ΕΥΡΕΣΗ ΣΤΟΙΧΕΙΩΝ ΜΕΓΑΛΗΣ ΤΑΞΗΣ ΣΕ ΠΕΠΕΡΑΣΜΕΝΑ ΣΩΜΑΤΑ

Κωνσταντινος Νικηφορος

Επιβλεπων Καθηγητης
Θεοδουλος Γαρεφαλακης

Μεταπτυχιακη Εργασια
Μαρτιος 2019

Τμημα Μαθηματικων και Εφαρμοσμενων Μαθηματικων
Πανεπιστημιο Κρητης

Στην οικογένειά μου
και τους φίλους μου.

Η παρούσα μεταπτυχιακή εργασία κατατέθηκε τον Μάρτιο του 2019 στο Πανεπιστήμιο Κρήτης. Την επιτροπή αξιολόγησής της αποτέλεσαν, εκτός του επιβλέποντα καθηγητή κ. Θεόδουλου Γαρεφαλάκη, οι κ. Κουβιδάκης Αλέξανδρος και κα. Λουκάκη Μαρία.

Ευχαριστίες

Η παρούσα εργασία αποτελεί διπλωματική εργασία στα πλαίσια του μεταπτυχιακού προγράμματος Μαθηματικά της Πληροφορικής του τμήματος Μαθηματικών και Εφαρμοσμένων Μαθηματικών του Πανεπιστημίου Κρήτης.

Πριν την παρουσίαση της εργασίας, θα ήθελα να ευχαριστήσω τους ανθρώπους με τους οποίους συνεργάστηκα και όλους όσους βοήθησαν για την πραγματοποίησή της.

Πρώτα, θα ήθελα να ευχαριστήσω τον επιβλέποντά μου, κ. Θεόδουλο Γαρεφαλάκη, ο οποίος ήταν πάντα πρόθυμος να επιλύσει οποιαδήποτε απορία μου και να με καθοδηγήσει όταν το χρειαζόμουν.

Επίσης, θα ήθελα να ευχαριστήσω και την υπόλοιπη επιτροπή αξιολόγησης, την οποία αποτέλεσαν ο κ. Αλέξανδρος Κουβιδάκης και η κα. Μαρία Λουκάκη.

Σε αυτό το σημείο, θα ήθελα να ευχαριστήσω και όσους καθηγητές αποτέλεσαν πηγή έμπνευσης για μένα, μερικοί εκ των οποίων είναι ο κ. Αθανάσιος Φειδάς, ο κ. Θεόδουλος Γαρεφαλάκης, ο κ. Ιωάννης Αντωνιάδης και η κα. Μαρία Λουκάκη.

Ακόμα, νιώθω την ανάγκη να ευχαριστήσω την οικογένειά μου που με στήριξε σε όλη μου την προσπάθεια.

Το ταξίδι αυτό, δεν θα μπορούσε να γίνει ευχάριστο και όμορφο χωρίς την παρουσία της Γιούλης και του Ιωσήφ.

Τέλος, θα ήθελα να εκφράσω τις αληθινές μου ευχαριστίες στον Μάνο για την ενθάρρυνση και τη στήριξη που μου παρείχε.

Περιεχόμενα

1 Εισαγωγή **6**

2 Συνδυαστικές Εκτιμήσεις **8**
2.1 Ανισότητες 8
2.2 Το Σύνολο $I_{s,t,m}$ 10

3 Εύρεση Στοιχείου Μεγάλης Τάξης της Επέκτασης Artin - Schreier **13**
3.1 Αναγωγισιμότητα Πολυωνύμων 13
3.2 Το Πεπερασμένο Σώμα $\mathbb{F}_q[X]/(X^p - X - 1)$ 14
3.3 Ένα Ισχυρό Φράγμα της Τάξης της Ομάδας $\langle\theta\rangle$ 19

4 Εύρεση Στοιχείου Μεγάλης Τάξης Μέσω Generic Root **24**
4.1 Η Ομάδα $\mathrm{PGL}_2(\mathbb{F}_q)$ 24
4.2 Ιδιότητες του A^n 26
4.3 Ένα Ισχυρό Φράγμα της Τάξης των Generic Root 29

Συμβολισμός

$\mathbb{N}, \mathbb{Z}, \mathbb{Z}_D, \mathbb{C}$	οι φυσικοί, οι ακέραιοι, οι ακέραιοι modulo D, οι μιγαδικοί
$\|A\|$	ο πληθάριθμος του συνόλου A
$a \mid b$	a διαιρεί το b
$\varphi(n)$	η τιμή της συνάρτησης του *Euler* για τον φυσικό n
$\mu\kappa\delta(a, b)$	ο μέγιστος κοινός διαιρέτης των a και b
$\deg(f)$	ο βαθμός του πολυωνύμου f
$\ker(f)$	ο πυρήνας της απεικόνισης f
$[X]$	το σύμπλοκο του X
$\mathbb{F}_q$	το πεπερασμένο σώμα με q στοιχεία
$\mathbb{F}_q^*$	το $\mathbb{F}_q$ χωρίς το μηδέν
$\overline{\mathbb{F}_q}$	η αλγεβρική κλειστότητα του $\mathbb{F}_q$
$\mathbb{F}_q[X]$	τα πολυώνυμα του X με συντελεστές στο σώμα $\mathbb{F}_q$
M/K	επέκταση σωμάτων
$[M : K]$	ο βαθμός της επέκτασης σωμάτων
$\dim_K(M)$	η διάσταση του M ως διανυσματικού χώρου πάνω από το K
$\mathrm{Tr}_{M/K}(a)$	το ίχνος του a στην επέκταση M/K
$\mathrm{ord}(M)$	η τάξη του πεπερασμένου σώματος M
$\mathbb{K}^{(n)}$	το n-οστό κυκλοτομικό σώμα
Φ_n	το κυκλοτομικό πολυώνυμο
$[A], [I]$	τον πίνακα A, τον μοναδιαίο πίνακα I
$\det(A)$	η ορίζουσα του πίνακα A
PGL_2	η projective general linear group

Για τη συγκεκριμένη εργασία, με p θα συμβολίζουμε έναν πρώτο αριθμό διαφορετικό του δύο και με q μία δύναμη πρώτου.

Abstract

The purpose of this master thesis is to find elements of high order in certain extensions of finite fields. We work on two cases. At first, we find such elements in Artin-Schreier extension and then we find such elements using generic roots of certain polynomials. In both cases, our goal is to find a strong lower bound of some elements' order. To do this, we compare the order of that elements with the cardinal number of some sets and we have the desired results.

Περίληψη

Σκοπός της παρούσας εργασίας είναι να βρούμε στοιχεία συγκεκριμένων επεκτάσεων πεπερασμένων σωμάτων που έχουν 'αρκετά μεγάλη' τάξη. Εργαζόμαστε για δύο περιπτώσεις. Αρχικά, βρίσκουμε στοιχεία μεγάλης τάξης στην επέκταση Artin-Schreier και στη συνέχεια βρίσκουμε στοιχεία μεγάλης τάξης μέσω των generic root συγκεκριμένων πολυωνύμων. Και στις δύο περιπτώσεις, στόχος μας είναι να φράξουμε από κάτω την τάξη κάποιων στοιχείων από ένα κατάλληλα μεγάλο αριθμό. Για να γίνει αυτό, συγκρίνουμε την τάξη των στοιχείων αυτών με κάποιους πληθαρίθμους συνόλων και παρουσιάζουμε το επιθυμητό αποτέλεσμα.

Κεφάλαιο 1

Εισαγωγή

Έστω $\mathbb{F}_q$ το σώμα με q στοιχεία, όπου το q είναι μια δύναμη ενός πρώτου p. Δοθέντος ενός φυσικού αριθμού n, είναι φυσικό να αναρωτηθούμε πώς μπορούμε να βρούμε στοιχεία μεγάλης τάξης στην πολλαπλασιαστική ομάδα $(\mathbb{F}_{q^n})^*$ ή με άλλα λόγια στην $\left(\mathbb{F}_q[X]/f(X)\right)^*$, όπου το $f(X)$ είναι ένα ανάγωγο πολυώνυμο βαθμού n, υπέρ το $\mathbb{F}_q$. Ιδανικά, θα επιθυμούσαμε να μπορούμε να βρίσκουμε γεννήτορες της παραπάνω ομάδας, όμως είναι γνωστό ότι αυτό είναι ένα δύσκολο υπολογιστικό πρόβλημα. Συγκεκριμένα, και μόνο για να πιστοποιήσουμε ότι ένα στοιχείο είναι γεννήτορας, πρέπει να γνωρίζουμε την παραγοντοποίηση του $q^n - 1$ ή να επιλύσουμε το πρόβλημα του διακριτού λογαρίθμου στο $\mathbb{F}_{q^n}$. Με όσα γνωρίζουμε μέχρι τώρα, τα παραπάνω προβλήματα είναι 'δύσκολα' και σε αυτά στηρίζεται η μοντέρνα κρυπτογραφία. Όμως, το να βρίσκουμε στοιχεία μεγάλης τάξης έχει επίσης πολλές σημαντικές εφαρμογές. Τέτοια στοιχεία χρησιμοποιούνται, για παράδειγμα, στον αλγόριθμο AKS [1] με σκοπό να ελέγξουμε εάν ένας αριθμός είναι πρώτος ή σύνθετος σε πολυωνυμικό χρόνο. Έχουν γίνει πολλές προσπάθειες με στόχο την εύρεση τέτοιων στοιχείων. Οι βασικές μέθοδοι που χρησιμοποιούνται είναι δύο ειδών, οι οποίες είναι οι μέθοδοι εύρεσης ενός μικρού υποσυνόλου του $\mathbb{F}_{q^n}$ με τουλάχιστον έναν γεννήτορα ή οι μέθοδοι εύρεσης στοιχείου του $\mathbb{F}_{q^n}$ με εγγυημένα μεγάλη τάξη (συνήθως μέσω ενός μεγάλου κάτω φράγματος της τάξης). Μερικά παραδείγματα από μεθόδους του πρώτου είδους είναι τα εξής:
Στο [18], υποθέτοντας την επεκτεταμένη υπόθεση του Riemann (ERH), ο Shoup παρουσιάζει ένα ντετερμινιστικό, πολυωνυμικού χρόνου αλγόριθμο, ο οποίος βρίσκει έναν γεννήτορα του $\mathbb{F}_{p^2}$, ενώ ο Bach στο [3] παρουσιάζει έναν αλγόριθμο, ο οποίος βρίσκει ένα σύνολο με $O((\log p)^4/(\log\log p)^3)$ στοιχεία, το οποίο περιέχει τουλάχιστον έναν γεννήτορα του $\mathbb{F}_p^*$. Στο [5], ο Gao κατασκευάζει έναν αλγόριθμο, ο οποίος βρίσκει στοιχεία μεγάλης τάξης σχεδόν για κάθε επέκταση $\mathbb{F}_{q^n}$ του $\mathbb{F}_q$, με τάξη που φράσσεται κάτω από μία συνάρτηση της μορφής $c(p)\frac{\log^2\log q}{\log\log\log q}$, όπου η $c(p)$ εξαρτάται μόνο από τη χαρακτηριστική του σώματος. Επίσης, ο Cheng στο [4] δείχνει πώς

μπορούμε να βρούμε, δοθέντων q, N, και ενός ακέραιου $n \in [N, 2qN]$, ένα στοιχείο $\theta \in \mathbb{F}_{q^n}$ με τάξη μεγαλύτερη από $5.8^{n \log q / \log n}$. Στην παρούσα εργασία, θα ασχοληθούμε με μεθόδους του δεύτερου είδους. Μερικά άλλα γνωστά αποτελέσματα είναι τα εξής:
Στα [12] και [13], ο Popovych δουλεύοντας στην περίπτωση, όπου $f(X) = \Phi_r(X)$, το r-οστό κυκλοτομικό πολυώνυμο, και $g(X) = X^n - a$ είναι ανάγωγα πολυώνυμα στο $\mathbb{F}_q[X]$ βρίσκει ένα κάτω φράγμα για την τάξη του $\langle \theta + c \rangle$, όπου θ είναι μια ρίζα του $f(X)$. Επίσης, στο [2], οι Ahmadi, Shparilinski και Voloch, έδειξαν ότι εάν $\theta \in \mathbb{F}_{q^{2n}}$ είναι μια πρωταρχική r-οστή ρίζα της μονάδας, όπου $r = 2n + 1$ είναι πρώτος, τότε η περίοδος Gauss $\alpha = \theta + \theta^{-1}$ έχει τάξη μεγαλύτερη από $\exp\left(\left(\pi\sqrt{\frac{2(p-1)}{3p}} + o(1)\right)\sqrt{n}\right)$, όπου p είναι η χαρακτηριστική του σώματος (άλλα αποτελέσματα για την τάξη της περιόδου Gauss βρίσκονται στα [7] και [8]). Επιπλέον, ο Popovych στα [12] και [14] βελτίωσε το προηγούμενο φράγμα δίνοντας ένα κάτω φράγμα για στοιχεία πιο γενικών μορφών, $\theta^e(\theta^f + a), (\theta^{-f} + a)(\theta^f + a)$ και $\theta^{-2e}(\theta^{-f} + a)(\theta^f + a)^{-1}$, όπου $a \in \mathbb{F}_q^*$. Συγκεκριμένα, απέδειξε ότι η πολλαπλασιαστική τάξη της περιόδου Gauss δεν είναι μικρότερη από $5^{\sqrt{(r-2)/2}-2}$, για κάθε $p \geq 5$ ($r = 2n + 1$). Τέλος, ο Popovych στο [15] δουλεύοντας στην επέκταση Artin-Schreier $\mathbb{F}_{p^p}$ του σώματος $\mathbb{F}_p$ βρίσκει ένα στοιχείο τάξης μεγαλύτερης από 4^p χρησιμοποιώντας στοιχειώδεις μεθόδους. Το παραπάνω αποτέλεσμα είναι ασθενέστερο από αυτό του Voloch στο [20], όπου ισχυρίζεται ότι η τάξη οποιασδήποτε ρίζας του $X^p - X - 1$ στο $\mathbb{F}_{p^p}$ ξεπερνάει το $2^{2.54p} \sim 5.81589^p$. Το άρθρο που δημοσίευσε δεν περιέχει την απόδειξη, όμως με χρήση του Sage Mathematics Software, πιστοποιείται ότι ο ισχυρισμός είναι αληθής μόνο όταν $p > 4647$.

Κεφάλαιο 2

Συνδυαστικές Εκτιμήσεις

2.1 Ανισότητες

Στην παρούσα ενότητα, θα παρουσιάσουμε μερικές ανισότητες, τις οποίες θα χρησιμοποιήσουμε για να φράξουμε από κάτω την τάξη στοιχείων πεπερασμένων σωμάτων.

Λήμμα 2.1.1. $\sum_{k=0}^{n} \binom{a+k}{a} = \binom{a+n+1}{a+1}$, *για* $n, a \in \mathbb{N}$.

Απόδειξη. Η απόδειξη θα γίνει με επαγωγή στο n.
Για $n = 1$, $\binom{a+0}{a} + \binom{a+1}{a} = 1 + (a+1) = a + 2 = \binom{a+1+1}{a+1}$.
Έστω, ότι ισχύει για $n = m$, δηλαδή ότι $\sum_{k=0}^{m} \binom{a+k}{a} = \binom{a+m+1}{a+1}$.
Θα το αποδείξουμε για $n = m + 1$.
$\sum_{k=0}^{m+1} \binom{a+k}{a} = \binom{a+m+1}{a+1} + \binom{a+m+1}{a} = \frac{(a+m+1)!}{(a+1)!(m+1)!}((m+1)+(a+1)) = \frac{(a+m+2)!}{(a+1)!(m+1)!} = \binom{a+m+2}{a+1}$. □

Πρόταση 2.1.2. *Το πλήθος των θετικών, ακέραιων λύσεων της ανισότητας* $x_1 + x_2 + \cdots + x_i \leq s$ *είναι* $\binom{s}{i}$, *όταν* $s \geq i$.

Απόδειξη. Προφανώς, αν $s < i$ η παραπάνω ανισότητα δεν έχει θετικές, ακέραιες λύσεις. Αν τώρα $s \geq i$, για να έχουμε θετικά $x_j, j = 1, \ldots, i$ αρχικά θεωρούμε ότι κάθε x_j είναι τουλάχιστον 1 και περισσεύουν ακόμα $s - i$ μονάδες. Το ζητούμενο πλήθος είναι το άθροισμα των μη αρνητικών, ακέραιων λύσεων των εξισώσεων
$x_1 + x_2 + \cdots + x_i = k$, για $k = 0, \ldots, s - i$.
Δηλαδή, $\sum_{k=0}^{s-i} \binom{i-1+k}{i-1} \overset{2.1.1}{=} \binom{i-1+s-i+1}{i-1+1} = \binom{s}{i}$. □

Πρόταση 2.1.3. ***Ταυτότητα Chu-Vandermonde***
$\sum_{j=0}^{k} \binom{m}{j}\binom{n}{k-j} = \binom{m+n}{k}$, *για* $m, n \in \mathbb{N}$ *και* $k \in \mathbb{N}_0$.

Απόδειξη. Έστω ότι έχουμε m άντρες και n γυναίκες. Θα μετρήσουμε με δύο τρόπους το εξής: με πόσους τρόπους μπορούμε να επιλέξουμε k από αυτούς.
Πρώτος Τρόπος: από τα $m+n$ άτομα επιλέγουμε k, με $\binom{m+n}{k}$ τρόπους.
Δεύτερος Τρόπος: από τους m άντρες επιλέγουμε $j, j \in \{0,1,\ldots,k\}$ και από τις n γυναίκες επιλέγουμε $k-j$, δηλαδή με $\sum_{j=0}^{k}\binom{m}{j}\binom{n}{k-j}$ τρόπους. □

Πρόταση 2.1.4. *Έστω $D \geq 2$ και $r \geq 3$. Τότε*

$$\binom{D^{\frac{r+2}{4}}}{D} \geq \sqrt{\frac{\frac{r+2}{4}}{2\pi\frac{r-2}{4}}}\left(\frac{\left(\frac{r+2}{4}\right)^{\frac{r+2}{4}}}{\left(\frac{r-2}{4}\right)^{\frac{r-2}{4}}}\right)^{D}\frac{1}{\sqrt{D}}e^{-\frac{1}{12D}(1+\frac{16}{r^2-4})}.$$

Απόδειξη. Η απόδειξη βρίσκεται στην πρόταση 1 του [17]. □

Πρόταση 2.1.5. ***Ανισότητα Stirling***

$$\sqrt{2\pi}n^{n+\frac{1}{2}}e^{-n}e^{\frac{1}{12n+1}} < n! < \sqrt{2\pi}n^{n+\frac{1}{2}}e^{-n}e^{\frac{1}{12n}}, n \in \mathbb{N}.$$

Απόδειξη. Η απόδειξη της συγκεκριμένης παραλλαγής της ανισότητας του Stirling βρίσκεται στο [16]. □

Πρόταση 2.1.6. *Έστω $D \geq 2$. Τότε $\binom{2D}{D} \geq \frac{4^D}{\sqrt{\pi D}}e^{-\frac{1}{8D}-\frac{1}{144D^2}}$.*

Απόδειξη. Έστω $D \geq 2$.

$$\binom{2D}{D} = \frac{(2D)!}{(D!)^2} \overset{2.1.5}{>} \frac{\sqrt{2\pi}(2D)^{2D+\frac{1}{2}}e^{-2D}e^{\frac{1}{24D+1}}}{(\sqrt{2\pi}D^{D+\frac{1}{2}}e^{-D}e^{\frac{1}{12D}})^2} = \frac{\sqrt{2\pi}4^D\sqrt{2}D^{2D+1/2}e^{-2D}e^{\frac{1}{24D+1}}}{2\pi D^{2D+1}e^{-2D}e^{\frac{1}{6D}}}$$

$$= \frac{4^D}{\sqrt{\pi D}}e^{\frac{1}{24D+1}-\frac{1}{6D}}.$$

Συνεπώς, για να έχουμε τη ζητούμενη σχέση αρκεί $\frac{1}{24D+1}-\frac{1}{6D} > -\frac{1}{8D}-\frac{1}{144D^2}$, το οποίο ισχύει, καθώς $\frac{1}{24D+1}-\frac{1}{6D} = -\frac{18D+1}{6D(24D+1)} > -\frac{18D+1}{6D*24D} = -\frac{1}{8D}-\frac{1}{144D^2}$. □

Λήμμα 2.1.7. *Για την ακολουθία*

$$a_n := \left(\frac{2n+1}{2n-1}\right)^{\frac{(2n-1)(p-1)+1}{2}}, \text{ όπου } n \geq 2 \text{ και } p \text{ πρώτος αριθμός, διάφορος του } 2,$$

ισχύουν τα εξής:

1. *Η a_n είναι γνησίως αύξουσα,*

2. $a_n > \sqrt{\frac{5}{3}}(2,1516)^{p-1}$ *και*

3. $\lim_{n\to\infty} a_n = e^{p-1}$.

Απόδειξη. 1. $a_{n+1} > a_n \Leftrightarrow \left(\frac{(2n+3)(2n-1)}{(2n+1)^2}\right)^{\frac{(2n-1)(p-1)+1}{2}} > \left(\frac{2n+1}{2n+3}\right)^{p-1}$, που ισχύει καθώς για $n \geq 2$ έχουμε $8n^2 > 10 \Rightarrow 8n^3 + 20n^2 + 6n - 9 > 8n^3 + 12n^2 + 6n + 1 \Rightarrow \frac{(2n+3)(2n-1)}{(2n+1)^2} > \frac{2n+1}{2n+3} > 0$ και $\frac{(2n-1)(p-1)+1}{2} > p - 1 > 0$.

2. $a_2 = \left(\frac{5}{3}\right)^{\frac{3(p-1)+1}{2}} = \sqrt{\frac{5}{3}}\left[\left(\frac{5}{3}\right)^{3/2}\right]^{p-1} > \sqrt{\frac{5}{3}}(2,1516)^{p-1}$ και a_n γνησίως αύξουσα, συνεπώς $a_n > \sqrt{\frac{5}{3}}(2,1516)^{p-1}$.

3.

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty}\left(\frac{2n+1}{2n-1}\right)^{\frac{(2n-1)(p-1)+1}{2}} = \lim_{n\to\infty}\sqrt{\frac{2n+1}{2n-1}}\lim_{n\to\infty}\left[\left(\frac{2n+1}{2n-1}\right)^{\frac{2n-1}{2}}\right]^{p-1}.$$

Όμως,

$$\lim_{n\to\infty}\sqrt{\frac{2n+1}{2n-1}} = 1$$

και

$$\lim_{n\to\infty}\left(\frac{2n+1}{2n-1}\right)^{\frac{2n-1}{2}} = \lim_{n\to\infty}\left(1+\frac{1}{\frac{2n-1}{2}}\right)^{\frac{2n-1}{2}} = \lim_{m\to\infty}\left(1+\frac{1}{m}\right)^{m} = e.$$

Συνεπώς,

$$\lim_{n\to\infty} a_n = e^{p-1}.$$

□

2.2 Το Σύνολο $I_{s,t,m}$

Όπως έχουμε ήδη αναφέρει, στόχος μας είναι να υπολογίσουμε την τάξη κάποιων στοιχείων, συγκρίνοντάς τη με τον πληθάριθμο ενός συνόλου. Στην ενότητα αυτή, ορίζουμε τα σύνολα τα οποία θα χρησιμοποιήσουμε και θα υπολογίσουμε ένα κάτω φράγμα των πληθαρίθμων τους.

Ορισμός 2.2.1. Για κάθε $s, t, m \in \mathbb{N}, m < D$, ορίζουμε το σύνολο

$$I_{s,t,m} \coloneqq \left\{(u_0,\ldots,u_{D-1}) \in \mathbb{Z}^D \mid \sum_{u_j>0} u_j \leq s, \sum_{u_j<0}|u_j| \leq t \text{ και οι πρώτες m συντεταγμένες είναι } 0\right\}$$

Λήμμα 2.2.2. *Έστω $I_{s,t,m}$, όπως στον ορισμό 2.2.1. Τότε,*

$$|I_{s,t,m}| = \sum_{i=0}^{D-m} \binom{D-m}{i}\binom{s}{i}\binom{D-m-i+t}{t}.$$

Συγκεκριμένα, για $t \geq \frac{D-m}{2}$,

$$|I_{t,t,m}| > \binom{\frac{D-m}{2}+t}{D-m}\binom{2D-2m}{D-m}.$$

Απόδειξη. Έστω $R = D-m$. Για κάθε $0 \leq i \leq R$ και $0 \leq j \leq R-i$ υπάρχουν $\binom{R}{i}\binom{R-i}{j}$ διαφορετικοί τρόποι ώστε να επιλέξουμε i συντεταγμένες από τις $u_m, \ldots, u_{D-1}$ ώστε να είναι θετικές και j να είναι αρνητικές (οι υπόλοιπες είναι μηδέν). Επιπλέον, το πλήθος των θετικών λύσεων της ανίσωσης $x_1+x_2+\cdots+x_i \leq s$ είναι $\binom{s}{i}$ και το πλήθος των θετικών λύσεων της ανίσωσης $x_1+x_2+\cdots+x_j \leq t$ είναι $\binom{t}{j}$. Συνεπώς, για κάθε ζεύγος i,j υπάρχουν $\binom{R}{i}\binom{R-i}{j}\binom{s}{i}\binom{t}{j}$ στοιχεία του $I_{s,t,m}$. Αθροίζοντας για κάθε i,j έχουμε

$$|I_{s,t,m}| = \sum_{i=0}^{R}\binom{R}{i}\binom{s}{i}\sum_{j=0}^{R-i}\binom{R-i}{j}\binom{t}{j} = \sum_{i=0}^{R}\binom{R}{i}\binom{s}{i}\binom{R-i+t}{t}. \tag{2.1}$$

Επίσης, $\binom{R+t-i}{t} = \frac{\binom{R}{i}\binom{R-i+t}{R}}{\binom{t}{i}}$. Έτσι, αντικαθιστώντας το στη σχέση 2.1 και για $s=t$ προκύπτει

$$|I_{t,t,m}| = \sum_{i=0}^{R}\binom{R}{i}^2\binom{R-i+t}{R} = \frac{1}{2}\sum_{i=0}^{R}\binom{R}{i}^2\left[\binom{R-i+t}{R}+\binom{i+t}{R}\right]$$

$$\geq \frac{1}{2}\left[\binom{\lfloor\frac{R}{2}\rfloor+t}{R}+\binom{\lceil\frac{R}{2}\rceil+t}{R}\right]\sum_{i=0}^{R}\binom{R}{i}^2$$

$$\geq \frac{1}{2}\left[\binom{\lfloor\frac{R}{2}\rfloor+t}{R}+\binom{\lceil\frac{R}{2}\rceil+t}{R}\right]\binom{2R}{R}$$

$$\geq \binom{\frac{R}{2}+t}{R}\binom{2R}{R},$$

όπου η τελευταία ανισότητα προκύπτει από το γεγονός ότι η συνάρτηση $\Gamma_N(x) := \binom{x}{N}$ είναι κυρτή για κάθε $x \geq N$. □

Πρόταση 2.2.3. *Για κάθε $D \geq 2$ και $r \geq 3$ ισχύουν τα εξής:*

1. $|I_{\lfloor \frac{Dr}{2} \rfloor, \lfloor \frac{Dr}{2} \rfloor, 0}| > \frac{1}{\sqrt{2\pi D}} \sqrt{\frac{r-1}{r+1}} \left(\frac{4(r+1)^{r+1}}{(r-1)^{r-1}} \right)^{\frac{D}{2}} e^{-\frac{1}{12D}\frac{5r^2+3}{r^2-1} - \frac{1}{144D^2}}$,

2. $|I_{\lfloor \frac{Dr}{4} \rfloor, \lfloor \frac{Dr}{4} \rfloor, 0}| > \frac{1}{\sqrt{2\pi D}} \sqrt{\frac{r-2}{r+2}} \left(\frac{(r+2)^{r+2}}{(r-2)^{r-2}} \right)^{\frac{D}{4}} e^{-\frac{5}{24D}\frac{r^2+4}{r^2-4} - \frac{1}{144D^2}}$ *και*

3. $|I_{\lfloor \frac{Dr}{2} \rfloor, \lfloor \frac{Dr}{2} \rfloor, \lfloor \frac{D}{2} \rfloor}| > \frac{\sqrt{2}}{\pi D} \sqrt{\frac{r}{r+1}} \left(\frac{4(r+1)^{r+1}}{r^r} \right)^{\frac{D}{2}} e^{-\frac{1}{12D}\frac{5r^2+5r+2}{r^2+r} - \frac{1}{144D^2}}$.

Απόδειξη. Θα απόδείξουμε το 2. και οι αποδείξεις των 1. και 3. είναι παρόμοιες. Κάνοντας απλές πράξεις, βλέπουμε ότι

$$\binom{\frac{D}{2} + \frac{Dr}{4} - 1}{D} = \frac{\frac{D}{2} + \frac{Dr}{4} - D}{\frac{D}{2} + \frac{Dr}{4}} \binom{D\frac{r+2}{4}}{D} = \frac{r-2}{r+2} \binom{D\frac{r+2}{4}}{D}.$$

Συνεπώς, από την πρόταση 2.1.4 έχουμε

$$\begin{aligned} \binom{\frac{D}{2} + \frac{Dr}{4} - 1}{D} &\geq \frac{r-2}{r+2} \sqrt{\frac{\frac{r+2}{4}}{2\pi \frac{r-2}{4}}} \left(\frac{\left(\frac{r+2}{4}\right)^{\frac{r+2}{4}}}{\left(\frac{r-2}{4}\right)^{\frac{r-2}{4}}} \right)^D \frac{1}{\sqrt{D}} e^{-\frac{1}{12D}(1+\frac{16}{r^2-4})} \\ &= \frac{1}{\sqrt{2\pi D}} \sqrt{\frac{r-2}{r+2}} \left(\frac{(r+2)^{\frac{r+2}{4}}}{4(r-2)^{\frac{r-2}{4}}} \right)^D e^{-\frac{r^2+12}{12D(r^2-4)}}. \end{aligned}$$

Τέλος, από το Λήμμα 2.2.2 και την πρόταση 2.1.6 για $s = t = \lfloor \frac{Dr}{4} \rfloor$ και $m = 0$ (άρα $R = D$), έχουμε

$$\begin{aligned} |I_{\lfloor \frac{Dr}{4} \rfloor, \lfloor \frac{Dr}{4} \rfloor, 0}| &\geq \binom{\frac{D}{2} + \lfloor \frac{Dr}{4} \rfloor}{D} \binom{2D}{D} \geq \binom{\frac{D}{2} + \frac{Dr}{4} - 1}{D} \binom{2D}{D} \\ &> \frac{1}{\sqrt{2\pi D}} \sqrt{\frac{r-2}{r+2}} \left(\frac{(r+2)^{r+2}}{(r-2)^{r-2}} \right)^{\frac{D}{4}} \frac{1}{4^D} e^{-\frac{r^2+12}{12D(r^2-4)}} \frac{4^D}{\sqrt{\pi D}} e^{-\frac{1}{8D} - \frac{1}{144D^2}} \\ &> \frac{1}{\sqrt{2\pi D}} \sqrt{\frac{r-2}{r+2}} \left(\frac{(r+2)^{r+2}}{(r-2)^{r-2}} \right)^{\frac{D}{4}} e^{-\frac{5}{24D}\frac{r^2+4}{r^2-4} - \frac{1}{144D^2}}. \end{aligned}$$

□

Κεφάλαιο 3

Εύρεση Στοιχείου Μεγάλης Τάξης της Επέκτασης Artin - Schreier

Στην παρούσα εργασία, με $\mathbb{F}_q$ θα συμβολίζουμε το πεπερασμένο σώμα τάξης q, όπου $q = p^n, p \in \mathbb{P}$, $p \neq 2$ και $n \in \mathbb{N}$.

3.1 Αναγωγισιμότητα Πολυωνύμων

Είναι γνωστό ότι για κάθε ανάγωγο πολυώνυμο $f(X) \in \mathbb{F}_q[X]$ βαθμού $d = \deg f$, το $\mathbb{F}_q[X]/(f)$ είναι πεπερασμένο σώμα τάξης q^d.
Ισχύει επιπλέον και το αντίστροφο, δηλαδή κάθε πεπερασμένο σώμα της μορφής $\mathbb{F}_{q^d}$ είναι ισόμορφο με το $\mathbb{F}_q[X]/(f)$, για κάποιο ανάγωγο πολυώνυμο f βαθμού d.
Θα παρουσιάσουμε, τώρα, ορισμένα θεωρήματα τα οποία μας εξασφαλίζουν την αναγωγισιμότητα πολυωνύμων σε πεπερασμένα σώματα.

Θεώρημα 3.1.1. *Το κυκλοτομικό σώμα $\mathbb{K}^{(n)}$ είναι μια απλή αλγεβρική επέκταση του $\mathbb{K}$. Επιπλέον:*

1. *αν $\mathbb{K} = \mathbb{Q}$, τότε το κυκλοτομικό πολυώνυμο Φ_n είναι ανάγωγο υπέρ το $\mathbb{K}$ και $[\mathbb{K}^{(n)} : \mathbb{K}] = \varphi(n)$.*

2. *αν $\mathbb{K} = \mathbb{F}_q$ με $\mu\kappa\delta(q, n) = 1$, τότε το Φ_n παραγοντοποιείται σε $\varphi(n)/d$ διακριτά μονικά ανάγωγα πολυώνυμα στο $\mathbb{K}[X]$ βαθμού d. Επιπλέον, το $\mathbb{K}^{(n)}$ είναι το σώμα ανάλυσης για καθένα ανάγωγο παράγοντα υπέρ του $\mathbb{K}$ και $[\mathbb{K}^{(n)} : \mathbb{K}] = d$, όπου d είναι ο ελάχιστος θετικός ακέραιος, ο οποίος ικανοποιεί τη σχέση $q^d \equiv 1 \pmod{n}$.*

Απόδειξη. Η απόδειξη βρίσκεται στο θεώρημα 2.47, σελίδα 61, του [9]. □

Θεώρημα 3.1.2. *Έστω $t \geq 2$, $t \in \mathbb{Z}$ και $a \in \mathbb{F}_q^*$. Τότε το διώνυμο $X^t - a$ είναι ανάγωγο υπέρ το $\mathbb{F}_q[X]$ αν και μόνο αν ικανοποιούνται τα εξής:*

(*i*) *κάθε πρώτος παράγοντας του t διαιρεί την τάξη e του a στο $\mathbb{F}_q^*$ αλλά δεν διαιρεί το $(q-1)/e$ και*

(*ii*) $q \equiv 1 \pmod 4$, *αν* $t \equiv 0 \pmod 4$.

Απόδειξη. Η απόδειξη βρίσκεται στο θεώρημα 3.75, σελίδα 116, του [9]. □

Θα παραθέσουμε επιπλέον μερικά γνωστά αποτελέσματα για την αναγωγισιμότητα κάποιων οικογενειών πολυωνύμων.

Λήμμα 3.1.3. *Το πολυώνυμο $X^p - X - a \in \mathbb{F}_q[X]$ είναι ανάγωγο, αν και μόνο αν, δεν έχει ρίζες στο $\mathbb{F}_q$.*

Απόδειξη. Η απόδειξη βρίσκεται στο θεώρημα 3.78 του [9]. □

Πιο συγκεκριμένα:

Πρόταση 3.1.4. *Έστω n θετικός ακέραιος και $a \in \mathbb{F}_p^*$. Το πολυώνυμο $f(X) = X^p - X - a$ είναι ανάγωγο στο $\mathbb{F}_q[X]$, αν και μόνο αν, $p \nmid n$.*

Απόδειξη. Για την απόδειξη της συγκεκριμένης πρότασης θα θεωρήσουμε γνωστό ότι

$$a = b^p - b, \text{ για κάποιο } b \in \mathbb{F}_q \Leftrightarrow \mathcal{T}r_{\mathbb{F}_q/\mathbb{F}_p}(a) = a + a^p + \ldots + a^{p^{n-1}} \neq 0.$$

Η απόδειξη του παραπάνω ισχυρισμού βρίσκεται στο θεώρημα 2.25 του [9].
Αφού $a \in \mathbb{F}_p$, έχουμε ότι $\mathcal{T}r_{\mathbb{F}_q/\mathbb{F}_p}(a) = na$. Όμως,

$$\mathcal{T}r_{\mathbb{F}_q/\mathbb{F}_p}(a) \neq 0 \Leftrightarrow na \neq 0 \Leftrightarrow p \nmid n.$$

□

3.2 Το Πεπερασμένο Σώμα $\mathbb{F}_q[X]/(X^p - X - 1)$

Για την ενότητα αυτή θα θεωρούμε πως το πολυώνυμο $X^p - X - 1$ είναι ανάγωγο υπέρ του $\mathbb{F}_q[X]$, δηλαδή ότι $q = p^n$, με μκδ$(p, n) = 1$. Επιπλέον, το θ θα αναπαριστά

το σύμπλοκο του X στην επέκταση Artin-Schreier $\mathbb{K} \coloneqq \mathbb{F}_q[X]/(X^p - X - 1)$ και το b θα είναι στοιχείο του $\mathbb{F}_q \setminus \mathcal{A}_n$, όπου

$$\mathcal{A}_n = \bigcup_{\substack{m|n \\ m \neq n}} \mathbb{F}_{p^m}.$$

Στόχος μας είναι να υπολογίσουμε την πολλαπλασιαστική τάξη του στοιχείου $\theta + b$. Προτού όμως γίνει αυτό, θα αποδείξουμε ότι σχεδόν κάθε στοιχείο $b \in \mathbb{F}_q$ ικανοποιεί τη συνθήκη που επιβάλαμε στο b.

Θεώρημα 3.2.1. *Το πλήθος των στοιχείων του συνόλου $\mathbb{F}_q \setminus \mathcal{A}_n$ είναι $\sum_{d|n} p^d \mu(n/d)$, όπου μ είναι η συνάρτηση Mobius. Μάλιστα, η πιθανότητα να επιλεγεί ένα στοιχείο του $\mathbb{F}_q$, το οποίο να μην ανήκει στο $\mathcal{A}_n$ είναι μεγαλύτερη από $1 - \frac{\log_r n}{q^{1-1/r}}$, όπου r είναι ο μικρότερος πρώτος διαιρέτης του n.*

Απόδειξη. Έστω $g : \mathbb{N}^* \longrightarrow \mathbb{N}$ η συνάρτηση που ορίζεται από τον τύπο

$$g(m) = |\mathbb{F}_{p^m} \setminus \mathcal{A}_m|.$$

Τότε, για κάθε φυσικό αριθμό m, το $g(m)$ μετράει πόσα στοιχεία του $\mathbb{F}_{p^m}$ δεν ανήκουν σε κανένα γνήσιο υπόσωμά του. Επιπλέον, κάθε γνήσιο υπόσωμα του $\mathbb{F}_{p^m}$ είναι της μορφής $\mathbb{F}_{p^l}, l \mid m, l \neq m$. Συνεπώς,

$$\sum_{d|m} g(d) = |\mathbb{F}_{p^m}| = p^m.$$

Από τον τύπο αντιστροφής Mobius, έχουμε ότι

$$g(m) = \sum_{d|m} p^d \mu(m/d).$$

Τώρα, θα υπολογίσουμε ένα άνω φράγμα για το πλήθος των στοιχείων του $\mathcal{A}_n$. Έστω $p_1^{\alpha_1} \dots p_s^{\alpha_s}$ η παραγοντοποίηση του n σε πρώτους παράγοντες, όπου $p_1 < \dots < p_s$. Για κάθε γνήσιο διαιρέτη d του n, υπάρχει πρώτος αριθμός $p_i, 1 \leq i \leq s$ έτσι, ώστε $d \mid (n/p_i)$. Πράγματι, $d \mid n$ άρα ο d θα είναι της μορφής $p_{j_1}^{\beta_{j_1}} \dots p_{j_l}^{\beta_{j_l}}$, όπου τα $j_1, \dots, j_l$ είναι κάποια από τα $1, \dots, s, l \leq s$ και $d \neq n$. Συνεπώς, $n = d p_1^{\gamma_1} \dots p_s^{\gamma_s}$, με $0 \leq \gamma_k \leq \alpha_k$ και $n \neq d$ άρα υπάρχει $1 \leq i \leq s$ τέτοιο, ώστε $\gamma_i \neq 0$. Έτσι, $d \mid (n_i)$. Άρα, $\mathcal{A}_n \subset \bigcup_{1 \leq i \leq s} \mathbb{F}_{p^{n_i}}$ όπου $n_i = n/p_i$. Συγκεκριμένα,

$$|\mathcal{A}_n| \leq |\bigcup_{1 \leq i \leq s} \mathbb{F}_{p^{n_i}}| \leq \sum_{1 \leq i \leq s} p^{n_i} \leq s p^{\frac{n}{p_1}} \leq p^{\frac{n}{p_1}} \log_{p_1} n = q^{\frac{1}{p_1}} \log_{p_1} n.$$

Έτσι, η πιθανότητα να επιλέξουμε τυχαία ένα στοιχείο του $\mathbb{F}_q$, το οποίο να μην ανήκει στο $\mathcal{A}_n$ είναι μεγαλύτερη από

$$1 - \frac{|\mathcal{A}_n|}{q} \geq 1 - \frac{\log_{p_1} n}{q^{1-\frac{1}{p_1}}}.$$

Πράγματι, αν με $\mathcal{P}(\mathcal{A}_n)$ συμβολίσουμε την πιθανότητα να επιλεγεί στοιχείο του $\mathcal{A}_n$ και με $\mathcal{P}(\mathcal{A}_n^c)$ την πιθανότητα να επιλεγεί στοιχείο του $\mathbb{F}_q$ που δεν ανήκει στο $\mathcal{A}_n$, τότε

$$\mathcal{P}(\mathcal{A}_n) = \frac{|\mathcal{A}_n|}{|\mathbb{F}_q|} \leq \frac{\log_{p_1} n}{q^{1-\frac{1}{p_1}}}.$$

Επίσης, $\mathcal{P}(\mathcal{A}_n^c) = 1 - \mathcal{P}(\mathcal{A}_n)$ και συνεπώς

$$\mathcal{P}(\mathcal{A}_n^c) \geq 1 - \frac{\log_{p_1} n}{q^{1-\frac{1}{p_1}}}.$$

□

Το παραπάνω θεώρημα αποδεικνύει ότι σχεδόν κάθε στοιχείο του $\mathbb{F}_q$ ικανοποιεί τη συνθήκη που επιβάλαμε στο b. Για να είμαστε σε θέση να αποδείξουμε το θεώρημα 3.3.2 θα χρειαστούμε κάποια τεχνικά λήμματα.

Λήμμα 3.2.2. *Έστω $i, j \in \mathbb{Z}$ τέτοιοι, ώστε $0 \leq i, j \leq np - 1$. Εάν $i \neq j$, τότε $i + b^{p^i} \neq j + b^{p^j}$.*

Απόδειξη. Έστω i_0 να είναι το υπόλοιπο της διαίρεσης του i από το n και j_0 το υπόλοιπο της διαίρεσης του j από το n. Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $i_0 \geq j_0$. Το b είναι στοιχείο του $\mathbb{F}_q$ και συνεπώς ισχύουν $b^{p^i} = b^{p^{i_0}}$ και $b^{p^j} = b^{p^{j_0}}$. Για να καταλήξουμε σε αντίφαση, υποθέτουμε επιπλέον ότι $i + b^{p^i} = j + b^{p^j}$. Έτσι, προκύπτουν τα εξής:

$$j - i = b^{p^i} - b^{p^j} \tag{3.1}$$

και

$$j - i = b^{p^{i_0}} - b^{p^{i_0}}. \tag{3.2}$$

Στην περίπτωση όπου $i_0 = j_0$, έχουμε ότι $j \equiv i \pmod{n}$, άρα $j = i + nk$ για κάποιο ακέραιο k. Τότε, όμως, η εξίσωση 3.1 γίνεται

$$0 = b^{p^i} - b^{p^j} = j - i = nk$$

και συνεπώς $p \mid k$ (καθώς μκδ$(p, n) = 1$), το οποίο είναι άτοπο αφού $0 < |i - j| < np$. Έτσι, $i_0 \neq j_0$, άρα $i_0 > j_0$ και έτσι $0 < i_0 - j_0 < n$. Υψώνοντας την εξίσωση 3.1 στην p^{n-j_0}-οστή δύναμη, προκύπτει

$$(j - i)^{p^{n-j_0}} = (b^{p^j} - b^{p^i})^{p^{n-j_0}},$$

$$j - i = b^{p^{n+i-j_0}} - b^{p^{n+j-j_0}},$$
$$j - i = (b^{p^n})^{p^{i_0-j_0}} - b^{p^n}, \text{ άρα}$$
$$j - i = b^{p^{i_0-j_0}} - b.$$

Δηλαδή, υπάρχει $0 \leq t < n$ τέτοιο, ώστε $b^{p^t} - b \in \mathbb{F}_p$ και συνεπώς

$$b^{p^{t+1}} - b^p = (b^{p^t} - b)^p = b^{p^t} - b.$$

Η τελευταία εξίσωση, όμως, μπορεί να γραφεί ως $b^p - b = (b^p - b)^{p^t}$, το οποίο δηλώνει ότι το $b^p - b$ είναι στοιχείο του $\mathbb{F}_{p^t}$. Επιπλέον, εάν είχαμε ότι $b \notin \mathbb{F}_{p^t}$, από το Λήμμα 3.1.3 προκύπτει ότι το πολυώνυμο $X^p - X - (b^p - b) \in \mathbb{F}_{p^t}[X]$ είναι ανάγωγο υπέρ του $\mathbb{F}_{p^t}$. Σε κάθε περίπτωση ισχύει ότι $b \in \mathbb{F}_{p^{pt}}$. Αφού το b είναι και στοιχείο του $\mathbb{F}_{p^n}$, τότε

$$b \in \mathbb{F}_{p^{pt}} \cap \mathbb{F}_{p^{\mu\kappa\delta(pt,n)}} = \mathbb{F}_{p^{\mu\kappa\delta(t,n)}},$$

όπου ο $\mu\kappa\delta(t, n) < n$ είναι ένας γνήσιος διαιρέτης του n και συνεπώς αυτό αντιβαίνει στη συνθήκη που επιβάλαμε για το b ($b \notin \mathcal{A}_n$).

□

Λήμμα 3.2.3. *Έστω t, s μη-αρνητικοί ακέραιοι τέτοιοι, ώστε $0 \leq t + s \leq p - 1$ και έστω $J_{s,t}$ το υποσύνολο του $\mathbb{Z}^{np}$ τέτοιο, ώστε*

$$\vec{r} := (r_0, r_1, \ldots, r_{np-1}) \in J_{s,t} \iff$$

$$\sum_{\substack{0 \leq j \leq np-1 \\ r_j < 0}} (-r_j) \leq t \text{ και } \sum_{\substack{0 \leq j \leq np-1 \\ r_j > 0}} r_j \leq s.$$

Τότε η συνάρτηση

$$\Lambda : J_{s,t} \longrightarrow G$$
$$\vec{r} \longmapsto \prod_{0 \leq j \leq np-1} (\theta + b)^{r_j p^j},$$

όπου $G = \langle \theta + b \rangle \leq \mathbb{K}^*$, είναι ένα προς ένα.

Απόδειξη. Αφού θ είναι το σύμπλοκο του X στο σώμα πηλίκων $\mathbb{K} = \mathbb{F}_q[X]/(X^p - X - 1)$, τότε κάθε στοιχείο του $\mathbb{K}$ είναι το σύμπλοκο ενός μοναδικού $h(\theta)$, όπου h είναι ένα πολυώνυμο του $\mathbb{F}_q[X]$ βαθμού το πολύ $p - 1$. Επιπλέον, $\theta^p = \theta + 1$ και, επομένως,

$$\theta^{p^{j+1}} = (\theta^p)^{p^j} = (\theta + 1)^{p^j} = \theta^{p^j} + 1, \text{ για κάθε } j \in \mathbb{N}.$$

Εύκολα αποδεικνύεται, με επαγωγή, ότι

$$\theta^{p^j} = \theta + j, \text{ για κάθε } j \geq 1,$$

και, συνεπώς, για κάθε $\vec{r} = (r_0, \ldots, r_{np-1}) \in J_{s,t}$ έχουμε

$$\Lambda(\vec{r}) = \prod_{0 \le i \le np-1} (\theta + b)^{r_i p^i} = \prod_{0 \le i \le np-1} (\theta + i + b^{p^i})^{r_i}.$$

Τώρα, υποθέτουμε ότι υπάρχει διάνυσμα $\vec{s} = (s_0, \ldots, s_{np-1})$ του $J_{s,t}$ τέτοιο, ώστε $\Lambda(\vec{r}) = \Lambda(\vec{s})$. Έτσι,

$$\prod_{0 \le i \le np-1} (\theta + i + b^{p^i})^{r_i} = \prod_{0 \le j \le np-1} (\theta + j + b^{p^j})^{s_j},$$

άρα το πολυώνυμο

$$F(X) = \prod_{\substack{0 \le i \le np-1 \\ r_i > 0}} (X + i + b^{p^i})^{r_i} \prod_{\substack{0 \le j \le np-1 \\ s_j < 0}} (X + j + b^{p^j})^{-s_j}$$

είναι ισότιμο με το πολυώνυμο

$$G(X) = \prod_{\substack{0 \le j \le np-1 \\ s_j > 0}} (X + j + b^{p^j})^{s_j} \prod_{\substack{0 \le i \le np-1 \\ r_i < 0}} (X + i + b^{p^i})^{-r_i}$$

modulo $X^p - X - 1$. Αφού, όμως, $\deg(F) \le s + t \le p - 1$ και $\deg(G) \le s + t \le p - 1$ συμπεραίνουμε ότι $F(X) = G(X)$. Επιπλέον, από το Λήμμα 3.2.2 γνωρίζουμε ότι $X + i + b^{p^i} \ne X + j + b^{p^j}$, για κάθε $0 \le i < j \le np - 1$ και έτσι έχουμε $\vec{r} = \vec{s}$. Δηλαδή, η συνάρτηση Λ είναι ένα προς ένα.

□

Λήμμα 3.2.4. *Έστω $J_{s,t}$ όπως ορίστηκε στο Λήμμα 3.2.3. Τότε*

$$|J_{s,t}| = \sum_{j=0}^{t} \sum_{i=0}^{s} \binom{np}{i} \binom{np-i}{j} \binom{s}{i} \binom{t}{j}. \tag{3.3}$$

Συγκεκριμένα,

$$|J_{s,t}| > \binom{np + t - s}{t} \binom{np + s}{s}.$$

Απόδειξη. Παρατηρούμε ότι για κάθε $j \le t$ και $i \le s$ μπορούμε να επιλέξουμε j συντεταγμένες του $\vec{r}$ να είναι αρνητικές και i συντεταγμένες να είναι θετικές. Αυτό μπορεί να γίνει με $\binom{np}{i}\binom{np-i}{j}$ τρόπους. Επιπλέον, το πλήθος των θετικών λύσεων της ανισότητας $x_1 + x_2 + \cdots + x_i \le s$ είναι $\binom{s}{i}$ και αντίστοιχα, το πλήθος των θετικών λύσεων της ανισότητας $x_1 + x_2 + \cdots + x_j \le t$ είναι $\binom{t}{j}$. Άρα, για κάθε ζεύγος i, j,

υπάρχουν $\binom{np}{i}\binom{np-i}{j}\binom{s}{i}\binom{t}{j}$ στοιχεία του $J_{s,t}$ και συνεπώς, αθροίζοντάς τα για κάθε $0 \leq i \leq s$ και $0 \leq j \leq t$ συμπεραίνουμε την εξίσωση 3.3. Επιπλέον,

$$\begin{aligned}
|J_{s,t}| &\geq \sum_{i=0}^{s} [\binom{s}{i}\binom{np}{i}(\sum_{j=0}^{t}\binom{np-i}{j}\binom{t}{j})] \\
&\overset{2.1.3}{=} \sum_{i=0}^{s}\binom{s}{i}\binom{np}{i}\binom{np+t-i}{t} \\
&> \binom{np+t-s}{t}\sum_{i=0}^{s}\binom{s}{i}\binom{np}{i} \\
&= \binom{np+t-s}{t}\binom{np+s}{s}.
\end{aligned}$$

□

Για να αποδείξουμε τα κεντρικά μας θεωρήματα, θα χρειαστούμε ένα ακόμη τεχνικό λήμμα.

Λήμμα 3.2.5. *Για κάθε $s > 0$ και $r > 1$, έχουμε*

$$c_r \cdot d_r^s \cdot \frac{1}{\sqrt{s}} \cdot \Theta(r,s) < \binom{rs}{s} < c_r \cdot d_r^s \cdot \frac{1}{\sqrt{s}},$$

όπου

$$c_r = \sqrt{\frac{r}{2\pi(r-1)}}, d_r = \frac{r^r}{(r-1)^{r-1}}$$

και

$$\Theta(r,s) = e^{-\frac{1}{12s}\left(1+\frac{1}{r(r-1)}\right)}.$$

Απόδειξη. Η απόδειξη του παραπάνω λήμματος βρίσκεται στην πρόταση 1 του [17]. □

Παρατηρούμε ότι το κάτω και το πάνω φράγμα του παραπάνω λήμματος είναι πολύ κοντά μεταξύ τους, όταν $s \gg 0$.

3.3 Ένα Ισχυρό Φράγμα της Τάξης της Ομάδας $\langle\theta\rangle$

Στην ενότητα αυτή, θα φράξουμε από κάτω την τάξη κάποιων στοιχείων της επέκτασης Artin-Schreier από έναν κατάλληλα μεγάλο αριθμό. Για να το επιτύχουμε αυτό, θα συγκρίνουμε την τάξη τους με τους πληθαρίθμους των συνόλων J που ορίσαμε πριν.

Ορισμός 3.3.1. Έστω $X^p - X - 1$ ανάγωγο πολυώνυμο του $\mathbb{F}_q[X]$, όπου $q = p^n$ και μκδ$(p, n) = 1$. Η επέκταση $\mathbb{F}_q[X]/(X^p - X - 1)$ θα λέγεται επέκταση Artin-Schreier.

Στόχος μας είναι να βρούμε ένα στοιχείο μεγάλης τάξης στην παραπάνω επέκταση.

Θεώρημα 3.3.2. *Έστω $X^p - X - a$ ένα ανάγωγο πολυώνυμο υπέρ το $\mathbb{F}_q$, με $q = p^n$, $n \geq 2$ και $a \in \mathbb{F}_p$. Έστω, επίσης, θ να είναι το σύμπλοκο του X στην επέκταση Artin − Schreier $\mathbb{F}_q[X]/(X^p - X - a)$ και $b \in \mathbb{F}_q$ τέτοιο, ώστε να ικανοποιεί τη σχέση $b \notin \mathbb{F}_{p^m}$, για κάθε $m \neq n, m|n$. Τότε, η πολλαπλασιαστική τάξη του στοιχείου $\theta + b$ φράσσεται κάτω από τον αριθμό*

$$\frac{1}{\pi(p-1)}\sqrt{\frac{2n+1}{2n-1}}\left(\frac{(2n+1)^{(2n+1)}}{(2n-1)^{(2n-1)}}\right)^{\frac{p-1}{2}} e^{-\frac{1}{3(p-1)}\left(\frac{4n^2}{4n^2-1}\right)}.$$

Συγκεκριμένα, για κάθε $\epsilon > 0$ και $n > N_\epsilon$,

$$|\langle\theta + b\rangle| > \frac{1}{\pi p}((e-\epsilon)(2n+1))^{p-1}.$$

Απόδειξη. Το θεώρημα αυτό αρκεί να αποδειχθεί στην περίπτωση όπου $a = 1$. Η απόδειξη αυτού του ισχυρισμού βρίσκεται στο τέλος της συγκεκριμένης ενότητας. Από το λήμμα 3.2.3 γνωρίζουμε ότι $|\langle\theta + b\rangle| \geq |J_{s,t}|$, για κάθε μη-αρνητικούς ακέραιους s και t τέτοιους, ώστε $s + t \leq p - 1$. Έτσι, από το Λήμμα 3.2.4 έχουμε ότι

$$|\langle\theta + b\rangle| > \max_{0\leq s+t\leq p-1}\binom{np+t-s}{t}\binom{np+s}{s} > \binom{np}{(p-1)/2}\binom{np+(p-1)/2}{(p-1)/2}. \tag{3.4}$$

Τώρα, χρησιμοποιώντας το Λήμμα 3.2.5, φράσσουμε από κάτω τους παραπάνω διωνυμικούς συντελεστές

$$\binom{np}{(p-1)/2} > \binom{2n(p-1)/2}{(p-1)/2} > \sqrt{\frac{2n}{\pi(2n-1)(p-1)}}\left(\frac{(2n)^{2n}}{(2n-1)^{2n-1}}\right)^{\frac{p-1}{2}}\tilde{\Theta}(2n-1)$$

και

$$\begin{aligned}\binom{np+(p-1)/2}{(p-1)/2} &> \binom{(2n+1)(p-1)/2}{(p-1)/2}\\ &> \sqrt{\frac{2n+1}{\pi(2n)(p-1)}}\left(\frac{(2n+1)^{2n+1}}{(2n)^{2n}}\right)^{\frac{p-1}{2}}\tilde{\Theta}(2n+1),\end{aligned}$$

όπου

$$\tilde{\Theta}(z) = e^{-\frac{1}{6(p-1)}(1+\frac{1}{z(z-1)})}.$$

Πολλαπλασιάζοντας, τώρα, τις δύο ανισότητες έχουμε ότι

$$\binom{np}{(p-1)/2}\binom{np+(p-1)/2}{(p-1)/2}$$

$$> \sqrt{\frac{2n}{\pi(2n-1)(p-1)}}\sqrt{\frac{2n+1}{\pi(2n)(p-1)}}\left(\frac{(2n)^{2n}}{(2n-1)^{2n-1}}\right)^{\frac{p-1}{2}}\left(\frac{(2n+1)^{2n+1}}{(2n)^{2n}}\right)^{\frac{p-1}{2}}\tilde{\Theta}(2n-1)\tilde{\Theta}(2n+1)$$

και συνεπώς

$$|\langle\theta+b\rangle| > \frac{1}{\pi(p-1)}\sqrt{\frac{2n+1}{2n-1}}\left(\frac{(2n+1)^{2n+1}}{(2n-1)^{2n-1}}\right)^{(p-1)/2} e^{-\frac{1}{3(p-1)}\left(\frac{4n^2}{4n^2-1}\right)}.$$

Έτσι, έχουμε αποδείξει το πρώτο μέρος του θεωρήματος. Μένει να δείξουμε ότι $|\langle\theta+b\rangle| > \frac{1}{\pi p}((e-\epsilon)(2n+1))^{p-1}$, για κάθε $\epsilon > 0$ και $n > N_\epsilon$. Προφανώς,

$$\sqrt{\frac{2n+1}{2n-1}}\left(\frac{(2n+1)^{2n+1}}{(2n-1)^{2n-1}}\right)^{(p-1)/2} > \left(\frac{2n+1}{2n-1}\right)^{\frac{(2n-1)(p-1)+1}{2}} \overset{2.1.7}{>} \sqrt{\frac{5}{3}}(2,1516)^{p-1},$$

για κάθε $n \in \mathbb{N}, n \geq 2$. Άρα, για $n \geq 2$,

$$|\langle\theta+b\rangle| > \frac{1}{\pi(p-1)}a_n(2n+1)^{p-1}e^{-\frac{1}{3(p-1)}\left(\frac{4n^2}{4n^2-1}\right)}$$

$$> \frac{\sqrt{5}}{\sqrt{3}\pi(p-1)}2,1516(2n+1)^{p-1}e^{-\frac{16}{45(p-1)}}.$$

Παρατηρούμε ότι η παραπάνω προσέγγιση είναι απλούστερη, όμως και ασθενέστερη. Στην περίπτωση, όμως, όπου το n είναι αρκετά μεγάλο, από τον ορισμό του ορίου της a_n (θυμόμαστε, από το λήμμα 2.1.7 $\lim_{n\to\infty} a_n = e^{p-1}$), έχουμε ότι

$$(e-\epsilon)^{p-1} < a_n < e^{p-1}.$$

Επίσης,

$$e^{-\frac{1}{3(p-1)}\left(\frac{4n^2}{4n^2-1}\right)} > 1 - \frac{16}{45(p-1)} = \frac{45p-61}{45(p-1)},$$

άρα

$$|\langle\theta+b\rangle| > \frac{45p-61}{45\pi(p-1)^2}((e-\epsilon)(2n+1))^{p-1}$$

$$> \frac{1}{\pi p}((e-\epsilon)(2n+1))^{p-1},$$

το οποίο ολοκληρώνει την απόδειξή μας.

□

Επιπλέον, στην περίπτωση όπου $p = q$, δηλαδή για $n = 1$, έχουμε το εξής αποτέλεσμα:

Θεώρημα 3.3.3. *Έστω $a \neq 0$ και $b \in \mathbb{F}_p$. Τότε η πολλαπλασιαστική τάξη του στοιχείου $\theta + b$ στην επέκταση Artin-Schreier $\mathbb{F}_p[X]/(X^p - X - a)$ φράσσεται κάτω από το*

$$\frac{\sqrt{3}}{\pi p} e^{-\frac{1}{12}} \left(\frac{16}{3}\right)^p.$$

Απόδειξη. Όπως και με το προηγούμενο θεώρημα, η απόδειξη θα γίνει για $a = 1$. Έστω ότι το πολυώνυμο $X^p - X - 1$ είναι ανάγωγο υπέρ του $\mathbb{F}_p[X]$, όπως υποθέσαμε, και επιπλέον το στοιχείο $b \in \mathbb{F}_q$ ικανοποιεί τη συνθήκη που επιβάλαμε. Από το λήμμα 3.2.4 έχουμε

$$\begin{aligned}
|\langle \theta + b \rangle| &> \max_{s+t=p-1} \binom{p+t-s}{t} \binom{p+s}{s} \\
&= \max_{0 \leq s \leq p-1} \binom{2p-1-2s}{p-1-s} \binom{p+s}{s} \\
&= \max_{\substack{0 \leq \lambda \leq \frac{p-1}{p} \\ p\lambda \in \mathbb{N}}} \binom{2p-1-2p\lambda}{p-1-p\lambda} \binom{p+p\lambda}{p\lambda} \\
&= \frac{1}{2} \max_{\substack{0 \leq \lambda \leq \frac{p-1}{p} \\ p\lambda \in \mathbb{N}}} \binom{p(2-2\lambda)}{p(1-\lambda)} \binom{p(1+\lambda)}{p\lambda}.
\end{aligned}$$

Αντίστοιχα, από το λήμμα 3.2.5 προκύπτει ότι

$$|\langle \theta + b \rangle|$$

$$> \max_{\substack{0 \leq \lambda \leq \frac{p-1}{p} \\ p\lambda \in \mathbb{N}}} \frac{1}{\pi p} \sqrt{\frac{1+\lambda}{2\lambda(1-\lambda)}} \left(\frac{4^{1-\lambda}(1+\lambda)^{1+\lambda}}{\lambda^\lambda}\right)^p \Theta(2, p(1-\lambda)) \Theta\left(\frac{1+\lambda}{\lambda}, p\lambda\right).$$

Έτσι, για $\lambda = 1/3$ προκύπτει

$$|\langle \theta + b \rangle| > \frac{\sqrt{3}}{\pi p} e^{-\frac{1}{12}} \left(\frac{16}{3}\right)^p.$$

□

Τώρα, θα αποδείξουμε ότι η συνάρτηση

$$\begin{aligned}
\tau : \mathbb{F}_q[X]/(X^p - X - a) &\longrightarrow \mathbb{F}_q[X]/(X^p - X - 1) \\
h(X) &\longmapsto h(aX)
\end{aligned}$$

αποτελεί ισομορφισμό σωμάτων και συνεπώς αρκούσε τα παραπάνω θεωρήματα να αποδειχθούν στην περίπτωση όπου $a = 1$.

Απόδειξη. Αρχικά, θα αποδείξουμε ότι η τ είναι καλά ορισμένη.
$\overline{h(X)} = h(X) + \langle X^p - X - a\rangle$, άρα $\tau(\overline{h(X)}) = h(aX) + \langle a^pX^p - aX - a\rangle = h(aX) + \langle a(X^p - X - 1)\rangle = h(aX) + \langle X^p - X - 1\rangle \in {}^{\mathbb{F}_q[X]}\!/_{(X^p - X - 1)}$. Στη συνέχεια θα δείξουμε ότι είναι ομομορφισμός.

1. $\tau(\overline{(h+g)(X)}) = \overline{(h+g)(aX)} = (h+g)(aX) + \langle X^p - X - 1\rangle = h(aX) + g(aX) + \langle X^p - X - 1\rangle = (h(aX) + \langle X^p - X - 1\rangle) + (g(aX) + \langle X^p - X - 1\rangle) = \tau(\overline{h(X)}) + \tau(\overline{g(X)})$.
2. $\tau(\overline{(h*g)(X)}) = \overline{(h*g)(aX)} = (h*g)(aX) + \langle X^p - X - 1\rangle = h(aX) * g(aX) + \langle X^p - X - 1\rangle = (h(aX) + \langle X^p - X - 1\rangle) * (g(aX) + \langle X^p - X - 1\rangle) = \tau(\overline{h(X)}) * \tau(\overline{g(X)})$.

Μένει να αποδείξουμε ότι η τ είναι ένα προς ένα και επί.
$h(X) \in \ker\tau \Rightarrow h(aX) \in \langle X^p - X - 1\rangle \Rightarrow h(X) \in \langle a^{-1}X^p - a^{-1}X - 1\rangle \Rightarrow h(X) \in \langle X^p - X - a\rangle$, συνεπώς η τ είναι ένα προς ένα.
Αν τώρα έχουμε $h(X) + \langle X^p - X - 1\rangle \in {}^{\mathbb{F}_q[X]}\!/_{(X^p - X - 1)}$, τότε αυτό το στοιχείο είναι η εικόνα της $h(a^{-1}X)$ μέσω της τ και συνεπώς η τ είναι επί. □

Κεφάλαιο 4

Εύρεση Στοιχείου Μεγάλης Τάξης Μέσω Generic Root

Στο κεφάλαιο αυτό θα φράξουμε από κάτω την τάξη των generic root κάποιων πολυωνύμων. Όπως και στο προηγούμενο κεφάλαιο, για να το επιτύχουμε αυτό θα συγκρίνουμε την τάξη τους με τους πληθαρίθμους (αυτή τη φορά) των συνόλων I που ορίσαμε στο Κεφάλαιο 2.

4.1 Η Ομάδα $\mathbf{PGL}_2(\mathbb{F}_q)$

Ορισμός 4.1.1. Ορίζουμε ως $\mathrm{GL}_2(\mathbb{F}_q)$ το σύνολο όλων των αντιστρέψιμων 2 επί 2 πινάκων με εγγραφές από το σώμα $\mathbb{F}_q$.

Είναι γνωστό ότι το σύνολο αυτό ορίζει ομάδα με τον συνηθισμένο πολλαπλασιασμό πινάκων. Επίσης, είναι προφανές ότι η σχέση $\sim$ τέτοια, ώστε αν $A, B \in GL_2(\mathbb{F}_q)$, $A \sim B \Leftrightarrow B = \lambda A$, για κάποιο $\lambda \in \mathbb{F}_q^*$, είναι σχέση ισοδυναμίας. Το πηλίκο $GL_2(\mathbb{F}_q)/_\sim$ θα το συμβολίζουμε με $\mathrm{PGL}_2(\mathbb{F}_q)$. Είναι, επίσης, γνωστό ότι το σύνολο $\mathrm{PGL}_2(\mathbb{F}_q)$ αποτελεί ομάδα με το συνηθισμένο πολλαπλασιασμό.

Θεώρημα 4.1.2. *Έστω πίνακας* $M = \begin{bmatrix} A \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in PGL_2(\mathbb{F}_q)$. *Τότε, κάθε ανάγωγος παράγοντας* f *του πολυωνύμου* $F_{A,r}(X) = bX^{q^r+1} - aX^{q^r} + dX - c \in \mathbb{F}_q(X)$ *είναι αναλλοίωτος από μία κατάλληλη φυσική δράση του πίνακα* $M = \begin{bmatrix} A \end{bmatrix}$ *και αντίστροφα, κάθε ανάγωγο πολυώνυμο* f*, το οποίο παραμένει αναλλοίωτο από τη δράση αυτή, είναι ένας παράγοντας του* $F_{A,r}(X)$ *για κάποιο* $r \geq 0$.

Απόδειξη. Η απόδειξη βρίσκεται στο [19]. □

Το παραπάνω θεώρημα χρησιμοποιήθηκε στο [19], όπου υπολόγισαν, ασυμπτωτικά, το πλήθος των ανάγωγων μονικών πολυωνύμων δοσμένου βαθμού, που παραμένουν

αναλλοίωτα από τη δράση του $\left[\begin{array}{c} \mathrm{A} \end{array}\right]$ και συμπέραναν ότι οι ανάγωγοι παράγοντες του $F_{A,r}(X)$ είναι βαθμού Dr, όπου D είναι η τάξη του $\left[\begin{array}{c} \mathrm{A} \end{array}\right]$ στην $\mathrm{PGL}_2(\mathbb{F}_q)$.

Δοθέντος ενός πίνακα $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$ θα συμβολίζουμε με $[A]$ την κλάση του A στην $\mathrm{PGL}_2(\mathbb{F}_q)$ και $D = \mathrm{ord}([A])$. Παρατηρούμε ότι, όταν $\det A = 1$ και ο A είναι διαγωνοποιήσιμος, τότε οι ιδιοτιμές του θα είναι γ και γ^{-1} και $D = \mathrm{ord}([A]) = \frac{\mathrm{ord}(\gamma)}{(\mathrm{ord}(\gamma),2)}$, οπότε $A^D = (-1)^{D+1}I$. Επιπλέον, για κάθε $n \in \mathbb{Z}$ θα συμβολίζουμε με (a_n, b_n) και (c_n, d_n) την πρώτη και τη δεύτερη γραμμή του πίνακα A^n, αντίστοιχα. Δηλαδή, $(a_n, b_n) = (1,0)A^n$ και $(c_n, d_n) = (0,1)A^n$. Στα [6] και [19] έχει μελετηθεί μια δράση της $\mathrm{GL}_2(\mathbb{F}_q)$ στο σύνολο των ανάγωγων πολυωνύμων βαθμού τουλάχιστον 2. Θα παρουσιάσουμε, τώρα, κάποια από τα αποτελέσματα του [19].

Ορισμός 4.1.3. Έστω $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$. Για ένα ανάγωγο πολυώνυμο $f(X) \in \mathbb{F}_q[X]$ βαθμού $n \geq 2$ και $\theta \in \bar{\mathbb{F}}_q \setminus \mathbb{F}_q$, ορίζουμε

1. $(A \circ f)(X) \coloneqq (bX+d)^n f\left(\frac{aX+c}{bX+d}\right)$,
2. $[A] \circ f(X) \coloneqq$ το μοναδικό μονικό πολυώνυμο g(X) τέτοιο, ώστε $(A \circ f)(X) = \lambda g(X)$, για κάποιο $\lambda \in \mathbb{F}_q$,
3. $[A] \circ \theta = A \circ \theta \coloneqq \frac{d\theta - c}{-b\theta + a}$.

Τα παραπάνω ορίζουν δράσεις της $\mathrm{GL}_2(\mathbb{F}_q)$ στο σύνολο των ανάγωγων πολυωνύμων βαθμού τουλάχιστον 2 στο $\mathbb{F}_q[X]$ και στο $\bar{\mathbb{F}}_q \setminus \mathbb{F}_q$, αντίστοιχα. Μάλιστα, οι δράσεις αυτές συνδέονται μεταξύ τους, βλ. λήμμα 2.7 στο [19], ως εξής: το θ είναι ρίζα του f αν και μόνο αν το $A \circ \theta$ είναι ρίζα του $A \circ f$.

Θεώρημα 4.1.4. *Έστω $f(X) \in \mathbb{F}_q[X]$ ένα μονικό, ανάγωγο πολυώνυμο βαθμού $n \geq 2$. Τα παρακάτω είναι ισοδύναμα:*

1. $[A] \circ f = f$
2. $f \mid F_{A,r}$ *για κάποιο μη αρνητικό ακέραιο* $r < n$.

Επιπλέον, κάθε ανάγωγος παράγοντας του $F_{A,r}$ έχει βαθμό ≤ 2 ή Dk, όπου $k \mid r$ και $\mu\kappa\delta\left(\frac{r}{k}, D\right) = 1$.

Απόδειξη. Η απόδειξη βρίσκεται στα θεωρήματα 4.2 και 4.5 του [19]. □

Έστω $N_{A,r}(n) = |\{f \in \mathbb{F}_q[X] : f \text{ μονικό, ανάγωγο, με } \deg(f) = n \text{ και } f \mid F_{A,r}\}|$.

Θεώρημα 4.1.5. *Έστω $A \in GL_2(\mathbb{F}_q)$ με $ord([A]) = D \geq 2$. Τότε*

1. $N_{A,r} = 0$, *αν* $D \nmid n, n \geq 2$ *και*

2. $N_{A,r}(Dr) \sim \frac{q^r}{Dr}$, *καθώς* $r \to \infty$

Συνεπώς, κάθε μη-γραμμικός ανάγωγος παράγοντας του $F_{A,r}$ *έχει βαθμό που διαιρείται από το* D *και καθώς* $r \to \infty$, *σχεδόν όλοι έχουν βαθμό* Dr.

Απόδειξη. Η απόδειξη βρίσκεται στο θεώρημα 5.2 του [19]. □

4.2 Ιδιότητες του A^n

Παρατήρηση 4.2.1.

$$\theta^{q^{jr}} = A^j \circ \theta, \text{ για κάθε } j \in \mathbb{Z}_{\geq 0}. \tag{4.1}$$

Πράγματι, για $j = 0$, $I_2 \circ \theta = \theta$. Επίσης, το θ είναι ρίζα κάποιου ανάγωγου παράγοντα, βαθμού Dr, του πολυωνύμου $F_{A,r}$, συνεπώς

$$b\theta^{q^{r+1}} - a\theta^{q^r} + d\theta - c = 0 \Rightarrow$$

$$\theta^{q^r}(b\theta - a) = c - d\theta \Rightarrow$$

$$\theta^{q^r} = \frac{d\theta - c}{-b\theta + a}$$

άρα $\theta^{q^r} = A \circ \theta$. Έστω, τώρα, ότι η παραπάνω σχέση ισχύει για κάποιο $k \geq 1$, θα αποδείξουμε ότι ισχύει και για το $k+1$. $\theta^{q^{(k+1)r}} = (\theta^{q^{kr}})^{q^r} = (A^k \circ \theta)^{q^r} = (\frac{d_k\theta - c_k}{-b_k\theta + a_k})^{q^r} = \frac{d_k\theta^{q^r} - c_k}{-b_k\theta^{q^r} + a_k} = A^k \circ \theta^{q^r} = A^k \circ (A \circ \theta) = (A^k A) \circ \theta = A^{k+1} \circ \theta$, όπου $A^k = \begin{bmatrix} a_k & b_k \\ c_k & d_k \end{bmatrix}$.

Για την απόδειξη του θεωρήματος 4.3.1 θα χρειαστούμε τα παρακάτω τεχνικά λήμματα.

Λήμμα 4.2.2. *Έστω* $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\bar{\mathbb{F}}_q)$, *με* $\det(A) = 1$ *και* $bc \neq 0$. *Έστω, επίσης,* (a_n, b_n) και (c_n, d_n) *η πρώτη και η δεύτερη γραμμή του πίνακα* A^n, *αντίστοιχα, για κάθε* $n \in \mathbb{N}$. *Τότε, για κάθε* $0 \leq k < n < D$, *τα διανύσματα* (a_n, b_n) και (a_k, b_k) *είναι γραμμικά ανεξάρτητα υπέρ το* $\bar{\mathbb{F}}_q$. *Το ίδιο συμβαίνει και με τα διανύσματα* $(c_n, d_n), (c_k, d_k)$.

Απόδειξη. Έστω ότι ο πίνακας A είναι διαγωνοποιήσιμος με δύο διαφορετικές ιδιοτιμές, α και α^{-1}. Τότε ο A γράφεται ως

$$A = M \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix} M^{-1}, \text{ όπου } M = \begin{bmatrix} t & u \\ v & w \end{bmatrix}, \text{ είναι αντιστρέψιμος.}$$

Τότε, $M^{-1} = \frac{1}{\det M} \begin{bmatrix} w & -u \\ -v & t \end{bmatrix}$, άρα $A = \frac{1}{\det M} \begin{bmatrix} tw\alpha - vu\alpha^{-1} & -tu\alpha + tu\alpha^{-1} \\ vw\alpha - vw\alpha^{-1} & -vu\alpha + tw\alpha^{-1} \end{bmatrix}$ και συνεπώς, η υπόθεση $bc \neq 0$ μας δίνει $tu(\alpha^{-1}-\alpha)vw(\alpha-\alpha^{-1}) \neq 0$, άρα $tuvw \neq 0$. Επίσης, $A^n = M \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix}^n M^{-1} = \begin{bmatrix} \delta(tw\alpha^n - uv\alpha^{-n}) & \delta ut(\alpha^{-n} - \alpha^n) \\ \delta vw(\alpha^n - \alpha^{-n}) & \delta(wt\alpha^{-n} - uv\alpha^n) \end{bmatrix}$, $n \in \mathbb{N}$, όπου $\delta := (tw - uv)^{-1} = \det^{-1} M$. Υποθέτουμε, (για να καταλήξουμε σε αντίφαση) ότι $(a_n, b_n) = \gamma(a_k, b_k)$, για κάποια $0 \leq k < n < D$ και $\gamma \in \bar{\mathbb{F}}_q$. Τότε,

$$\begin{cases} tw\alpha^n - uv\alpha^{-n} = & \gamma(tw\alpha^k - uv\alpha^{-k}) \\ ut(\alpha^{-n} - \alpha^n) & = \gamma ut(\alpha^{-k} - \alpha^k) \end{cases}$$

το οποίο συνεπάγεται

$$\begin{cases} tw(\alpha^n - \gamma\alpha^k) = & uv(\alpha^{-n} - \gamma\alpha^{-k}) \\ \alpha^n - \gamma\alpha^k & = \alpha^{-n} - \gamma\alpha^{-k} \end{cases}$$

Αν, τώρα, $\alpha^n \neq \gamma\alpha^k$, από το παραπάνω σύστημα προκύπτει ότι $tw = uv$, το οποίο είναι άτοπο, καθώς ο πίνακας M είναι αντιστρέψιμος. Άρα $\alpha^n = \gamma\alpha^k$ και $\alpha^{-n} = \gamma\alpha^{-k}$, οπότε $\alpha^{2(n-k)} = 1$, δηλαδή $\mathrm{ord}(\alpha) \mid 2(n-k)$. Αν η $\mathrm{ord}(\alpha)$ είναι άρτιος αριθμός, τότε $2D = \mathrm{ord}(\alpha)$ και $0 < 2(n-k) < 2D$ ↯. Αν η $\mathrm{ord}(\alpha)$ είναι περιττός αριθμός, τότε $\mathrm{ord}(\alpha) \mid (n-k)$, $D = \mathrm{ord}(\alpha)$ και $0 < n-k < D$ ↯. Συνεπώς, τα (a_n, b_n) και (a_k, b_k) είναι γραμμικά ανεξάρτητα υπέρ το $\bar{\mathbb{F}}_q$. Αντίστοιχα, αποδεικνύεται η γραμμική ανεξαρτησία των (c_n, d_n) και (c_k, d_k) υπέρ το $\bar{\mathbb{F}}_q$ για $0 \leq k < n < D$.
Έστω, τώρα, ότι ο πίνακας A δεν διαγωνοποιείται. Τότε θα είναι της μορφής $A = M^{-1} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} M$, όπου $M = \begin{bmatrix} t & u \\ v & w \end{bmatrix}$, αντιστρέψιμος. Επίσης, $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix}$, άρα $A^n = \begin{bmatrix} 1 - n\delta tu & -n\delta u^2 \\ n\delta t^2 & 1 + n\delta tu \end{bmatrix}$, όπου $n \in \mathbb{N}$ και $\delta = \det^{-1} M$. Κάνοντας αντίστοιχη διαδικασία με την προηγούμενη περίπτωση, έχουμε το επιθυμητό αποτέλεσμα. □

Λήμμα 4.2.3. *Έστω* $A = \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} \in GL_2(\bar{\mathbb{F}}_q)$ *με* $c \neq 0$ *και* (c_n, d_n) *όπως ορίσαμε στο προηγούμενο λήμμα. Τότε, για κάθε* $0 \leq k < n < D$, *τα διανύσματα* (c_n, d_n) *και* (c_k, d_k) *είναι γραμμικά ανεξάρτητα υπέρ το* $\bar{\mathbb{F}}_q$.

Απόδειξη. Επαγωγικά, έχουμε ότι $A^n = \begin{bmatrix} a^n & 0 \\ c(a^{n-1}+a^{n-2}d+\cdots+ad^{n-2}+d^{n-1}) & d^n \end{bmatrix}$

Δηλαδή, $A^n = \begin{cases} \begin{bmatrix} a^n & 0 \\ c\frac{a^n-d^n}{a-d} & d^n \end{bmatrix} & \text{εάν } a \neq d \\ \begin{bmatrix} a^n & 0 \\ nca^{n-1} & a^n \end{bmatrix} & \text{εάν } a = d \end{cases}$. Έστω, τώρα, ότι $(c_n, d_n) = \gamma(c_k, d_k)$ για κάποιο $0 \leq k < n < D$ και $\gamma \in \bar{\mathbb{F}}_q$. Αν $a \neq d$ προκύπτει ότι $d^n = \gamma d^k$ και $c\frac{a^n-d^n}{a-d} = \gamma c\frac{a^k-d^k}{a-d}$, δηλαδή ότι $\gamma = d^{n-k}$ και $c\frac{a^n-d^n}{a-d} = cd^{n-k}\frac{a^k-d^k}{a-d}$. Αφού $c \neq 0$, έχουμε $a^n - d^n = d^{n-k}a^k - d^n$, άρα $a^{n-k} = d^{n-k}$. Όμως, τότε $A^{n-k} = \begin{bmatrix} a^{n-k} & 0 \\ c\frac{a^{n-k}-d^{n-k}}{a-d} & d^{n-k} \end{bmatrix} = \begin{bmatrix} a^{n-k} & 0 \\ 0 & a^{n-k} \end{bmatrix} = a^{n-k}I_2$ και $0 < n-k < D$ ↯.
Ενώ αν $a = d$, προκύπτει ότι $nca^{n-1} = \gamma kca^{k-1}$ και $a^n = \gamma a^k$, άρα $\gamma = a^{n-k}$ και $na^{n-1} = ka^{n-k}a^{k-1}$, δηλαδή $n = k$ ↯. □

Παρατήρηση 4.2.4. Όταν ο πίνακας A είναι τριγωνικός (για παράδειγμα $A = \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\bar{\mathbb{F}}_q)$) και αν $A \neq I$, τότε $\mathrm{ord}(A) = \begin{cases} \mathrm{ord}\left(\frac{a}{d}\right) & \text{εάν } a \neq d \\ \mathrm{p} & \text{εάν } a = d \text{ και } c \neq 0. \end{cases}$

Λήμμα 4.2.5. *Έστω $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\bar{\mathbb{F}}_q)$ και (a_n, b_n) και (c_n, d_n) η πρώτη και η δεύτερη γραμμή του πίνακα A^n, αντίστοιχα, για κάθε $n \in \mathbb{N}$. Έστω, επίσης, ότι $(c_n, d_n) = \gamma(a_n, b_n)$ για κάποια $0 \leq k, n < D$ και $\gamma \in \bar{\mathbb{F}}_q$. Τότε, αν θεωρήσουμε $g = n - k$, έχουμε*

$$(c_i, d_i) = \epsilon_i \gamma(a_{i-g}, b_{i-g}), 0 \leq i \leq D-1,$$

όπου $\epsilon_i \in \{-1, 1\}$ όπου οι δείκτες είναι υπολογισμένοι mod D.

Απόδειξη. Εξ ορισμού, $(a_k, b_k) = (1,0)A^k$ και $(c_n, d_n) = (0,1)A^n$. Έτσι, $(c_n, d_n) = \gamma(a_n, b_n), \gamma \in \bar{\mathbb{F}}_q \Rightarrow (0,1)A^n = \gamma(1,0)A^k \overset{A \in \mathrm{GL}_2(\bar{\mathbb{F}}_q)}{\Longrightarrow} (0,1)A^g = \gamma(1,0)$, όπου $g = n-k$. Οπότε, $(0,1)A^{g+i} = \gamma(1,0)A^i$, δηλαδή

$$(c_{g+i}, d_{g+i}) = \gamma(a_i, b_i), \forall i \geq 0. \tag{4.2}$$

Έστω ότι $k < n$. Από την παραπάνω σχέση, προκύπτουν

$$(c_{g+i}, d_{g+i}) = \gamma(a_i, b_i),\ i = 0,\ 1, \ldots, D-g-1$$

και

$$(c_{D+i}, d_{D+i}) = \gamma(a_{D-g+i}, b_{D-g+i}),\ i = 0,\ 1, \ldots, g-1.$$

Αφού $A^D = (-1)^{D+1} I_2$, έχουμε $(c_{D+i}, d_{D+i}) = (0,1)A^{D+i} = (-1)^{D+1}(c_i, d_i)$, άρα

$$(c_i, d_i) = \gamma(-1)^{D-1}(a_{D-g+i}, b_{D-g+i}),\ i = 0, 1, \ldots, g-1,$$

$$(c_i, d_i) = \gamma(a_{i-g}, b_{i-g}),\ i = g, \ldots, D-1.$$

Η περίπτωση όπου $k > n$ αποδεικνύεται ομοίως, ενώ η περίπτωση όπου $k = n$ είναι αδύνατη καθώς τα (a_k, b_k) και (c_k, d_k) είναι γραμμικά ανεξάρτητα. □

Παρατήρηση 4.2.6. Εάν ρ είναι ο μικρότερος πρώτος παράγοντας του D και το g είναι όπως στο Λήμμα 4.2.5, είναι προφανές ότι

$$\text{μκδ}(g, D) \leq \frac{D}{\rho}.$$

Το παραπάνω φράγμα δεν επιδέχεται βελτίωση, καθώς η ισότητα μπορεί να ισχύει. Για παράδειγμα, αν το q δεν είναι δύναμη του ρ, $\beta \in \mathbb{F}_q$ μια πρωταρχική $2\rho n$ ρίζα της μονάδας και $\alpha = \beta^n$, θεωρούμε τους πίνακες $M = \begin{bmatrix} 1 & 1 \\ \alpha & \alpha^{-1} \end{bmatrix}$ και $A = M^{-1} \begin{bmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{bmatrix} M$. Παρατηρούμε ότι $\text{ord}(A) = \rho n$ και εάν g είναι ο ελάχιστος θετικός ακέραιος τέτοιος, ώστε

$$\beta^{2g} = \frac{uv}{tw} = \frac{\alpha}{\alpha^{-1}} = \beta^{2n},$$

τότε $g = n = \frac{D}{\rho}$, όπου τα t, u, v, w ορίζονται όπως στο Λήμμα 4.2.2.

Για την απόδειξη του βασικού μας θεωρήματος θα χρησιμοποιήσουμε ένα γενικό φράγμα (που δεν εξαρτάται από το ρ), $\text{μκδ}(g, D) \leq \lfloor \frac{D}{2} \rfloor$.

4.3 Ένα Ισχυρό Φράγμα της Τάξης των Generic Root

Υπενθυμίζουμε ότι $F_{A,r}(X) = bX^{q^r+1} - aX^{q^r} + dX - c \in \mathbb{F}_q(X)$, όπου $\left[\ \text{A}\ \right] = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{PGL}_2(\mathbb{F}_q)$ και $r \geq 0$. Στόχος μας είναι, μέσω του παραπάνω πολυωνύμου να βρούμε μια επέκταση και ένα στοιχείο μεγάλης τάξης στην επέκταση αυτή.
Θα διατυπώσουμε, τώρα, το θεώρημα το οποίο μας δίνει το ζητούμενο φράγμα και θα το αποδείξουμε στο τέλος της ενότητας αυτής.

Θεώρημα 4.3.1. *Έστω $A \in GL_2(\mathbb{F}_q), [A] \neq [I]$ και θ generic root του $F_{A,r}$ δηλαδή $\theta \in \bar{\mathbb{F}}_q$ και $\dim_{\mathbb{F}_q} \mathbb{F}_q[\theta] = Dr$, με $D = ord([A])$ και $r > 2$. Η πολλαπλασιαστική τάξη του θ είναι κάτω φραγμένη από*

$$\frac{\sqrt{2}}{\pi D}\sqrt{\frac{r}{r+1}}\left(\frac{4(r+1)^{r+1}}{r^r}\right)^{\frac{D}{2}} e^{-\frac{1}{12D}\frac{5r^2+5r+2}{r^2+r}-\frac{1}{144D^2}}, \tag{4.3}$$

στην περίπτωση όπου ο A είναι τριγωνικός πίνακας και

$$\frac{1}{\sqrt{2}\pi D}\sqrt{\frac{r-2}{r+2}}\left(\frac{(r+2)^{r+2}}{(r-2)^{r-2}}\right)^{\frac{D}{4}} e^{-\frac{5}{24D}\frac{r^2+4}{r^2-4}-\frac{1}{144D^2}}, \tag{4.4}$$

αλλιώς.

Παρατήρηση 4.3.2. Για κάθε $\epsilon > 0$ και $r > R_e$, το κάτω φράγμα 4.4 είναι μεγαλύτερο από

$$\frac{1}{\sqrt{2}\pi D}((e-\epsilon)(r+2))^D$$

και το κάτω φράγμα 4.3 είναι μεγαλύτερο από

$$\frac{\sqrt{2}}{\pi D}(2(e-\epsilon)(r+1))^{D/2}.$$

Παρατηρούμε ότι, ενώ το θ είναι μια "generic root" ενός ανάγωγου παράγοντα f του $F_{A,r}$, για την κατασκευή του $\left(\mathbb{F}_q[X]/f(X)\right)^*$ χρειαζόμαστε να γνωρίζουμε το πολυώνυμο $f(X)$. Είναι γνωστό ότι για την παραγοντοποίηση του $F_{A,r}$ χρειαζόμαστε πολυωνυμικό χρόνο ως προς το q^r. Θα θέλαμε να έχουμε έναν αλγόριθμο που να κατασκευάζει το σώμα $\mathbb{F}_{q^{rD}}$ σε πολυωνυμικό χρόνο ως προς τα r, D και $\log q$. Σύμφωνα με την παρατήρηση 4.2.4, η D είναι ίδιας τάξης μεγέθους με το q, συνεπώς $D = \Omega(q^\epsilon)$, για κάθε $\epsilon > 0$, και για μικρές τιμές του r (ιδιαιτέρως για $r = 1$), η παραγοντοποίηση του $F_{A,r}$ χρειάζεται πολυωνυμικό χρόνο ως προς D.
Το βασικό μας αποτέλεσμα είναι συνέπεια του παρακάτω θεωρήματος.

Θεώρημα 4.3.3. *Έστω $A \in GL_2(\mathbb{F}_q), A \neq I_2$ και θ μια generic root του $F_{A,r}$. Τότε η απεικόνιση*

$$\Lambda : I_{s,t,m} \longrightarrow \langle\theta\rangle$$
$$(u_0, \dots u_{D-1}) \longmapsto \prod_{j=0}^{D-1} \theta^{u_j q^{jr}}$$

είναι ένα προς ένα στις παρακάτω περιπτώσεις:

1. *ο A είναι τριγωνικός πίνακας, $m = 0$ και $s + t < Dr$.*
2. *ο A δεν είναι τριγωνικός πίνακας, τα $(0,1)A^i$ και $(1,0)A^j$ είναι γραμμικά ανεξάρτητα για κάθε i, j, $m = 0$ και $s + t < \frac{Dr}{2}$.*

3. ο A δεν είναι τριγωνικός πίνακας, υπάρχει $0 < g < D$ τέτοιο, ώστε τα $(1,0)$ και $(0,1)A^g$ να είναι γραμμικά εξαρτημένα, $m = \text{μκδ}(g, D)$ και $s + t < \frac{Dr}{2}$.

Απόδειξη. Είναι προφανές ότι $I_{s,t,g} \subset I_{s,t}$ για κάθε $1 \leq g \leq D$. Για το $(u_0, \dots u_{D-1}) \in I_{s,t}$, υπολογίζουμε

$$\Lambda(u_0, \dots u_{D-1}) = \prod_{j=0}^{D-1} \left(\theta^{q^{jr}}\right)^{u_j} = \prod_{j=0}^{D-1} \left(A^j \circ \theta\right)^{u_j}.$$

Για κάθε πίνακα B στην κλάση $[A] \in \mathrm{PGL}_2(\bar{\mathbb{F}}_q)$ έχουμε $A^j \circ \theta = B^j \circ \theta$, επομένως μπορούμε να αντικαταστήσουμε τον πίνακα A με τον $\delta^{-1}A$, όπου $\delta^2 = \det(A)$. Αυτό μας επιτρέπει να δουλέψουμε για πίνακες $A \in \mathrm{GL}_2(\mathbb{F}_{q^2})$, με $\det(A) = 1$. Έχουμε,

$$\Lambda(u_0, \dots u_{D-1}) = \prod_{j=0}^{D-1} \left(A^j \circ \theta\right)^{u_j} = \prod_{j=0}^{D-1} \left(\frac{d_j\theta - c_j}{-b_j\theta + a_j}\right)^{u_j}.$$

Έστω, τώρα, $(u_0, \dots u_{D-1}), (v_0, \dots v_{D-1}) \in Is, t$ με $\Lambda(u_0, \dots u_{D-1}) = \Lambda(v_0, \dots v_{D-1})$. Τότε, έχουμε

$$\prod_{\substack{0\leq j\leq D\\ u_j>0}} \left(d_j\theta - c_j\right)^{u_j} \prod_{\substack{0\leq j\leq D\\ u_j<0}} \left(-b_j\theta + a_j\right)^{-u_j} \prod_{\substack{0\leq j\leq D\\ v_j<0}} \left(d_j\theta - c_j\right)^{-v_j} \prod_{\substack{0\leq j\leq D\\ v_j>0}} \left(-b_j\theta + a_j\right)^{v_j}$$

$$= \prod_{\substack{0\leq j\leq D\\ v_j>0}} \left(d_j\theta - c_j\right)^{v_j} \prod_{\substack{0\leq j\leq D\\ v_j<0}} \left(-b_j\theta + a_j\right)^{-v_j} \prod_{\substack{0\leq j\leq D\\ u_j<0}} \left(d_j\theta - c_j\right)^{-u_j} \prod_{\substack{0\leq j\leq D\\ u_j>0}} \left(-b_j\theta + a_j\right)^{u_j}.$$

Άρα, το θ είναι ρίζα του $F(X) - G(X)$, όπου

$$F(X) = \prod_{\substack{0\leq j\leq D\\ u_j>0}} \left(d_jX - c_j\right)^{u_j} \prod_{\substack{0\leq j\leq D\\ u_j<0}} \left(-b_jX + a_j\right)^{-u_j} \prod_{\substack{0\leq j\leq D\\ v_j<0}} \left(d_jX - c_j\right)^{-v_j} \prod_{\substack{0\leq j\leq D\\ v_j>0}} \left(-b_jX + a_j\right)^{v_j}$$

και

$$G(X) = \prod_{\substack{0\leq j\leq D\\ v_j>0}} \left(d_jX - c_j\right)^{v_j} \prod_{\substack{0\leq j\leq D\\ v_j<0}} \left(-b_jX + a_j\right)^{-v_j} \prod_{\substack{0\leq j\leq D\\ u_j<0}} \left(d_jX - c_j\right)^{-u_j} \prod_{\substack{0\leq j\leq D\\ u_j>0}} \left(-b_jX + a_j\right)^{u_j}.$$

Θα αποδείξουμε, τώρα, το θεώρημα για κάθε μία από τις τρεις περιπτώσεις.
Περίπτωση 1: έστω ότι ο A είναι τριγωνικός πίνακας. Παρατηρούμε πως αν το θ είναι ρίζα του $F_{A,r}$, τότε το θ^{-1} είναι ρίζα του πολυωνύμου $F_{B,r}$, όπου $B = \begin{bmatrix} d & c \\ b & a \end{bmatrix}$. Πράγματι, $F_{B,r}(\theta^{-1}) = 0 \iff c\theta^{-(q^r+1)} - d\theta^{-q^r} + a\theta^{-1} - b = 0 \iff c - d\theta + a\theta^{q^r} - b\theta^{q^r+1} = 0 \iff F_{A,r}(\theta) = 0$. Έτσι, μπορούμε να υποθέσουμε χωρίς

βλάβη της γενικότητας, ότι ο A είναι κάτω τριγωνικός (αφού αν ήταν άνω τριγωνικός, αντί για το θ θα δουλεύαμε με το θ^{-1} και συνεπώς με τον πίνακα B που θα είναι κάτω τριγωνικός). Έτσι, $b_j = 0$ για κάθε j και οι βαθμοί των πολυωνύμων $F(X)$ και $G(X)$ είναι

$$\sum_{u_j \geq 0} u_j - \sum_{v_j \leq 0} v_j \leq s+t \text{ και } \sum_{v_j \geq 0} v_j - \sum_{u_j \leq 0} u_j \leq s+t,$$

αντίστοιχα. Αφού $\deg(F(X)) \leq s+t < Dr$, $\deg(G(X)) \leq s+t < Dr$ και το $F(X) - G(X)$ διαιρείται από το ελάχιστο πολυώνυμο του θ, το οποίο έχει βαθμό Dr, προκύπτει ότι $F(X) = G(X)$. Από το 4.2.3, τα διώνυμα $d_jX - c_j$, για $0 \leq j \leq D-1$, είναι ανά δύο διακριτά. Έτσι, από τη μοναδικότητα ανάλυσης στο $\mathbb{F}_q[X]$ έπεται ότι $(u_0, \dots u_{D-1}) = (v_0, \dots v_{D-1})$, άρα η Λ είναι ένα προς ένα.

Περίπτωση 2: για την περίπτωση αυτή, η απόδειξη είναι ανάλογη της πρώτης περίπτωσης, όμως χρησιμοποιούμε το λήμμα 4.2.2 αντί το λήμμα 4.2.3 και έχουμε ότι τα διώνυμα $-b_jX + a_j$, για $0 \leq j \leq D-1$ είναι ανά δύο διακριτά, καθώς και τα $d_jX - c_j$, για $0 \leq j \leq D-1$, είναι ανά δύο διακριτά. Τέλος, τα διώνυμα $-b_jX + a_j$ και $d_jX - c_j$, για $0 \leq j \leq D-1$, είναι διακριτά από την υπόθεση της περίπτωσης αυτής.

Περίπτωση 3: έστω ότι υπάρχουν $0 \leq k, n < D$ τέτοια, ώστε $(c_n, d_n) = \gamma(a_k, b_k)$, για κάποιο $\gamma \in \mathbb{F}_{q^2}^*$. Ορίζουμε $g = n-k$ και $m = \text{μκδ}(g, D)$. Για να αποδείξουμε ότι η Λ είναι ένα προς ένα θα την περιορίσουμε στο $I_{s,t,m}$. Μάλιστα, αποδεικνύεται ότι ο περιορισμός αυτός είναι απαραίτητος. Από το λήμμα 4.2.5 έχουμε

$$d_jX - c_j = \epsilon_j\gamma(b_{j-g}X - a_{j-g}), \text{ για } 0 \leq j \leq D-1$$

και συνεπώς

$$F(X) = \epsilon_F\gamma^{e_F} \prod_{u_j<0} \left(b_jX - a_j\right)^{-u_j} \prod_{v_j>0} \left(b_jX - a_j\right)^{v_j} \prod_{u_j>0} \left(b_{j-g}X - a_{j-g}\right)^{u_j} \prod_{v_j<0} \left(b_{j-g}X - a_{j-g}\right)^{-v_j}$$

και

$$G(X) = \epsilon_G\gamma^{e_G} \prod_{v_j<0} \left(b_jX - a_j\right)^{-v_j} \prod_{u_j>0} \left(b_jX - a_j\right)^{u_j} \prod_{v_j>0} \left(b_{j-g}X - a_{j-g}\right)^{v_j} \prod_{u_j<0} \left(b_{j-g}X - a_{j-g}\right)^{-u_j},$$

όπου $\epsilon_F, \epsilon_G \in \{-1, 1\}$, $e_F = \sum_{u_j>0} u_j - \sum_{v_j<0} v_j$ και $e_G = \sum_{v_j>0} v_j - \sum_{u_j<0} u_j$. Από τον ορισμό του $I_{s,t,m}$ έχουμε ότι $\deg(F(X)), \deg(G(X)) < Dr$ και κατά συνέπεια $F(X) = G(X)$. Έτσι,

$$\epsilon\gamma^{e_G - e_F} \prod_{j=0}^{D-1} (b_jX - a_j)^{u_j - u_{j+g}} = \prod_{j=0}^{D-1} (b_jX - a_j)^{v_j - v_{j+g}},$$

όπου $\epsilon \in \{-1, 1\}$. Ανάλογα με τις προηγούμενες περιπτώσεις, από το λήμμα 4.2.2, έχουμε

$$u_j - u_{j+g} = v_j - v_{j+g}, 0 \leq j \leq D-1.$$

Ορίζουμε, τώρα $x_j = u_j - v_j, 0 \leq j < D$. Τότε έχουμε $x_{j+g} = x_j$ για $j \geq 0$, όπου οι δείκτες είναι υπολογισμένοι mod D. Έστω, τώρα, $J = \{\bar{j} : x_j = 0\}$. Εφόσον $m = \text{μκδ}(g, D)$, έχουμε $\{\bar{0}, \ldots, \overline{\text{μκδ}(g, D) - 1}\} \subseteq J$ και $x_{j+g} = x_j$ για $j \geq 0$, άρα και $\{\overline{a + ig} : 0 \leq a < \text{μκδ}(g, D), i \geq 0\} \subseteq J$. Για να έχουμε ότι $(u_0, \ldots u_{D-1}) = (v_0, \ldots v_{D-1})$ και κατά συνέπεια ότι η Λ είναι ένα προς ένα αρκεί να δείξουμε ότι $x_i = 0$, για κάθε $i = 0, \ldots, D-1$, δηλαδή ότι $J = \mathbb{Z}_D$. Είναι προφανές ότι $J \subseteq \mathbb{Z}_D$. Επιπλέον, αν $0 \leq j < D$, τότε η ισοτιμία $j \equiv a + ig \pmod{D}$ έχει λύση ως προς i αν και μόνο αν $\text{μκδ}(g, D) \mid j - a$. Συνεπώς, για να έχουμε $\mathbb{Z}_D \subseteq J$, αρκεί ισχύει $j - a \equiv 0 \pmod{\text{μκδ}(g, D)}$ για κάποιο $0 \leq a < \text{μκδ}(g, D)$. Επιλέγουμε το $a \equiv j \pmod{\text{μκδ}(g, D)}$.

□

Είμαστε, πλέον, σε θέση να αποδείξουμε το θεώρημα 4.3.1.

Απόδειξη. Έστω $A \in GL_2(\mathbb{F}_q), [A] \neq [I]$ και θ generic root του $F_{A,r}$. Έστω, επίσης, ότι ο A είναι τριγωνικός. Τότε, από την περίπτωση (1) του θεωρήματος 4.3.3, για $m = 0, s = t = \lfloor \frac{Dr}{2} \rfloor$ και χρησιμοποιώντας το φράγμα (3) της πρότασης 2.2.3 έχουμε έχουμε ότι

$$|\langle\theta\rangle| \geq |I_{\lfloor \frac{Dr}{2} \rfloor, \lfloor \frac{Dr}{2} \rfloor, 0}| \overset{0 < \lfloor \frac{D}{2} \rfloor}{\geq} |I_{\lfloor \frac{Dr}{2} \rfloor, \lfloor \frac{Dr}{2} \rfloor, \lfloor \frac{D}{2} \rfloor}| >$$

$$> \frac{\sqrt{2}}{\pi D} \sqrt{\frac{r}{r+1}} \left(\frac{4(r+1)^{r+1}}{r^r} \right)^{\frac{D}{2}} e^{-\frac{1}{12D} \frac{5r^2+5r+2}{r^2+r} - \frac{1}{144D^2}}.$$

Διαφορετικά, εμπίπτουμε στις περιπτώσεις (2) και (3) του θεωρήματος 4.3.3 όπου μπορούμε να επιλέξουμε $s = t = \lfloor \frac{Dr}{4} \rfloor$ και $m = 0$. Έτσι,

$$|\langle\theta\rangle| \geq |I_{\lfloor \frac{Dr}{4} \rfloor, \lfloor \frac{Dr}{4} \rfloor, 0}| \overset{2.2.3}{>} \frac{1}{\sqrt{2}\pi D} \sqrt{\frac{r-2}{r+2}} \left(\frac{(r+2)^{r+2}}{(r-2)^{r-2}} \right)^{\frac{D}{4}} e^{-\frac{5}{24D} \frac{r^2+4}{r^2-4} - \frac{1}{144D^2}}.$$

□

Βιβλιογραφία

[1] Agrawal, M., Kayal, N., Saxena, N., *Primes is in P*, Ann. of Math., (2) 160:781-793, 2004.

[2] Ahmadi, O., Shparlinski, I., Voloch, J. F.., *Multiplicative order of Gauss periods*, Int. J. Number Theory, 6 877–882, 2010.

[3] Bach, E., *Comments on search procedures for primitive roots*, Math. Comp., 66 no.220 1719–1727, 1997.

[4] Cheng, Q., *Constructing finite field extensions with large order elements.*, SIAM J. Discrete Math, 213:726-730, 2007.

[5] Gao, S., *Elements of provable high orders in finite fields*, Proc. Amer. Math. Soc., 127:1615-1623, 1999.

[6] Garefalakis, T., *On the action of* $GL(2, q)$ *on irriducible polynomials over* $\mathbb{F}_q$, J. Pure and Appl. Algebra, 215:1835-1843, 2011.

[7] Gathen, J., Shparlinski, I.E., *Orders of Gauss periods in finite fields*, Appl. Algebra in Engin. Commun. and Compo, 9 15–24, 1998.

[8] Gathen, J., Shparlinski, I.E., *Constructing elements of large order in finite fields. Applied algebra, algebraic algoriths and error-correcting codes*, Lecture Notes in Comput. Sci., 1719 404–409, 1999.

[9] Lidl, R., Niederreiter, H., *Finite Fields*, Encyclopedia of Mathematics and Its Applications, Vol. 20, Addison-Wesley, 1983.

[10] Brochero Martinez, Theodoulos Garefalakis, Lucas Reis, Eleni Tzanaki, *On the multiplicative order of the roots of* $bX^{q^r+1} - aX^{q^r} + dX - c$, Finite Fields and Applications, Vol. 47, 33-45, 2017.

[11] F.E. Brochero Martinez, Lucas Reis, *Elements of high order in Artin-Schreier extensions of finite fields* $\mathbb{F}_q$. Finite Fields Appl., 41:24-33, 2016.

[12] Popovych, R., *Elements of high order in finite fields of the form* $\mathbb{F}_q[x]/\Phi_r(x)$, Finite Fields Appl., 18:700–710, 2012.

[13] Popovych, R., *Elements of high order in finite fields of the form* $\mathbb{F}_q[x]/(x^m-a)$, Finite Fields Appl., 19:86–92, 2013.

[14] Popovych, R., *Sharpening of the explicit lower bounds for the order of elements in finite field extensions based on cyclotomic polynomials.* , Ukrainian Math. J. 66 916–927, 2014.

[15] Popovych, R., *Elements of high order in Artin-Schreier extensions of finite fields*, Mat. Stud., 39 115–118, 2013.

[16] Robbins, Herbert, *A Remark on Stirling's Formula*, The American Mathematical Monthly, 62 (1): 26–29 pp, 1955.

[17] Sasvari, Z., *Inequalities for binomial coefficients*, J. Math Anal. Appl. 236:223-226, 1999.

[18] Shoup, V., *Searching for primitive roots in finite fields*, Math. Comp., 58 no. 197, 369-380, 1992.

[19] Stichtenoth, H., Topuzoglu, A., *Factorization of a class of polynomials over finite fields*, Finite Fields Appl., 18:108-122, 2012.

[20] Voloch, J. F., *On some subgroups of the multiplicative group of finite rings*, J. Theor. Nombres Bordeaux, 16 233–239, 2004.