conjugacy class in the group* $N_{\mathbf{W}}(\mathbf{W}_J)/\mathbf{W}_J$*.*

Proof: See [8]. □

3.3. Decomposition of the Polynomials $x^{\langle n-1\rangle} + x - \alpha$

In this section we will assume that $\mathbb{F}_q \subseteq \mathbb{F}$ and consider the polynomial $h(x) = x^{\langle n-1\rangle} + x$ over $\mathbb{F}$, where $\langle i\rangle = q^i + q^{i-1} + ...q^1 + 1$ with the conventions $\langle 0\rangle = 1$ and $\langle -1\rangle = 0$. We point out here that the polynomial that we studied in Section 2.3 is the special case $n = 2$. Let $h(x) = z$. In the paper [1], Abhyankar has shown that $\mathbb{F}(x)/\mathbb{F}(z)$ has the Galois closure M with $Gal(M/\mathbb{F}(z)$ isomorphic to $PGL(n, q)$. Furthermore he has proved that in the extension $\mathbb{F}(x)/\mathbb{F}(z)$ the only ramified places of $\mathbb{F}(z)$ are P_0 and P_∞. In this section we want to find the decomposition of a place $P \in \mathbb{P}_{\mathbb{F}(z)}$ in the extension $\mathbb{F}(x)/\mathbb{F}(z)$. In particular, if P is a rational place corresponding to the element $\alpha \in \mathbb{F}$, we will find the number of roots of $h(x) - \alpha$ in $\mathbb{F}$.

Now we consider the group $PGL(n, q)$ as the group of fixed points of $PGL(n, \overline{\mathbb{F}}_p)$ under the standard Frobenius map $\mathbf{F}$. It is well known that the type of $PGL(n, \overline{\mathbb{F}}_p)$ is A_{n-1} and the Weyl group of linear algebraic groups of type A_{n-1} is the symmetric group S_n on n letters. It is a Coxeter group generated by $I = \{s_i = (i, i+1) |\ 1 \le i \le n-1\}$. As explained by [19] in example 22.6 and beginning of Section 22.2, $\mathbf{F}$ acts trivially on the Weyl group S_n of $PGL(n, \overline{\mathbb{F}}_p)$. Hence the automorphism ϕ acts on $\mathbf{W}$ as the identity.

First we will determine the structure of the subgroup H of $PGL(n,q)$ whose fixed field is $\mathbb{F}(x)$. Indeed it is a parabolic subgroup of $PGL(n,q)$. To see this, observe that the degree of the extension $\mathbb{F}(x)/\mathbb{F}(h(x))$ is $1+q+...+q^{n-1}$ which is prime to p. Hence H contains a Sylow p-subgroup of $PGL(n,q)$. By definition, a parabolic subgroup contains a Borel subgroup of $PGL(n,q)$. So it is enough to show that a maximally split torus is also contained in H. To do this we look at the order of $PGL(n,q)$. It is given by

$$q^{n(n+1)/2}(q^2-1)(q^3-1)\cdot ... \cdot(q^n-1)$$

On the other hand, since ϕ fixes each element of I, then the length of each orbit of ϕ is just 1. By the order formula given in [6] Section 2.9, a maximally split torus of G has order $(q-1)^{n-1}$. Therefore H contains a maximally split torus T, hence contains a Borel subgroup B. We recall that by Borel subgroups of $PGL(n,q)$ we mean that they are the fixed points $\mathbf{B}^{\mathbf{F}}$ of $\mathbf{F}$-rational Borel subgroups of $\mathbf{PGL}(n,\overline{\mathbb{F}}_p)$. Therefore it is a parabolic subgroup. Hence H is of the form $\mathbf{B}\mathbf{W}_\mathbf{J}\mathbf{B}^\mathbf{F}$ for a subset $J\subset I$.

Our next aim is to determine the set J. To do this first we need the following: Recall that a Coxeter group W is a group generated by a subset $\{s_1,...,s_k\}\subset W$ such that $(s_i)^2=1$ for all $1\leq i\leq k$.

Let W be a finite Coxeter group with a generating set $I=\{s_1,...,s_k\}$. A subgroup of W is called parabolic if it is conjugate to the subgroup W_J generated by some $J\subset I$. By definition, W_J is also a Coxeter group. Let l be the length function on W relative to I. See Appendix for the definition. The following proposition summarizes the behavior of l on W_J.

Proposition 3.3.32 *Let W be a finite Coxeter group with a generating set I and let $J\subset I$. Let l be the length function on W.*

(i) Viewing W_J as a Coxeter group with length function l_J relative to the generating set J, we have $l=l_J$ on W_J

(ii) Define $W^J:=\{w\in W|\ l(ws)>l(w)$ for all $s\in J\}$. Given $w\in W$, there is a unique $u\in W^J$ and a unique $v\in W_J$ such that $w=uw$. Their lengths satisfy $l(w)=l(u)+l(v)$. Moreover, u is the unique element of smallest length in the coset wW_J.

Proof: See [14], Proposition in Section 1.10.

The distinguished coset representatives in W^J are called minimal coset representatives of the subgroup W_J.

Let W be a Coxeter group. Given a subset X of W we define a polynomial $X(t)$ attached to X as follows.

$$X(t):=\sum_{w\in X}t^{l(w)}$$

When $X = W$, we call $W(t)$ the Poincare polynomial of W.

Proposition 3.3.33 *Let notation be as above. Then* $W(t) = W_J(t)W^J(t)$

Proof: It is stated in [14], Section 1.11. □

We notice here that given a subgroup W' of W, $W'(t)$ divides $W(t)$ if and only if the subgroup W' has minimal coset representatives.

Let $\mathbf{G}$ be a connected reductive algebraic group with a Frobenius endomorphism $\mathbf{F}$. Now given an $\mathbf{F}$-stable parabolic subgroup $\mathbf{P}_J$ of $\mathbf{G}$, we want to express $|\mathbf{G}^{\mathbf{F}}/{\mathbf{P}_J}^{\mathbf{F}}|$ in terms of Poincare polynomials. First we need to show that ${\mathbf{W}_J}^{\mathbf{F}}$ has minimal coset representatives in $\mathbf{W}^{\mathbf{F}}$. But first we will state that $\mathbf{W}^{\mathbf{F}}$ is a Coxeter group.

Proposition 3.3.34 *Let* $\mathbf{W}$ *be the Weyl group of a root system with set of simple reflections* $I \subset \mathbf{W}$ *and* ϕ *an automorphism of* $\mathbf{W}$ *stabilizing* I.

(i) For each ϕ*-orbit* $J \subset I$, ${\mathbf{W}_J}^{\phi} = \langle s_J \rangle$ *for a (unique) involution* $s_J \in \mathbf{W}_J$.

(ii) The group of fixed points $\mathbf{W}^{\mathbf{F}}$ *is a Coxeter group generated by* $\{s_J| \ J \ \text{ is a } \ \phi-$ *orbit*$\}$.

Proof: See [19],Lemma 23.3 □

Observe that a parabolic subgroup $\mathbf{G}^{\mathbf{F}}$-conjugate to $\mathbf{P}_J$ is rational if and only if J is fixed by ϕ. Let J be a ϕ-stable subset of I. Let I' and J' be the sets of ϕ-orbits on I and on J respectively. Then J' is a subset of I'. Since the set I' is generating set of $\mathbf{W}^{\mathbf{F}}$ as a Coxeter group, ${\mathbf{W}_J}^{\mathbf{F}}$ is a parabolic subgroup of $\mathbf{W}^{\mathbf{F}}$. Hence we obtain that there is a bijection between G-conjugacy classes of rational parabolic subgroups of $\mathbf{G}$, and the set of subsets of I'. Related argument can be found in Section 6.5 of [3].

We define $\mathbf{W}^{\mathbf{F}}(t) = \sum_{v \in \mathbf{W}^{\mathbf{F}}} q^{l(v)}$. We point out that $l(v)$ is the length of v in $\mathbf{W}$, not in $\mathbf{W}^{\mathbf{F}}$.

Proposition 3.3.35 *Let notation be as above, then* $\mathbf{W}_J^{\mathbf{F}}(t)|\mathbf{W}^{\mathbf{F}}(t)$.

Proof: We know by Proposition 3.2.24 that the number of Borel subgroups of $\mathbf{G}^{\mathbf{F}}$ is $\sum_{v \in \mathbf{W}^{\mathbf{F}}} q^{l(v)}$ which is equal to $\mathbf{W}^{\mathbf{F}}(q)$. Let $\mathbf{L}_J$ be a Levi complement of $\mathbf{P}_J = \mathbf{B}\mathbf{W}_J\mathbf{B}$ for some rational Borel subgroup of $\mathbf{G}$. Then again by Proposition 3.2.24 $\mathbf{W}_J^{\mathbf{F}}(q) = \sum_{v \in \mathbf{W}_J^{\mathbf{F}}} q^{l(v)}$ is the number of Borel subgroups of $\mathbf{L}_J^{\mathbf{F}}$. But since any Borel subgroup of $\mathbf{L}_J$ is extended uniquely to a Borel subgroup of $\mathbf{P}_J$, $\mathbf{W}_J^{\mathbf{F}}(q)$ is equal to the number of Borel subgroups of $\mathbf{P}_J^{\mathbf{F}}$. But $\mathbf{B}$ is a subgroup of $\mathbf{P}$ and $N_{\mathbf{P}}(\mathbf{B}) = \mathbf{B}$, hence $\mathbf{W}_J^{\mathbf{F}}(q)$ is equal to the number of all Borel subgroups of $\mathbf{P}_J$. So $\mathbf{W}_J^{\mathbf{F}}(t)|\mathbf{W}^{\mathbf{F}}(t)$. □

Since $\mathbf{W}_J^{\mathbf{F}}(t)|\mathbf{W}^{\mathbf{F}}(t)$, we conclude that $\mathbf{W}_J^{\mathbf{F}}$ has minimal coset representatives in $\mathbf{W}^{\mathbf{F}}$. Let $\mathbf{W}^{J\mathbf{F}}$ be the set of minimal coset representatives of ${\mathbf{W}_J}^{\mathbf{F}}$ in $\mathbf{W}^{\mathbf{F}}$, and let $\mathbf{W}^{J\mathbf{F}}(q) = \sum_{v \in \mathbf{W}^{J\mathbf{F}}} q^{l(v)}$.

Proposition 3.3.36 *Let $\boldsymbol{G}$ be a reductive algebraic group defined over $\mathbb{F}_q$ and let $\mathbf{B}$ be a rational Borel subgroup under a Frobenius endomorphism $\mathbf{F}$. Let $\mathbf{P}$ be a rational parabolic subgroup of $\boldsymbol{G}$ which is conjugate to $\mathbf{B}\mathbf{W}_J\mathbf{B}$ for some ϕ-stable $J \subset I$. Denote by G the group $\mathbf{G}^{\mathbf{F}}$ and by P the group $\mathbf{P}^{\mathbf{F}}$. Then $|G/P| = \mathbf{W}^{J\mathbf{F}}(q)$. In particular the index of $\mathbf{W}_J$ is equal to sum of coefficients of $\mathbf{W}^{J\mathbf{F}}(t)$.*

Proof: We know that in G, all Borel subgroups are conjugate, and they are self normalizing subgroups of G. So $|G/B|$ is the number of Borel subgroups contained in G. By Proposition 3.2.24, this number is given by $\sum_{v\in\mathbf{W}^{\mathbf{F}}} q^{l(v)}$ which is the Poincare polynomial $\mathbf{W}^{\mathbf{F}}(q)$. On the other hand $|G/B| = |G/P| \cdot |P/B|$. We already know by Proposition 3.3.35 that $|P/B| = W_J^F(q)$ is the number of Borel subgroups of G contained in P. Combining all of these, we obtain that $|G/P| = |G/B|/|P/B| = \frac{\mathbf{W}_J{}^{\mathbf{F}}(q)\cdot W^{J\mathbf{F}}(q)}{\mathbf{W}_J{}^{\mathbf{F}}(q)} = \mathbf{W}^{J\mathbf{F}}(q)$. Since the set $\mathbf{W}^{J\mathbf{F}}$ is a set of coset representatives of the subgroup $\mathbf{W}_J{}^{\mathbf{F}}$, the sum of coefficients of $\sum_{w\in\mathbf{W}^{J\mathbf{F}}} q^{l(w)}$ clearly gives the index of $\mathbf{W}_J{}^{\mathbf{F}}$ in $\mathbf{W}$. □

In particular, since $|G/H| = 1+q+...+q^{n-1}$, and ϕ is identity, by Proposition 3.3.36, we conclude that $|\mathbf{W}/\mathbf{W}_J|$ is n. As we noted above, the type of $\mathbf{PGL}(n, \overline{\mathbb{F}}_p)$ is A_{n-1} and in this type, each conjugacy class of parabolic subgroups of S_n gives rise to a partition of n. If $(n_1, ...n_r)$ is the partition of n corresponding to J, then $\mathbf{W}_J = S_{n_1} \times ... \times S_{n_r}$. All related arguments can be found in [18],Section 2.1. So $|\mathbf{W}/\mathbf{W}_J| = \frac{n!}{n_1!\cdot...\cdot n_r!}$. Hence the parabolic subgroup of $\mathbf{W}$ corresponding to H should be in the class given by the partition $(1, n-1)$ of n. We deduce that $\mathbf{W}_J$ is the group S_{n-1}.

In type A_n, all roots have the same lengths, hence there is no longest root. Therefore all closed connected subgroups of $\mathbf{G} = PGL(n, \overline{\mathbb{F}}_p)$ of maximal rank are Levi subgroups. Therefore for any $s \in \mathbf{G}$, $C_{\mathbf{G}}(s)^0$ is a Levi subgroup of $\mathbf{G}$, hence $\mathbf{W}(s)$ is isomorphic to W_J for some $J \subset I$. In $\mathbf{G}$ all Levi subgroups of a parabolic subgroup are conjugate. But this is no longer true in $\mathbf{G}^{\mathbf{F}}$. The following theorem gives the $\mathbf{G}^{\mathbf{F}}$-conjugacy classes of Levi subgroups.

Theorem 3.3.37 *Let Φ be a set of roots of $\boldsymbol{G}$ with respect to a maximally split torus $\mathbf{T}_0$. Let Δ be a basis in Φ. Then $\mathbf{G}^{\mathbf{F}}$-conjugacy classes of Levi subgroups of G are parametrized by $\mathbf{F}$- conjugacy classes of $\mathbf{W}_J w$ where $J \subset \Delta$ and ${}^{w\mathbf{F}}\mathbf{W}_J = \mathbf{W}_J$.*

Proof: See [9], Proposition 4.3

Note here that when $\mathbf{L}_J$ corresponds to the class $\mathbf{W}_J w$, then the maximally split torus of $\mathbf{L}_J$ is obtained twisting $\mathbf{T}_0$ by $w \in \mathbf{C}_w$, where $\mathcal{C}_w$ is a ϕ-conjugacy class in W. Indeed we have seen that $w \in \mathbf{W}_J$. So this conjugacy class $\mathcal{C}_w$ is in $\mathbf{W}_J$. On the other hand, since ϕ is identity, ϕ-conjugacy classes of S_n are usual conjugacy classes of S_n. Hence we obtain that $\mathbf{W}_J{}^{w}\mathbf{F} = C_{\mathbf{W}_J}(w)$.

Recall that maximal tori of $\mathbf{G}$ are also Levi subgroups of $\mathbf{G}$ with root system corresponding to the empty set $\subset \Delta$. Hence they are parametrized by conjugacy classes of S_n by Theorem 3.3.37. We also note that for each maximal torus $\mathbf{T}$ of $\mathbf{G}$, there is a semisimple element s in $\mathbf{G}$ whose centralizer $C_{\mathbf{G}}(s)^0$ is T. Such an element is called a regular element of $\mathbf{G}$. See [9], Proposition 14.6 and Corollary 14.7 for the existence of these elements.

We summarize:

Theorem 3.3.38 *Let notation be as above. Let P_α be a rational place of $\mathbb{F}(h(x))$ corresponding to $\alpha \in \mathbb{F}$. Assume that a Frobenius element $g \in G$ of P_α in the extension $M/\mathbb{F}(h(x))$ has order prime to p. Let m_i be the number of irreducible factors $h_i(x)$ of $h(x) - \alpha$ of degree i in $\mathbb{F}$. If $i|n$, then there exist a subset $J \subset I$, and a conjugacy class $\mathcal{C}_w$ of $\mathbf{W}_J$ containing w such that*

$$m_i = \frac{\mu_n(i)}{n} N_{S_n}(C_{\mathbf{W}_J}(w))/N_{S_{n-1}}(C_{\mathbf{W}_J}(w)) \cdot \sum_{v \in C_{\mathbf{W}_J}(w)} q^{l(v)}.$$

Proof: Recall that if $i \nmid n$ there are no irreducible factors of degree i. So we consider the case $i|n$. By Theorem 3.2.26, the number of degree i places of $\mathbb{F}(x)$ lying over P_α is given by

$$m_i = \frac{\mu_n(i)}{n} \cdot \frac{C_{N_{\mathbf{W}}(\mathbf{W}(s^i))}(w\phi)}{C_{N_{\mathbf{W}_J}(\mathbf{W}(s^i))}(w\phi)} \sum_{v \in \mathbf{W}(s^i)^{\mathbf{F}}} q^{l(v)}.$$

Since $C_G(s)^0$ is a Levi subgroup, $\mathbf{W}(s)^{\mathbf{F}}$ is of the form $C_{\mathbf{W}_J}(w)$ for some $J \subset I$. Since the group H has a Levi subgroup whose Weyl group is S_{n-1}, the result follows. □

Corollary 3.3.39 *Let notation be as above. Let P_α be a rational place of $\mathbb{F}(h(x))$ corresponding to $\alpha \in \mathbb{F}$. Assume that the Frobenius element $g \in G$ of P_α in the extension $M/\mathbb{F}(h(x))$ is $g = su = us$ where the order of s is prime to p and u has order a power of p. For $i|n$, let $J \subset \Delta$ and $\mathbf{W}_J w$ correspond to $C_{\mathbf{G}}(s^i)^0$ as in Theorem 3.3.37. Let $\mathbf{B}_u$ be the set of all Borel subgroups of $C_G(s^i)^{0\mathbf{F}}$ containing u. Then the number of irreducible factors $h_i(x)$ of $h(x) - \alpha$ of degree i is*

$$N_{S_n}(C_{\mathbf{W}_J}(w))/N_{S_{n-1}}(C_{\mathbf{W}_J}(w)) \cdot |\mathbf{B}_u|.$$

CHAPTER 4

Appendix

4.1. Structure of Algebraic Groups

Definition 4.1.1 *An **algebraic group** is an affine variety over an algebraically closed field $\mathbb{K}$ endowed with a group structure such that the multiplication and inverse maps are algebraic. For such a group $\mathbf{G}$, we will call elements of $\mathbf{G}$ the elements of the set $\mathbf{G}(\mathbb{K})$ of $\mathbb{K}$- valued points of $\mathbf{G}$.*

Example 4.1.1 *(i) The multiplicative group $\mathbb{G}_{\mathbf{m}}$, and the additive group $\mathbb{G}_{\mathbf{a}}$, defined respectively by the algebras $\mathbb{K}[T, T^{-1}]$ and $\mathbb{K}[T]$ are examples of algebraic groups. We have $\mathbb{G}_{\mathbf{m}} \simeq \mathbb{K}^{\times}, \mathbb{G}_{\mathbf{a}} \simeq \mathbb{K}^{+}$.*

(ii) The linear group GL_n and its subgroup, the special linear group SL_n.

Definition 4.1.2

*(i) An algebraic group is called **linear** if it is isomorphic to a closed subgroup of GL_n.*

*(ii) An element of a linear algebraic group $\mathbf{G}$ is called **semi-simple**(respectively, **unipotent**) if its image in some embedding of $\mathbf{G}$ in a GL_n is semi-simple (respectively unipotent).*

Theorem 4.1.1 ***(Jordan decomposition)*** *Let $\boldsymbol{G}$ be a linear algebraic group. Then for any embedding ρ of $\boldsymbol{G}$ into some $GL(V)$, and for any $g \in \boldsymbol{G}$, there exist unique $g_s, g_u \in \boldsymbol{G}$ such that $g = g_s \cdot g_u = g_u \cdot g_s$ where $\rho(g_s)$ is semisimple and $\rho(g_u)$ is unipotent. This decomposition of g is independent of the chosen embedding.*

Proof: See [19], Theorem 2.5. □

Tori, solvable groups, Borel subgroups

Definition 4.1.3 *(i) A **torus** is an algebraic group defined over* $\mathbb{K}$ *which is isomorphic to the product of a finite number of copies of the multiplicative group* $\mathbb{K}^\times$.

(ii) A rational character of an algebraic group $\boldsymbol{G}$ *is an algebraic group morphism from* $\boldsymbol{G}$ *to* $\mathbb{G}_{\mathbf{m}}$.

(iii) The character group $\mathbf{X}(\mathbf{T})$ *is the group of rational characters of* $\mathbf{T}$.

Let $\mathbf{G}$ be a linear algebraic group. The irreducible components of $\mathbf{G}$ are pairwise disjoint. So they are connected components of $\mathbf{G}$

Definition 4.1.4 *Let* $\boldsymbol{G}$ *be a linear algebraic group. The irreducible component* $\boldsymbol{G}^0$ *of* $\boldsymbol{G}$ *containing* $1 \in \boldsymbol{G}$ *is a closed normal subgroup of finite index in* $\boldsymbol{G}$ *and called the* ***identity component*** *of* $\boldsymbol{G}$.

Proposition 4.1.2 *For a solvable algebraic group* $\boldsymbol{G}$,

(i) Every semi-simple element of $\boldsymbol{G}^0$ *lies in a maximal torus of* $\boldsymbol{G}$.

(ii) All maximal tori are conjugate.

(iii) If $\boldsymbol{G}$ *is connected, the set* $\boldsymbol{G}_{\mathbf{u}}$ *of unipotent elements of* $\boldsymbol{G}$ *is a normal connected subgroup, and for every maximal torus* $\mathbf{T}$ *of* $\boldsymbol{G}$, *there is a semi-direct product decomposition* $\boldsymbol{G} = \boldsymbol{G}_{\mathbf{u}} \rtimes \mathbf{T}$.

Proof: See [23], 6.11. □

Definition 4.1.5 *Maximal closed connected solvable subgroups of an algebraic group are called* ***Borel subgroups***.

These groups are of paramount importance in the theory. The next theorem states their basic properties.

Theorem 4.1.3 *Let* $\boldsymbol{G}$ *be a connected algebraic group. Then:*

(i) All Borel subgroups are conjugate,

(ii) Every element of $\boldsymbol{G}$ *is in some Borel subgroup.*

(iii) A Borel subgroup is equal to its normalizer in $\boldsymbol{G}$.

Proof: For a detailed proof see [23], 7.2.6, 7.3.3, 7.3.7. □

Theorem 4.1.4 *Let $\boldsymbol{G}$ be a connected algebraic group. Then:*

(i) Any closed subgroup containing a Borel subgroup is equal to its normalizer in $\boldsymbol{G}$, and is connected.

(ii) Two closed subgroups, containing the same Borel subgroup and conjugate in $\mathbf{G}$ are equal.

Proof: For a detailed proof see [9], 0.12. □

Definition 4.1.6 *A closed subgroup of $\boldsymbol{G}$ containing a Borel subgroup is called parabolic subgroup of $\boldsymbol{G}$.*

Radical, unipotent radical, reductive and semi-simple groups

Definition 4.1.7 *A **unipotent subgroup** of an algebraic group is a subgroup containing only unipotent elements.*

The product of all the closed connected normal solvable subgroups of $\mathbf{G}$ is also closed connected normal solvable subgroup of $\mathbf{G}$, called **the radical** of $\mathbf{G}$, and denoted by $R(\mathbf{G})$. Similarly, the set of all closed connected normal unipotent subgroups of $\mathbf{G}$ has a unique maximal element called **unipotent radical** of $\mathbf{G}$, and denoted by $R_u(\mathbf{G})$.

Definition 4.1.8 *An algebraic group is called **reductive**, if its unipotent radical is trivial, and **semi-simple**, if its radical is trivial.*

Example 4.1.2 *The group GL_n is reductive. The group SL_n is semi-simple.*

Roots, coroots, root systems, structure theorem for reductive groups

Let $\mathbf{T}$ be a torus. Algebraic group homomorphisms from $\mathbb{G}_\mathbf{m}$ to $\mathbf{T}$ are called **one-parameter subgroups** of $\mathbf{T}$. They form an abelian group denoted by $Y(\mathbf{T})$. There is an exact pairing between $X(\mathbf{T})$ and $Y(\mathbf{T})$ (i.e, a map $X(\mathbf{T}) \times Y(\mathbf{T}) \to \mathbb{Z}$) obtained as follows: given $\chi \in X(\mathbf{T})$ and $\psi \in Y(\mathbf{T})$ the composite map $\chi \circ \psi$ is a homomorphism from $\mathbb{G}_\mathbf{m}$ to itself, so is of the form $x \mapsto x^n$ for some $n \in \mathbb{Z}$. The map $X(\mathbf{T}) \times Y(\mathbf{T}) \to \mathbb{Z}$ is defined as $(\chi, \psi) \mapsto n$.

Definition 4.1.9 *A **root system** in a real vector space V is a subset Φ with the following properties:*

(i) Φ is finite, generates V and $0 \notin \Phi$

(ii) For any $\alpha \in \Phi$, there exists $\widehat{\alpha}$ in the vector space dual to V such that $\langle \alpha, \widehat{\alpha} \rangle = 2$ and such that Φ is stable under the reflection $s_\alpha : V \to V$ defined by

$$x \mapsto x - \langle x, \widehat{\alpha} \rangle \cdot \alpha$$

(iii) $\widehat{\alpha}(\Phi) \subset \mathbb{Z}$ *for any* $\alpha \in \Phi$

The $\widehat{\alpha}$ form a root system $\widehat{\Phi}$ in the dual of V. They are called **coroots**. There exists a scalar product on V invariant by the s_α. Let us identify V with its dual. Under this identification, $\widehat{\alpha}$ becomes $\alpha/\langle \alpha, \alpha \rangle$. Note that by (ii), if α is a root, then $-\alpha$ is also a root. The root system is **reduced** if any line in V containing a root contains exactly two (opposite) roots. If Φ is the union of two orthogonal subsets then each of them is root system in the subspace of V that it generates. A root system is **irreducible**, if there is no such decomposition.

Definition 4.1.10 *The group W generated by the s_α's is called the* ***Weyl group*** *of the root system Φ.*

Definition 4.1.11 *Let Φ be a root system in V. A subset Φ^+ is called a positive system if there is $\lambda \in Y(\mathbf{T})$ with $\langle \alpha, \lambda \rangle \neq 0$ for all $\alpha \in X(\mathbf{T})$ such that*

$$\Phi^+ = \{\alpha \in \Phi | \ \langle \alpha, \lambda \rangle > 0\}.$$

Φ is disjoint union of Φ^+ and $\Phi^- := -\Phi^+$ and the elements of Φ^+ (resp. Φ^-) are called positive (resp. negative) roots. Positive roots which are indecomposable into a sum of other positive roots are called ***simple roots****. The set of simple roots is called the* ***basis*** *of Φ relative to given order*

Proposition 4.1.5 *A subset $\Delta \subset \Phi$ is a basis for some order if and only if Δ is a basis of V and every element of Φ is a linear combination of elements of Δ with integral coefficients which all have the same sign.*

Proof: See [9], Proposition 0.27. □

Proposition 4.1.6 *Let Δ_1 and Δ_2 be two bases of Φ. then there exist a unique $w \in W$ such $w(\Delta_1) = \Delta_2$.*

Proof: See [19], Proposition 9.4. □

Proposition 4.1.7 *Every positive system in Φ contains a unique basis. Conversely, any base is contained in a unique positive system.*

Proof: See [19], Proposition A.7

Definition 4.1.12 *Let W be the Weyl group of a root system Φ with a base Δ. Let Φ^+ be a positive system relative to Δ. The length of an element w is the integer $l(w) = |\{\beta \in \Phi^+|; \ w(\beta) \in \Phi^-\}|$.*

Theorem 4.1.8 *(**Structure theorem for reductive groups**) Let $\boldsymbol{G}$ be a connected reductive group and $\mathbf{T}$ be a maximal torus of $\boldsymbol{G}$.*

(i) Non-trivial minimal closed unipotent subgroups of $\boldsymbol{G}$ normalized by $\mathbf{T}$ are isomorphic to $\mathbb{G}_{\mathbf{a}}$; the conjugation action of $\boldsymbol{T}$ is mapped by this isomorphism to an action of $\mathbf{T}$ on $\mathbb{G}_{\mathbf{a}}$ of the form $x \to \alpha(t) \cdot x$, where $\alpha \in \mathbf{T}$.

*(ii) The elements $\alpha \in \mathbf{T}$ thus obtained are all distinct and non-zero and are finite in number. They form a **reduced** root system Φ in the subspace $X(\mathbf{T}) \otimes \mathbb{R}$ that they generate. The group $\mathbf{W}(\mathbf{T}) = N_{\boldsymbol{G}}(\mathbf{T})/\mathbf{T}$ is isomorphic to the Weyl group of Φ.*

(iii) The group $\boldsymbol{G}$ is generated by $\mathbf{T}$ and $\{\mathbf{U}_\alpha\}_{\alpha\in\Phi}$ where $\mathbf{U}_\alpha$ is the unipotent subgroup corresponding to α by (i) and (ii).

(iv) The Borel subgroups containing $\mathbf{T}$ correspond one to one to bases of Φ; if Φ^+ is the set of positive roots corrresponding to such a basis, the corresponding Borel subgroup is equal to $\mathbf{T}\prod_{\alpha\in\Phi^+}\mathbf{U}_\alpha$ for any order in Φ^+.

Proof: See [9], Theorem 0.31.

Definition 4.1.13 *The elements α in the Structure Theorem (ii) are called the **roots of G relative to** $\mathbf{T}$. For each $\alpha \in \Phi$ there is an isomorphism u_α of $\mathbf{G}_a$ onto a unique closed subgroup $\mathbf{U}_\alpha$ of $\mathbf{G}$ such that for any $t \in \mathbf{T}$ and $x \in \mathbb{K}^+$, $tu_\alpha(x)t^{-1} = u_\alpha(\alpha(t)x)$. The subgroup $\mathbf{U}_\alpha$ is called a **root subgroup** of $\boldsymbol{G}$.*

Corollary 4.1.9 *Let $\mathbf{U}$ be the unipotent radical of a Borel subgroup $\mathbf{B}$ of $\boldsymbol{G}$. Let Φ be a root system relative to a maximal torus $\mathbf{T}$ of $\boldsymbol{G}$ contained in $\mathbf{B}$. Let Δ be the basis corresponding to $\mathbf{B}$ with positive system Φ^+. Then $\mathbf{U} = \prod_{\alpha\in\Phi^+}\mathbf{U}_\alpha$.*

BN-pairs, parabolic subgroups, Levi subgroups

Definition 4.1.14 *Let G be a group with two subgroups B and N. Then G is a group with BN-pair if*

(i) $G = \langle B, N\rangle$;

(ii) $H = B \cap N$ is normal in N;

(iii) $N/H = W$ is generated by a set of elements s_i, $i \in I$ with $s_i^2 = 1$;

(iv) If $n_i \in N$ maps to $s_i \in W$ under the natural homomorphism $\pi : N \to W$, then $n_iBn_i \neq B$;

(v) For each $n \in N$ and each n_i we have $n_iBn \subseteq Bn_inB \cup BnB$.

The group $W = N/T$ is called **Weyl group** of the BN-pair G. The cardinality of the set I is called the **rank of** G

Definition 4.1.15 *Let G be a group with a BN-pair (B, N). This is said to be a split BN-pair of characteristic p, if the following additional hypotheses are satisfied.*

(i) $B = UT$ *with* U *is normal in* B*, and* T *a complement of* U*.*

(ii) $\bigcap_{n\in N} nBn^{-1} = T$

Theorem 4.1.10 *(Tits) Let* $\mathbf{G}$ *be a connected reductive algebraic group, and let* $\mathbf{B}$ *be a Borel subgroup and* $\mathbf{N} := N_{\mathbf{G}}(\mathbf{T})/\mathbf{T}$ *for some maximal torus* $\mathbf{T} \subset \mathbf{B}$*. Then* $(\mathbf{B}, \mathbf{N})$ *is a split BN-pair in* $\mathbf{G}$ *whose Weyl group is equal that of* $\mathbf{G}$

Proof: See [9], Theorem 1.2

Parabolic subgroups and Levi subgroups

Let G be a group with a split BN-pair. Any conjugate of B is called a **Borel subgroup** of G. A **parabolic subgroup** of G is any subgroup of G that contains a Borel subgroup.

Proposition 4.1.11 *Let W be the Weyl group of G with respect to (B, N).*

(i) W is a Coxeter group generated by reflections s_i, $i \in I$.

(ii) Let J be a subset of the index set I. Let W_J be the subgroup of W generated by the elements $s_j, j \in J$, and let N_J be the subgroup of N satisfying $N_J/H = W_J$. Then the following hold;

(a) $P_J = BN_JB$ is a subgroup of G.

(b) Any subgroup of G containing B is of the form P_J for some $J \subseteq I$.

(c) If J, K are distinct subsets of I then P_J, P_K are distinct and non-conjugate subgroups of G.

(d) For all $J \subseteq I$ we have $N_G(P_J) = P_J$.

Proof: See [9], Section 1.

Now assume that $\mathbf{G}$ is a connected reductive group, and $\mathbf{T} \leq \mathbf{G}$ is a maximal torus contained in a Borel subgroup $\mathbf{B}$ of $\mathbf{G}$. Let Φ be the root system of $\mathbf{G}$ with respect to $\mathbf{T} \leq \mathbf{B}$ and $\Delta \subset \Phi$ be a set of simple roots , $I = \{s_\alpha | \ \alpha \in \Delta\}$ the corresponding set of generating reflections of the Weyl group $\mathbf{W} = N_{\mathbf{G}}(\mathbf{T})/\mathbf{T}$. By $\mathbf{W_J}$ we denote the subgroup of $\mathbf{W}$ generated by J. For $J \subset I$ define $\Delta_J = \{s_\alpha | \ \alpha \in \Delta_J\}$ and

$$\Phi_J = \Phi \cap \sum_{\alpha\in\Delta_J} \mathbb{Z}\alpha$$

Proposition 4.1.12 *Let $J \subset I$. Let $\dot{w}$ be a representative of $w \in W$ in $N_{\boldsymbol{G}}(\mathbf{T})$.*

(i) Then Φ_J is a root system in $\mathbb{R}\Phi_J$ with base Δ_J and Weyl group W_J.

(ii) $P_J := BW_JB = \cup_{w \in W_J} B\dot{w}B$ is a closed connected subgroup of $\boldsymbol{G}$

(iii) $P_J = \langle T, U_\alpha | \quad \alpha \in \Phi^+ \cup \Phi_J \rangle$

Moreover all subgroups of $\boldsymbol{G}$ containing $\mathbf{B}$ arise in this way.

Proof: See [19], Proposition 12.2. □

Definition 4.1.16 *Let $\mathbf{P} \leq \mathbf{G}$ be a parabolic subgroup. Then there are subgroups $\mathbf{U_P}$ and $\mathbf{L}$ of $\mathbf{P}$ such that*

$$\mathbf{P} = \mathbf{U_P}\mathbf{L} = \mathbf{L}\mathbf{U_P}$$

*The group $\mathbf{U_P}$ is the largest normal unipotent subgroup of $\mathbf{P}$ and is called **unipotent radical** of $\mathbf{P}$, and $\mathbf{L}$ is a complement to $\mathbf{U_P}$ in $\mathbf{P}$. The decomposition is called a Levi decomposition of $\mathbf{P}$, and $\mathbf{L}$ is denoted by a **Levi complement** of $\mathbf{G}$. It is well known that any two Levi complements of $\mathbf{P}$ are conjugate by unique element $u \in \mathbf{U}$. Note that $R_u(\mathbf{P}) = \mathbf{U_P}$.*

The following Theorem gives the structures of parabolic subgroups and the structure of their Levi complements.

Theorem 4.1.13 *Let $\mathbf{P}$ be a parabolic subgroup of $\boldsymbol{G}$ containing the Borel subgroup $\mathbf{B}$ and of the form $\mathbf{BW}_J\mathbf{B}$. Let $\Phi^+ \subset \Phi$ be a positive system in the root system Φ of $\boldsymbol{G}$ with respect to a maximal torus $\mathbf{T}$ contained in $\mathbf{B}$. Then*

(i) $\mathbf{U_P} = \prod_{\alpha \in \Phi^+ \setminus \Phi_J} \mathbf{U}_\alpha$.

(ii) $\mathbf{L}_J = \langle \mathbf{T}, \mathbf{U}_\alpha | \quad \alpha \in \Phi_J \rangle$.

Proof: See [19], Proposition 12.6. □

Proposition 4.1.14 *(i) Let $\mathbf{P}$ be a parabolic subgroup of $\boldsymbol{G}$ and $\mathbf{T}$ be a maximal torus of $\mathbf{P}$. There exist a unique Levi subgroup of $\mathbf{P}$ containing $\mathbf{T}$.*

(ii) Two Levi subgroups of a parabolic subgroup $\mathbf{P}$ are conjugate by a unique element of $R_u(\mathbf{P})$

Proof: See [9], Proposition 1.17, and Proposition 1.18.

4.2. Finite Groups of Lie Type

Frobenius maps and finite reductive groups

Let $\mathbf{G} \leq GL_n(\overline{\mathbb{F}}_p)$ be a connected reductive algebraic group. A **Frobenius map** $\mathbf{F} : \mathbf{G} \longrightarrow \mathbf{G}$ is an endomorphism such that $\mathbf{F}^m$ is a homomorphism of $\mathbf{G}$ of the form $\mathbf{F}^m : \mathbf{G} \longrightarrow \mathbf{G}$, $\mathbf{F}^m((a_{ij})) = (a_{ij}^q)$ where q is a power of p and $m \geq 1$. Here $\mathbf{F}^m$ denotes the compositions of $\mathbf{F}$ m times. Let $\mathbf{G}$ be a connected reductive algebraic group over $\overline{\mathbb{F}}_q$, and let $\mathbf{F}$ be a Frobenius map of $\mathbf{G}$. Then

$$\mathbf{G}^{\mathbf{F}} = \{g \in \mathbf{G} |\ \ \mathbf{F}(g) = g\}$$

is a finite group.

Example 4.2.3 *Let q be a power of p and let $\mathbf{F} = F_q$ be the corresponding standard Frobenius map of $\mathbf{GL}_n(\overline{\mathbb{F}}_q)$. Then $GL_n(\overline{\mathbb{F}}_p)^{\mathbf{F}} = GL_n(q)$, $\mathbf{SL}_n(\overline{\mathbb{F}}_q)^{\mathbf{F}} = SL_n(q)$, and $\mathbf{SO}_{2m+1}(\overline{\mathbb{F}}_q)^{\mathbf{F}} = SO_{2m+1}(q)$.*

Definition 4.2.17 *Let $\boldsymbol{G}$ be a connected reductive group, $\mathbf{F} : \boldsymbol{G} \to \boldsymbol{G}$ a Frobenius map. Then the finite group of fixed points $\boldsymbol{G}^{\mathbf{F}}$ is called a **finite group of Lie type**.*

The theorem of Lang-Steinberg

The crucial tool transferring results from algebraic groups $\mathbf{G}$ to finite groups $\mathbf{G}^{\mathbf{F}}$ of fixed points under a Frobenius map $\mathbf{F}$ is the theorem of Lang-Steinberg.

Theorem 4.2.15 *(Lang-Steinberg Theorem) Let $\boldsymbol{G}$ be a connected linear algebraic group over $\overline{\mathbb{F}}_q$ with a Frobenius map $\mathbf{F} : \boldsymbol{G} \to \boldsymbol{G}$. Then the morphism*

$$\mathbf{L} : \boldsymbol{G} \to \boldsymbol{G}, \quad g \to \mathbf{F}(g)g^{-1}$$

is surjective.

Proof: See [24], Theorem 10.1. □

One of important consequence of Lang Steinberg Theorem is that $\mathbf{G}$ has a $\mathbf{F}$-rational Borel subgroup. Before stating another important consequence of Lang-Steinberg Theorem, we need the following definition.

Definition 4.2.18 *Let H be a group, σ an automorphism of H. We say that h_1, h_2 are σ-conjugate if there exist an $x \in H$ with $h_2 = (x)h_1\sigma(x)^{-1}$. The equivalence classes for this relation are called **σ-conjugacy classes** of H.*

Proposition 4.2.16 *Let* $\mathbf{H}$ *be closed connected rational subgroup of* $\boldsymbol{G}$*, then*

(i) $(\boldsymbol{G}/\mathbf{H})^{\mathbf{F}} = \boldsymbol{G}^{\mathbf{F}}/\mathbf{H}^{\mathbf{F}}$

(ii) Assume that $\mathbf{H}$ *is normal.Then there is a bijection between the set of* $\boldsymbol{G}^{\mathbf{F}}$*-conjugacy classes in* $\mathbf{H}$ *and* $\mathbf{F}$*- conjugacy classes of* $\mathbf{G}/\mathbf{H}$*.*

Proof: , See [9], for (i) Corollary 3.13, for (ii) Lemma 3.22. □

If $\mathbf{H}$ is a connected closed subgroup of $\mathbf{G}$ and $\mathbf{V}$ is the set of $\mathbf{F}$-stable conjugates of $\mathbf{H}$ in $\mathbf{G}$, then $\mathbf{G}$ acts on $\mathbf{V}$ transitively, and this action is clearly a compatible $\mathbf{F}$-action. Thus we have the following corollaries.

Corollary 4.2.17 *Let* $\boldsymbol{G}$ *and* $\mathbf{F}$ *be as above. The set of* $\mathbf{G}^{\mathbf{F}}$*- conjugacy classes of rational maximal tori is parametrized by the set of* $\mathbf{F}$*-conjugacy classes in* $\mathbf{W}$*.*

Corollary 4.2.18 *Let* $\mathbf{P}$ *be a* $\mathbf{F}$*-stable parabolic subgroup of* $\boldsymbol{G}$*. There is unique* $\mathbf{G}^{\mathbf{F}}$*-conjugacy class of conjugates of* $\mathbf{P}$*.*

Proof: We know that $N_{\mathbf{G}}(\mathbf{P}) = \mathbf{P}$. Applying Theorem **??** to the set $\mathbf{V}$ of all conjugate of P with the action of $\mathbf{G}$, we see that $\mathbf{G}_{\mathbf{P}} = \mathbf{P}$. Since $\mathbf{P}$ is connected, $\mathbf{P}^0 = \mathbf{P}$; and the result follows.
Let $\mathbf{G}$ and $\mathbf{F}$ be as above and $\mathbf{B}$ a Borel subgroup and let $\mathbf{T}$ be a maximal torus contained in $\mathbf{B}$. Since $\mathbf{T}$ is rational then $N_{\mathbf{G}}(\mathbf{T})$ is also rational. Hence $\mathbf{F}$ also acts on $\mathbf{W}$ by sending $n\mathbf{T}$ to $\mathbf{F}(n)\mathbf{T}$. Let Φ^+ be the positive system of roots in Φ that correspond to $\mathbf{B}$, i.e $\mathbf{B} = \mathbf{T}\prod_{\alpha\in\Phi^+}\mathbf{U}_\alpha$. Since $\mathbf{B}$ is $\mathbf{F}$-stable, $\mathbf{F}$ permutes the root subgroups $\mathbf{U}_\alpha$ of $\mathbf{B}$. Thus $\mathbf{F}$ permutes Φ^+. Recall that Φ^+ is the set of linear combinations of the elements in a simple system $\Delta \subset \Phi$ with positive coefficients. So $\mathbf{F}$ fixes Δ.

$\mathbf{F}$ acts on both the character group and cocharacter group $X(\mathbf{T})$ and $Y(\mathbf{T})$ of $\mathbf{T}$. These actions are defined as follows:

$$\mathbf{F}(\chi)(t) = \chi(\mathbf{F}(t)) \text{ for } \chi \in X(\mathbf{T}), t \in \mathbf{T}$$
$$\mathbf{F}(\gamma(c)) = \mathbf{F}(\gamma(c)) \text{ for } \gamma \in Y(\mathbf{T}), c \in \overline{\mathbb{F}}_q^{\times}$$

Write $\Phi \subset X(\mathbf{T})$ for the root system of $\mathbf{G}$, with positive system Φ^+ with respect to $\mathbf{T}$ and $\mathbf{B}$. For $\alpha \in \Phi$ lets choose isomorphisms $u_\alpha : \mathbf{G}_a \to U_\alpha$ onto the root subgroups. We set $\mathbf{X}_{\mathbb{R}} := X(\mathbf{T}) \otimes_{\mathbb{Z}} \mathbb{R}$.

Proposition 4.2.19 *Let* $\mathbf{G}$ *be a connected reductive algebraic group with Frobenius endomorphism* $\mathbf{F} : \mathbf{G} \to \mathbf{G}$*, and* $\mathbf{T}, \mathbf{B}, X(\mathbf{T}), \Phi$ *as above.*

- *(a) There exists a permutation ρ of Φ^+ and, for each $\alpha \in \Phi^+$, a positive integral power q_α of p and $a_\alpha \in \overline{\mathbb{F}}_p^\times$ such that $\mathbf{F}(\rho(\alpha)) = q_\alpha \alpha$ and $\mathbf{F}(u_\alpha(c)) = u_{\rho(\alpha)}(a_\alpha c_\alpha^q)$ for all $\in \overline{\mathbb{F}}_p$*

- *(b) There exists $\delta \geq 1$ such that $\mathbf{F}^\delta|_{X(\mathbf{T})} = q^\delta id$ and $\mathbf{F} = q\phi$ on $\mathbf{X}_\mathbb{R}$ for some positive fractional power q of p and some $\phi \in Aut(\mathbf{X}_\mathbb{R})$ of order δ inducing ρ^{-1} on Φ^+.*

Proof: See [19] Proposition 22.2.

BN-pair of $\mathbf{G^F}$

Theorem 4.2.20 *Let $\boldsymbol{G}$ be a connected reductive group with Frobenius map $\mathbf{F}:\boldsymbol{G}\to\boldsymbol{G}$ and let $\mathbf{T}$ be an $\mathbf{F}$-stable maximal torus in an $\mathbf{F}$-stable Borel subgroup of $\boldsymbol{G}$, with normalizer $\mathbf{N}:=N_{\boldsymbol{G}}(\mathbf{T})$. Then $\mathbf{B^F}$, $\mathbf{N^F}$ is a BN-pair in $\boldsymbol{G}^{\mathbf{F}}$ whose Weyl group is isomorphic to $\mathbf{W^F}$.*

Proof: See [19], Theorem 24.10.
Centralizer of semisimple elements

Definition 4.2.19

Let $\mathbf{G}$ be a connected reductive group. Let s be a semisimple element of $\mathbf{G}$. Since every semisimple element lies in a maximal torus of $\mathbf{G}$, there is a maximal torus $\mathbf{T}$ of $\mathbf{G}$ containing s. Since $\mathbf{T}$ is abelian, $\mathbf{T}\subseteq C_{\mathbf{G}}(s)$.

Theorem 4.2.21 *Let s be a semisimple element of $\boldsymbol{G}$ contained in a maximal torus $\mathbf{T}$. Let Φ be a root system of $\boldsymbol{G}$ relative to $\mathbf{T}$. Then $C_{\boldsymbol{G}}(s)$ is reductive. Its connected component $C_{\boldsymbol{G}}(s)^0$ is generated by $\mathbf{T}$ together with $\mathbf{U}_\alpha$, $\alpha\in\Phi$ for which $\alpha(s)=1$.*

Proof: See [9], Proposition 2.3

Let Φ the be root system of $\mathbf{G}$ with respect to the maximal torus $\mathbf{T}$.

Definition 4.2.20 *A subset $\Psi\subset\Phi$ is said to be closed if whenever $\alpha,\beta\in\Psi$ and n,m are positive integers such that $n\alpha+m\beta$ is a root, then $n\alpha+m\beta\in\Psi$. A subset $\Psi\subset\Phi$ is called symmetric if α in Ψ then $-\alpha$ in Ψ*

Proposition 4.2.22 *The connected reductive subgroups of $\boldsymbol{G}$ which contain $\mathbf{T}$ are $\boldsymbol{G}_\Psi=\langle\mathbf{T},\mathbf{U}_\alpha|\ \alpha\in\Psi\rangle$, where Ψ is a closed and symmetric subset of Φ.*

Remark 4.2.1 *Since Φ is a finite set, its closed and symmetric subsets are also finite. Recall that for a basis $\Delta\subset\Phi$ its subset Δ' gives a closed and symmetric subset of Φ. Indeed they are corresponding to Levi complement of some parabolic subgroups of $\boldsymbol{G}$. Hence we conclude that almost all of* ***centralizers of semisimple elements are Levi subgroups of $\boldsymbol{G}$****.*

Bibliography

[1] S.S.Abhyankar, *Projective polynomials*, Proc. Amer. Math. Society, **125**, Number 6, (1997), 1643-1650

[2] A. Bluher, *On the polynomial $x^{q+1}+ax^q+b$*, Finite Fields and Their Applications (**3**), (10), (2004), 285305

[3] P. J. Cameron, H. R. Maimani, G. R. Omidi and B. Tayfeh-Rezaie, *3-Designs from $PGL_2(q)$*, The Electronic Journal Of Combinatorics 13 (2006), R50

[4] R. Carter, *Centralizers of semisimple elements in finite groups of Lie type* Proc. London Math. Soc. (**3**) 37 (1978) 491-507

[5] R. Carter, *Centralizers of semisimple elements in finite classical groups*, Proc. London Math. Soc. (**3**) 42 (1981) 1-41

[6] R. Carter, *Finite groups of Lie type*, John WileysSons, New York, 1993.

[7] D. I. Deriziotis, *Centralizers of semisimple elements in Chevalley groups*, Comm. Algebra, **9** (1981), 1997-2014

[8] D. I. Deriziotis, *The centralizers of semisimple elements in the Chevalley groups E_7 and E_8*, Tokyo J. of Math., **6**(1983), 191-216

[9] F. Digne, J. Michel, *Representations of Finite Groups of Lie type*, Lon. Math. Society, Student Texts **21** (1991)

[10] J. Humphreys, *Conjugacy classses in semisimple algebraic groups*, American Math. Soc. Mathematical surveys and Monographs, Vol: **43** (1995)

[11] A. Dold, B. Eckmann *Seminar on algebraic Groups and Related Finite Groups* Springer-Verlag, Lecture notes in Mathematics **131** (1986)

[12] J. Humphreys,*Introduction to Lie algebras and representation Theory* Springer, (1997)

[13] J. Humphreys, *Linear algebraic groups*, Springer-Verlag, 2^{nd} Edition, Graduate Texts in Mathematics, **21**, (1998).

[14] J. Humphreys, *Reflection groups and Coxeter groups*, Cambridge University Press, Cambridge Studies in Advanced Mathematics, **29**, (2000)

[15] D. Gorenstein, R. Lyons, R. Solomon, *The classification of the finite simple groups*, Mathematical surveys and monographs Volume 40, **3** (1998)

[16] R. Guralnick, *Polynomials with PSL(2) monodromy*, *Annal of math.* **172** (2010), Pages 1315-1359

[17] Michael J. Klass, *A generalization of Burnside's combinatorial lemma*, J. Combinatorial Theory, Series A Volume **20**, Issue 3 , (1976), Pages 273278

[18] M. Konvalinka; G. Pfeiffer; C.E Rover, *A note on element centralizers in finite Coxeter groups*, J. Of Group Theory, Volume **14**, (5), (2011), 727-746

[19] G. Malle, D. Testerman, *Linear algebraic groups and finite groups of Lie type*, Cambridge university Press, Cambridge studies in advanced math. No:133 (2011)

[20] N. Spaltenstein, *On unipotent and nilpotent elements of groups of type* E_6, J. London Math. Soc. (2) **27** (1983), 413-420.

[21] M. Rosen, *Number theory in function fields* Springer-Verlag, Graduate Texts in Mathematics No:**221**, (2002).

[22] Rotman, Joseph, *An introduction to the theory of groups*, Springer-Verlag (1995)

[23] T. A. Springer, *Linear algebraic groups*, Modern Birkhauser Classics, 2$^{\text{nd}}$ printing, (2008).

[24] J. Steinberg, *Endomorphisms of linear algebraic groups* , Mem. Amer. Math. Soc. **80** (1968) 22.

[25] H. Stichtenoth, *Algebraic function fields and codes*, 2$^{\text{nd}}$ Edition, Springer-Verlag, Graduate Texts in Mathematics No. **254** (2009).

[26] R. C. Valantini, M. L. Madan, *A Hauptsatz of L.E Dickson and Artin-Schreier extensions*, J. Reine Angew. Math, **318**, 156-177.