ΒΕΛΤΙΣΤΕΣ ΚΑΝΟΝΙΚΕΣ ΒΑΣΕΙΣ ΕΠΕΚΤΑΣΕΩΝ GALOIS

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Αλέξανδρος Γ. Συγκελάκης

Επιβλέπων Καθηγητής

Θεόδουλος Γαρεφαλάκης

Μεταπτυχιακο Προγραμμα

Τμημα Μαθηματικων

Πανεπιστημιο Κρητης

Ηρακλειο

ΑΠΡΙΛΙΟΣ 2008

Η μεταπτυχιακή αυτή εργασία κατατέθηκε στο Τμήμα Μαθηματικών της Σχολής Θετικών και Τεχνολογικών Επιστημών του Πανεπιστημίου Κρήτης τον Απρίλιο του 2008.
Την επιτροπή αξιολόγησης αποτέλεσαν οι:
Θεόδουλος Γαρεφαλάκης
Αλέξανδρος Κουβιδάκης
Νικόλαος Τζανάκης.

Έκδοση 1.02

Στους γονείς μου και στην Ανάστα

Περιεχόμενα

Συμβολισμοί **v**

Πρόλογος **vi**

1 Εισαγωγή **1**

1.1 Πρώτα σώματα 1

1.2 Κανονικές Βάσεις 7

1.2.1 Ύπαρξη κανονικής βάσης σε επεκτάσεις Galois . 7

1.2.2 Κανονική βάση σε πεπερασμένα σώματα 11

1.3 Δυϊκή Βάση Επέκτασης 20

1.4 Αριθμητική σε πεπερασμένα σώματα 27

2 Χαρακτηρισμός βέλτιστων κανονικών βάσεων Πεπερασμένων επεκτάσεων Galois **38**

2.1 Βέλτιστες κανονικές Βάσεις 38

2.2 Τρείς χρήσιμες σχέσεις 46

2.3 Κεντρικό Θεώρημα 55

3 Βέλτιστες κανονικές βάσεις Πεπερασμένων Σωμάτων **69**

3.1 Τύπου I 69

3.2 Τύπου II 70

3.3 Επίλογος 75

4 Παράρτημα **79**

Βιβλιογραφία **81**

Ευρετήριο Όρων **83**

Συμβολισμοί

L/K = Επέκταση L πάνω από το K.

$\mathbb{F}_p$ = Σώμα με p στοιχεία, p πρώτος

$\mathbb{F}_{q^n}$ = Σώμα με q στοιχεία, q πρώτος και n φυσικός.

$\mathbb{F}^*$ = Η πολλαπλασιαστική ομάδα των μη μηδενικών στοιχείων του σώματος $\mathbb{F}$.

$\mathbb{F}[X]$ = Ο δακτύλιος των πολυωνύμων με συντελεστές στο σώμα $\mathbb{F}$.

$H \leq G$ = H υποομάδα της G.

$H \trianglelefteq G$ = H κανονική υποομάδα της G.

$\mathrm{char}\mathbb{F}$ = Χαρακτηριστική του σώματος $\mathbb{F}$.

$\mathrm{Tr}\,(\alpha)$ = Ίχνος του στοιχείου α.

$\min(\alpha, \mathbb{F}_q)$ = Το ελάχιστο πολυώνυμο του στοιχείου πάνω από το σώμα $\mathbb{F}_q$.

$\mathrm{ord}_p\,(k)$ = Η τάξη του $k \mod p$.

id = Ο ταυτοτικός αυτομορφισμός της ομάδας $Galois$.

$\sigma_i\,|_K$ = Ο περιορισμός του αυτομορφισμού σ, στο σύνολο K.

$\sharp\{...\}$ = Πληθικός αριθμός του συνόλου $\{...\}$.

$\mathrm{Irr}\,(\alpha, K)$ = Το ελάχιστο πολυώνυμο του α πάνω από το K.

$G(K/L)$ = Η ομάδα των αυτομορφισμών της επέκτασης K/L.

$\deg p(x)$ = Ο βαθμός του πολυωνύμου $p(x)$.

$\det(A)$ = Η ορίζουσα του πίνακα A.

I_n = Ο μοναδιαίος $n \times n$ πίνακας.

$a|b$ = Το a διαιρεί το b.

Πρόλογος

Το ενδιαφέρον για τις κανονικές βάσεις πάνω από πεπερασμένα σώματα και γενικά πάνω από επεκτάσεις Galois προήλθε κυρίως από τις πρακτικές εφαρμογές. Υπάρχει εκτενής βιβλιογραφία που ασχολείται με διάφορες ιδιότητες των κανονικών βάσεων. Το πλεονέκτημα της χρήσης τους για να αναπαραστήσουμε πεπερασμένα σώματα, σημειώθηκε για πρώτη φορά από τον Hensel το 1888. Με την εισαγωγή των βέλτιστων κανονικών βάσεων, προβλήματα που βρίσκουν εφαρμογή σε διάφορα κρυπτογραφικά συστήματα μπορούν πλέον να λυθούν με λιγότερο υπολογιστικό κόστος αφού οι πράξεις οι οποίες γίνονται όταν χρησιμοποιούνται βέλτιστες κανονικές βάσεις, είναι πολύ λιγότερες. Στην εργασία αυτή υπάρχει ο πλήρης χαρακτηρισμός των βέλτιστων κανονικών βάσεων πεπερασμένων σωμάτων και πεπερασμένων επεκτάσεων Galois.

Το **Πρώτο κεφάλαιο** ασχολείται με κάποιες εισαγωγικές έννοιες που αφορούν τις κανονικές βάσεις καθώς επίσης και την απόδειξη ύπαρξης κανονικών βάσεων σε (πεπερασμένες) επεκτάσεις Galois καθώς και σε πεπερασμένα σώματα. Επίσης, περιέχονται παραδείγματα τέτοιων κανονικών βάσεων, αναφέρεται η έννοια της δυϊκής βάσης μίας βάσης (κύρια έννοια για τη συνέχεια) και κάποιες βοηθητικές προτάσεις που την αφορούν. Το κεφάλαιο αυτό τελειώνει με τον τρόπο με τον οποίο γίνεται αριθμητική σε πεπερασμένα σώματα, με τη χρήση κανονικών βάσεων, τις δυσκολίες τις οποίες αντιμετωπίζουμε (κυρίως στον πολλαπλασιασμό), το υπολογιστικό «κόστος» κατά τη χρήση κανονικών βάσεων, αναφέρονται παραδείγματα και έτσι προετοιμάζεται με φυσιολογικό τρόπο το επόμενο κεφάλαιο.

Το **Δεύτερο Κεφάλαιο** περιέχει τον ορισμό των βέλτιστων κανονικών βάσεων καθώς επίσης και κάποιες βοηθητικές προτάσεις των οποίων γίνεται χρήση για την απόδειξη του Κεντρικού Θεωρήματος με το οποίο

χαρακτηρίζονται οι βέλτιστες κανονικές βάσεις τυχαίας (πεπερασμένης) επέκτασης Galois με την οποία κλείνει και το κεφάλαιο.

Η Μεταπτυχιακή εργασία, τελειώνει με το **Τρίτο Κεφάλαιο** το οποίο αναφέρεται στο ισοδύναμο του Κεντρικού Θεωρήματος στην περίπτωση των πεπερασμένων σωμάτων, την απόδειξη της ισοδυναμίας αυτής μέσω του κεντρικού θεωρήματος που αποδεικνύουμε στην εργασία και την διάκριση των βέλτιστων κανονικών βάσεων πεπερασμένων σωμάτων σε Τύπου Ι και Τύπου ΙΙ.

Θα ήθελα σε αυτό το σημείο να ευχαριστήσω τον επιβλέποντα καθηγητή μου Θεόδουλο Γαρεφαλάκη για τη συνολική συμβολή του και την καθοδήγησή του καθ' όλη τη διάρκεια της μελέτης και συγγραφής της μεταπτυχιακής μου εργασίας, αλλά και όλους τους καθηγητές που έτυχε να μου κάνουν μάθημα στο μεταπτυχιακό πρόγραμμα από τους οποίους έμαθα τόσα πολλά. Θα ήταν παράλειψή μου να μην ευχαριστήσω ονομαστικά τους Καθηγητές του Πανεπιστημίου Κρήτης Ν. Τζανάκη και Μ. Λάμπρου, κυρίως γιατί αποτελούν για μένα το πιο καλό παράδειγμα ΔΑΣΚΑΛΟΥ, το πρότυπο ενός σωστού επιστήμονα και ανθρώπου αλλά και γιατί όλες τις φορές η συζήτηση μαζί τους ήταν καρποφόρα.

Τέλος, νιώθω την ανάγκη να ευχαριστήσω την οικογένειά μου και ιδιαίτερα τους γονείς μου που ήταν αρωγοί σε κάθε προσπάθειά μου. Τους ευχαριστώ που κράτησαν καλά τα ¨χαλινάρια¨ τις στιγμές εκείνες που χρειαζόταν, πράγμα που με βοήθησε να πετύχω τα περισσότερα απ' όσα έχω κάνει έως τώρα. Για τα υπόλοιπα...ευχαριστώ την Ανάστα, συνοδοιπόρο μου τα τελευταία 5 χρόνια, για την αγάπη της, την υπομονή της, αλλά και το κουράγιο που μου έδινε σε κάθε δύσκολη στιγμή.

Αλέξανδρος Γ. Συγκελάκης
Ηράκλειο, Απρίλιος 2008

1 Εισαγωγή

1.1 Πρώτα σώματα

Ορισμός 1.1 *Ένα σώμα K_0 ονομάζεται* **πρώτο σώμα** *εάν δεν έχει γνήσια υποσώματα.*

□

Πρόταση 1.1 (i) *Κάθε σώμα K έχει ακριβώς ένα πρώτο σώμα K_0 ως υπόσωμα (Το K_0 ονομάζεται* **πρώτο σώμα** *του K).*

(ii) *Κάθε πρώτο σώμα K_0 είναι ισομορφικό με το $\mathbb{Q}$ είτε με το $\mathbb{Z}/p\mathbb{Z}$ για κάποιο πρώτο p (Εξαρτάται εάν $\mathrm{char}K_0 = 0$ ή $\mathrm{char}K_0 = p > 0$).*

Απόδειξη:

(i) Η τομή όλων των υποσωμάτων του K είναι υπόσωμα του K και μάλιστα το μικρότερο υπόσωμα του K, άρα το πρώτο σώμα.

(ii) Διακρίνουμε τις εξής περιπτώσεις

- $\underline{\mathrm{char}K_0 = 0}$. Το σώμα K_0 περιέχει μαζί με το 1 και όλα τα πολλαπλάσια $n1$ για $n \in \mathbb{Z}$. Επειδή $\mathrm{char}K_0 = 0$, έχουμε $n1 \neq 0$ για $n \neq 0$. Θεωρούμε την απεικόνιση

$$\begin{array}{rcl} \phi : \mathbb{Q} & \to & K_0 \\ \dfrac{n}{m} & \mapsto & \dfrac{n1}{m1}, \end{array} \qquad \text{για } n, m \in \mathbb{Z},\ m \neq 0$$

  Η απεικόνιση ϕ είναι ομομορφισμός και επειδή το $\mathbb{Q}$ είναι σώμα και επομένως δεν έχει άλλα ιδεώδη εκτός από το $\mathbb{Q}$

και το τετριμμένο, είναι μονομορφισμός. Άρα η εικόνα $\phi(\mathbb{Q})$ είναι ένα υπόσωμα του K_0 και ισόμορφο προς το $\mathbb{Q}$. Επειδή το K_0 είναι πρώτο, συμπεραίνουμε ότι $\phi(\mathbb{Q}) = K_0$ και επομένως $K_0 \cong \mathbb{Q}$.

- $\underline{\mathrm{char}K_0 = p,\ p \text{ πρώτος}}$. Το ότι $\mathrm{char}K_0 = p,\ p$ πρώτος, σημαίνει ότι $n1 = 0$, εάν και μόνο εάν $p|n$. Άρα η απεικόνιση

$$\begin{aligned} f : \mathbb{Z} &\rightarrow K_0 \\ n &\mapsto n1, \end{aligned}$$

είναι ομομορφισμός με πυρήνα $Kerf$, το κύριο ιδεώδες $< p >= p\mathbb{Z}$. Επομένως $\mathbb{Z}/p\mathbb{Z} \cong f(\mathbb{Z})$. Επειδή το ιδεώδες $p\mathbb{Z}$ είναι μέγιστο και μη τετριμμένο, ο δακτύλιος $\mathbb{Z}/p\mathbb{Z}$ είναι σώμα και μάλιστα το σώμα $\mathbb{Z}_p$ των ακεραίων $modp$. Άρα το $f(\mathbb{Z})$ είναι ένα υπόσωμα του K_0 και επειδή το K_0 είναι πρώτο, έχουμε $f(\mathbb{Z}) = K_0$. Από αυτό συμπεραίνουμε ότι $K_0 \cong \mathbb{Z}_p$.

□

Παρατήρηση: Από την παραπάνω πρόταση συμπεραίνεται ότι από αλγεβρική άποψη τα πρώτα σώματα είναι: Το σώμα $\mathbb{Q}$ των ρητών και όλα τα σώματα $\mathbb{Z}_p$, όπου p ένα πρώτος ακέραιος αριθμός.

Πρόταση 1.2 *Έστω K σώμα, K_0 το αντίστοιχο πρώτο σώμα του K, p πρώτος αριθμός και πολυώνυμο $f(x) = x^{p-1}+x^{p-2}+\cdots+x+1 \in K_0[x]$.*

(i) *Αν $\mathrm{char}K = 0$ τότε το $f(x)$ είναι ανάγωγο πάνω από το K_0.*

(ii) *Αν $\mathrm{char}K = p > 2$ τότε το $f(x)$ δεν είναι ποτέ ανάγωγο πάνω από το K_0.*

(iii) *Αν* $\mathrm{char}K = p = 2$ *τότε το* $f(x)$ *είναι ανάγωγο πάνω από το* K_0.

(iv) *Αν* $\mathrm{char}K = l \neq p$ *με* l *πρώτο, τότε το* $f(x)$ *είναι ανάγωγο πάνω από το* K_0 *αν-ν* $\mathrm{ord}_p(l) = p - 1$.

Απόδειξη:

(i) Λόγω της Πρότασης 4.1 το $f(x)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$ και λόγω του (1.1) είναι ανάγωγο πάνω από το K_0.

(ii) Είναι προφανές. Αφού έχει ως ρίζα το 1, άρα αναλύεται στο K_0 σαν γινόμενο ενός πρωτοβάθμιου πολυωνύμου επί ένα πολυώνυμο βαθμού $p - 1 \geq 1$.

(iii) Είναι επίσης προφανές, αφού τότε $f(x) = x + 1$ το οποίο είναι ανάγωγο.

(iv)

- Ας υποθέσουμε ότι $\mathrm{char}K = l$ και $\mathrm{ord}_p(l) = p - 1$. Λόγω της Πρότασης 1.1 έχουμε $K_0 \cong \mathbb{F}_l$. Ας υποθέσουμε ότι ζ είναι μία ρίζα του $f(x)$. Τότε $\zeta^p = 1$ και $\zeta \neq 1$ άρα $\mathrm{ord}\ (\zeta) = p$. Εάν $m(x)$ είναι το $\mathrm{Irr}\,(\zeta, \mathbb{F}_l)$ με $\deg m(x) = d$ τότε $\mathbb{F}_l(\zeta) = \mathbb{F}_{l^d}$ και $\mathrm{ord}\ (\zeta) | l^d - 1$ δηλαδή $l^d \equiv 1 \pmod p$. Όμως $\mathrm{ord}_p(l) = p - 1$ άρα $p - 1 | d$ και αφού $d \leq p - 1$ άρα $p - 1 = d$. Συνεπώς αφού τα $f(x), m(x)$ είναι και τα δύο μονικά με τον ίδιο βαθμό και $m(x) | f(x)$, άρα ταυτίζονται συνεπώς $f(x)$ ανάγωγο .
- Ας υποθέσουμε, αντίστροφα, ότι το $f(x)$ είναι ανάγωγο πάνω από το $\mathbb{F}_l$. Αν ζ ρίζα του $f(x)$ τότε αφού $f(x)$ ανάγωγο, έχουμε ότι αφενός $\mathrm{Irr}\,(\zeta, \mathbb{F}_l) = f(x)$ και αφετέρου ότι $\zeta \in \mathbb{F}_l(\zeta) = \mathbb{F}_{l^{p-1}}$. Αν υποθέσουμε ότι $\mathrm{ord}(l) = d$, τότε $l^d \equiv 1 \pmod p$. Επίσης, αφού $l \neq p$, άρα $l^{p-1} \equiv 1 \pmod p$, συνεπώς $d | p - 1$. Όμως $\zeta^p = 1$ άρα $\zeta^{l^d - 1} = 1$ $\big($αφού $l^d \equiv 1 \pmod p\big)$ δηλαδή $\zeta^{l^d} = \zeta$ που δείχνει ότι $\zeta \in \mathbb{F}_{l^d}$ κι έτσι $\mathbb{F}_l(\zeta) \subseteq \mathbb{F}_{l^d}$ και τελικά

$\mathbb{F}_{l^{p-1}} \subseteq \mathbb{F}_{l^d}$ που δείχνει ότι $p-1|d$ άρα τελικά $p-1=d$ κι έτσι ord $(l) = p-1$.

□

Πρόταση 1.3 *Έστω K σώμα, K_0 το αντίστοιχο πρώτο σώμα του K και p πρώτος αριθμός. Τότε, το πολυώνυμο $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ είναι ανάγωγο πάνω από το K αν-ν είναι ανάγωγο πάνω από το K_0 και επιπλέον $K_0(\zeta) \cap K = K_0$, όπου ζ είναι μία ρίζα του $f(x)$ σε μία επέκταση του K.*

Απόδειξη:

- Ας υποθέσουμε αρχικά ότι $f(x)$ ανάγωγο πάνω από το K. Τότε $f(x)$ ανάγωγο πάνω από το K_0 και μένει να δείξουμε ότι $K_0(\zeta) \cap K = K_0$. Προφανώς $L := K_0(\zeta) \cap K \supseteq K_0$ άρα έχουμε $K_0 \subseteq L \subseteq K_0(\zeta)$. Η επέκταση $K_0(\zeta)/K_0$ είναι $Galois$ βαθμού $p-1$ και έχει ομάδα $Galois$ την

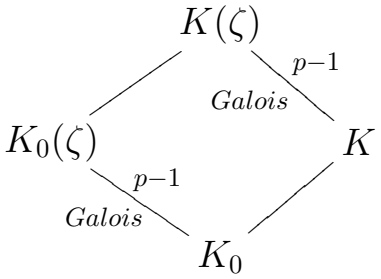
$$G = \{\sigma_i : 1 \leq i \leq p-1, \sigma_i(\zeta) = \zeta^i\}.$$

  Επίσης, η επέκταση $K_0(\zeta)|L$ είναι $Galois$ βαθμού, ας υποθέσουμε d, με αντίστοιχη ομάδα $Galois$ την

$$H = \{\tau_i : 1 \leq i \leq d-1\}.$$

  Από το θεμελιώδες Θεώρημα της Θεωρίας $Galois$ έχουμε ότι $H \leq G$.

  Άρα εάν δείξουμε ότι για κάθε $\beta \in L$, έχουμε ότι $\sigma_i(\beta) = \beta$ (δηλαδή οι σ_i σταθεροποιούν το L), εχουμε τελειώσει αφού τότε $H \leq G$ και τα τ_i θα ταυτίζονται με τα σ_i, άρα $H = G$ οπότε $L = K_0$.



Έστω G' η ομάδα $Galois$ της επέκτασης $K(\zeta)/K$. Τότε

$$G' = \{\rho_i : 1 \leq i \leq p-1, \rho_i(\zeta) = \zeta^i\}$$

και ισχύει $\rho_i \mid_{K_0(\zeta)} = \sigma_i$. Άρα

$$\sigma_i(\beta) = \rho_i \mid_{K_0(\beta)} (\beta) \overset{\beta \in K_0(\zeta)}{=} \rho_i(\beta) = {}^1\beta$$

- Ας υποθέσουμε, αντίστροφα ότι $L = K_0$ και έστω $G = \{\sigma_i\}, G' = \{\rho_i\}$ οι ομάδες $Galois$ των επεκτάσεων $K_0(\zeta)/L$ (δηλαδή της $K_0(\zeta)/K_0$) και $K(\zeta)/K$ αντίστοιχα. Θεωρούμε την καλά ορισμένη απεικόνιση

$$\begin{aligned} \theta : G' &\to G \\ \rho_i &\mapsto \rho_i \mid_{K_0(\zeta)} \end{aligned}$$

Εύκολα ελέγχουμε ότι είναι ομομορφισμός. Επίσης

$$\begin{aligned} \ker\theta &= \{\rho_i \in G' : \theta(\rho_i) = id\} = \{\rho_i \in G' : \rho_i \mid_{K_0(\zeta)} = id\} \\ &\overset{(\star)}{=} \{id \ \tau ou \ K(\zeta)\} \end{aligned}$$

[1] Αφού $\beta \in K$ και οι ρ_i σταθεροποιούν το K.

όπου η $(\star)$ ισχύει διότι ο ρ_i σταθεροποιεί το $K_0(\zeta)$ άρα και το ζ. Όμως σταθεροποιεί και το K εξ'ορισμού, άρα τελικά σταθεροποιεί και το $K(\zeta)$ δηλαδή είναι ο id του $K(\zeta)$.

Άρα ο θ είναι μονομορφισμός. Θα δείξουμε ότι είναι και επιμορφισμός. Επειδή $\sigma \in G$, άρα ο σ χαρακτηρίζεται πλήρως από τη δράση του στο ζ και έτσι θα πρέπει να στέλνει το ζ σε κάποια άλλη ρίζα του αναγώγου πολυωνύμου δηλαδή σε κάποια άλλη πρωταρχική $p-$ρίζα της μονάδος.Όμως όλες οι πρωταρχικές $p-$ρίζες της μονάδος είναι της μορφής ζ^i για $1 \leq i \leq p-1$. Συνεπώς $\sigma(\zeta) = \zeta^j$ για κάποιο j, με $1 \leq j \leq p-1$. Διαλέγουμε λοιπόν $\rho \in G'$ ώστε $\rho(\zeta) = \zeta^j$. Τότε $\rho|_{K_0(\zeta)} = \sigma$ κι έτσι τελικά $\theta(\rho) = \sigma$. Άρα ο θ είναι και επιμορφισμός.

□

Παρατήρηση: Οι παραπάνω προτάσεις χαρακτηρίζουν πλήρως τις περιπτώσεις στις οποίες το πολυώνυμο $f(x)$ είναι ανάγωγο πάνω από οποιοδήποτε σώμα K.

1.2 Κανονικές Βάσεις

Ορισμός 1.2 *Ας είναι L/K μία πεπερασμένη επέκταση $Galois$ βαθμού n και $G := G(L/K)$ η αντίστοιχη ομάδα $Galois$. Μία βάση του L πάνω από το K, ονομάζεται* **κανονική** *εάν είναι της μορφής $(\sigma\alpha)_{\sigma\in G}$ με $\alpha \in L$.*

□

Παράδειγμα 1.1 *Ας υποθέσουμε ότι έχουμε το πεπερασμένο σώμα $\mathbb{F}_{2^3}$ πάνω από το $\mathbb{F}_2$ και α ρίζα του αναγώγου πολυωνύμου $x^3+x+1 \in \mathbb{F}_2[x]$. Ως γνωστόν, όλες οι επεκτάσεις πεπερασμένων σωμάτων είναι επεκτάσεις Galois και το σύνολο $\{1, \alpha, \alpha^2\}$ αποτελεί βάση της επέκτασης $\mathbb{F}_{2^3}/\mathbb{F}_2$. Το σύνολο $\{\alpha, \alpha^2, \alpha^{2^2} = \alpha^2 + \alpha\}$ δεν αποτελεί βάση της επέκτασης, ενώ εάν επιλέξουμε $\beta = \alpha^3 = \alpha + 1$ τότε το σύνολο $\{\beta = \alpha + 1, \beta^2 = \alpha^2 + 1, \beta^{2^2} = \alpha\}$ είναι γραμμικώς ανεξάρτητο σύνολο πάνω από το $\mathbb{F}_2$ άρα αποτελεί $\mathbb{F}_2-$βάση του $\mathbb{F}_{2^3}$ οπότε κανονική βάση.*

□

Γεννιέται λοιπόν φυσιολογικά το ερώτημα εάν κάθε επέκταση $Galois$ έχει κανονική βάση. Η απάντηση είναι θετική και την παραθέτουμε παρακάτω.

1.2.1 Ύπαρξη κανονικής βάσης σε επεκτάσεις Galois

Πρόταση 1.4 *Έστω L/K επέκταση $Galois$ βαθμού n, το K να έχει πλήθος στοιχείων μεγαλύτερο του $n(n-1)$ και $G = \{\sigma_1, \ldots, \sigma_n\}$ η αντίστοιχη ομάδα $Galois$. Τότε υπάρχει $\theta \in L$ τέτοιο, ώστε τα $\sigma_1(\theta), \ldots, \sigma_n(\theta)$ να είναι γραμμικά ανεξάρτητα.*

Απόδειξη:

Η L/K είναι διαχωρίσιμη επέκταση άρα υπάρχει $\alpha \in L$ τέτοιο ώστε $L = K(\alpha)$. Έστω $f(x) = \mathrm{Irr}\,(\alpha, K)$, $\sigma_i(\alpha) = \alpha_i$ με $\alpha = \alpha_1$ και

$$\begin{aligned} g(x) &= \frac{f(x)}{(x-\alpha_1)f'(\alpha_1)} := g_1(x), \\ g_i(x) &= \sigma_i\left(g(x)\right) = \frac{f(x)}{(x-\alpha_i)f'(\alpha_i)},\ i = 2, \ldots, n. \end{aligned}$$

Παρατηρούμε ότι $f'(\alpha_i) \neq 0,\ i = 1, \ldots, n$, διότι $\alpha_i \neq \alpha_j$ για $i \neq j$ (λόγω διαχωρισιμότητας).

Συνεπώς $g_i(x) \in L[x],\ i = 1 \ldots, n$ και έχει ως ρίζα κάθε α_k με $k \neq i$.

Άρα

$$g_i(x)g_k(x) \equiv 0 \pmod{f(x)} \tag{1.1}$$

Αυτό συμβαίνει διότι για να διαιρείται ένα πολυώνυμο από το $f(x)$, αρκεί να έχει τουλάχιστον ως ρίζες, τις ρίζες του $f(x)$.

Το πολυώνυμο $g_1(x) + \cdots + g_n(x) - 1$ έχει βαθμό το πολύ $n-1$ και από την άλλη έχει τα $\alpha_i,\ i = 1 \ldots, n$ ως ρίζες διότι $g_i(\alpha_i) = 1$ και $g_i(\alpha_k) = 0,\ i \neq k$. Άρα

$$g_1(x) + \cdots + g_n(x) - 1 = 0 \tag{1.2}$$

Πολλαπλασιάζοντας την τελευταία με $g_i(x),\ i = 1, \ldots, n$ και κάνοντας χρήση της σχέσης (1.1), παίρνω ότι

$$\left(g_i(x)\right)^2 \equiv g_i(x) \pmod{f(x)} \tag{1.3}$$

Θεωρούμε τώρα την ορίζουσα

$$D(x) = \det\left(\sigma_i\sigma_k\left(g(x)\right)\right) \in L[x],\ i, k = 1, \ldots, n$$

και θα δείξουμε ότι $D(x) \neq 0$. Αρκεί να δείξουμε ότι $D^2(x) \neq 0$.

Όμως

$$\begin{aligned} D^2(x) &= \det\left(\sigma_i\sigma_k\left(g(x)\right)\right)\det\left(\sigma_i\sigma_k\left(g(x)\right)\right) \\ &= \det\left(\sigma_i\sigma_k\left(g(x)\right)\right)\det\left(\sigma_k\sigma_i\left(g(x)\right)\right) \\ &= \det\left(\left(\sigma_i\sigma_j\left(g(x)\right)\right)\cdot\left(\sigma_k\sigma_i\left(g(x)\right)\right)\right). \end{aligned} \tag{1.4}$$

Το τυπικό στοιχείο A_{ij} του πίνακα μέσα στην ορίζουσα, είναι το άθροισμα

$$A_{ij} = \sum_{k=1}^{n} \sigma_i\sigma_k(g(x)) \cdot \sigma_j\sigma_k(g(x)) = \sum_{k=1}^{n} \sigma_i(g_k(x)) \cdot \sigma_j(g_k(x))$$

και εξ' ορισμού των $g_i(x)$ έχουμε διαδοχικά

$$\begin{aligned} \sigma_i(g_k(x)) = \sigma_j(g_k(x)) &\iff \sigma_i\sigma_k(\alpha) = \sigma_j\sigma_k(\alpha) \iff \sigma_i\sigma_k = \sigma_j\sigma_k \\ &\iff \sigma_i = \sigma_j \iff i = j. \end{aligned}$$

(i) Εάν $i = j$ τότε

$$\begin{aligned} A_{ii} &= \sum_{k=1}^{n}(\sigma_j(g_k(x)))^2 \overset{(\star)}{=} \sum_{r=1}^{n}(g_r(x))^2 \\ &\overset{(1.3)}{\equiv} \sum_{r=1}^{n} g_r(x) \overset{(1.2)}{=} 1 \pmod{(f(x))} \\ &\quad \text{για} \quad \text{κάποιο} \ \ r \in \{1,\ldots,n\}. \end{aligned}$$

Σημείωση : Αξίζει να σημειώσουμε ότι $\sigma_i(g_k(x)) = g_r(x)$ για κάποιο $r \in \{1,\ldots,n\}$ και μάλιστα για διαφορετικό i παίρνω και διαφορετικό $\sigma_i(g_k(x))$ δηλαδή διαφορετικό r ώστε $\sigma_i(g_k(x)) = g_r(x)$,

οπότε πράγματι η άθροιση στην ισότητα $(\star)$ είναι πάνω σε όλα τα $r \in \{1, \ldots, n\}$ καθώς το k διατρέχει τα $1, \ldots, n$.

(ii) Εάν $i \neq j$ τότε από τα παραπάνω έχουμε $\sigma_i(g_k(x)) \neq \sigma_j(g_k(x))$, συνεπώς λόγω της σχέσης (1.1), έχουμε

$$A_{ij} \equiv 0 \pmod{f(x)}.$$

Συγκεντρώνοντας λοιπόν τα παραπάνω, το γινόμενο των πινάκων μέσα στην ορίζουσα, έχει στην κύρια διαγώνιο το $1 \pmod{f(x)}$ και παντού αλλού το $0 \pmod{(f(x))}$, άρα

$$D^2(x) \equiv 1 \pmod{f(x)}.$$

Το $D(x)$ έχει βαθμό το πολύ $n(n-1)$ άρα έχει πεπερασμένο πλήθος ριζών στο K οπότε εάν το K έχει περισσότερα από $n(n-1)$ στοιχεία (πόσο μάλλον όταν έχει άπειρα στοιχεία), υπάρχει στοιχείο $\beta \in K$ τέτοιο, ώστε $D(\beta) \neq 0$. Θέτουμε

$$\theta = g(\beta).$$

Τότε $D(\beta) = \det(\sigma_i \sigma_k(\theta)) \neq 0$.

Έστω τώρα ότι υπάρχει μη τετριμμένος γραμμικός συνδυασμός

$$k_1\sigma_1(\theta) + \cdots + k_n\sigma_n(\theta) = 0,\ k_i \in K, \quad \text{όχι όλα μηδέν.}$$

Εφαρμόζωντας σε αυτόν, τον αυτομορφισμό $\sigma_i,\ i = 1, \ldots, n$ παίρνουμε n εξισώσεις με αγνώστους τα k_i

$$k_1\sigma_i\sigma_1(\theta) + \cdots + k_n\sigma_i\sigma_n(\theta) = 0,\ i = 1, \ldots, n$$

δηλαδή το ομογενές σύστημα

$$\sum_{k=1}^{n} x_k \sigma_i \sigma_k(\theta) = 0,\ i = 1, \ldots, n$$

έχει τη μη μηδενική λύση $k_1, \ldots, k_n$ οπότε η ορίζουσά του, $\det(\sigma_i\sigma_k(\theta)) = D(\beta) = 0$, άτοπο. Άρα

$$k_i = 0, i = 1, \ldots, n$$

άρα τα $\sigma_1(\theta), \ldots, \sigma_n(\theta)$ είναι γραμμικώς ανεξάρτητα.

□

Πόρισμα 1.1 *Μία πεπερασμένη επέκταση $Galois$, έστω L/K βαθμού n με πλήθος στοιχείων του K μεγαλύτερο του $n(n-1)$, έχει πάντοτε κανονική βάση.*

Πόρισμα 1.2 *Μία άπειρη επέκταση $Galois$, έστω L/K έχει πάντοτε κανονική βάση.*

Τί γίνεται όμως στην περίπτωση που το πλήθος των στοιχείων του K είναι πεπερασμένο και μικρότερο ή ίσο από $n(n-1)$; Σε αυτή την περίπτωση έχουμε να κάνουμε με επέκταση πεπερασμένου σώματος και η απόδειξη διαφέρει από την παραπάνω. Την παραθέτουμε παρακάτω.

1.2.2 Κανονική βάση σε πεπερασμένα σώματα

Για να δείξουμε το Θεώρημα ύπαρξης κανονικής βάσης στην περίπτωση πεπερασμένων σωμάτων θα κάνουμε χρήση ορισμένων βασικών προτάσεων της Γραμμικής Άλγεβρας.

Ορισμός 1.3 *Ας είναι V ένας διανυσματικός χώρος πάνω από το σώμα $\mathbb{F}$, $T : V \to V$ μία γραμμική απεικόνιση και $Id : V \to V$ η ταυτοτική γραμμική απεικόνιση. Για κάθε πολυώνυμο $\mathbb{F}[x] \ni p(x) = a_n x^n + \cdots +$*

$a_1x + a_0$, *ορίζουμε του τελεστή* $p(T) := a_nT^n + \cdots + a_1T + a_0Id$, *όπου* $T^k = \underbrace{T \circ \cdots \circ T}_{k \text{ συνθέσεις}}$.

□

Πρόταση 1.5 *Ας είναι* V *ένας διανυσματικός χώρος πάνω από το σώμα* $\mathbb{F}$ *και* $T : V \to V$ *μία γραμμική απεικόνιση . Τότε*

(*i*) *Εάν* $\mathbb{F}[x] \ni p(x) = a_nx^n + \cdots + a_1x + a_0$, *τότε το* $p(T)$ *είναι γραμμική απεικόνιση του διανυσματικού χώρου* V *πάνω από το σώμα* $\mathbb{F}$.

(*ii*) *Το σύνολο* $\mathcal{A}$ *των πολυωνύμων* $p(x) \in \mathbb{F}[x]$ *για τα οποία* $p(T) = 0$, *είναι ιδεώδες του* $\mathbb{F}[x]$.

Απόδειξη:

(*i*)
- Έστω $v_1, v_2 \in V$. Τότε

$$\begin{aligned} p(T)(v_1 + v_2) &= a_nT^n(v_1 + v_2) + \cdots + a_1T(v_1 + v_2) \\ &+ a_0Id(v_1 + v_2) \\ &= a_n[T^n(v_1) + T^n(v_2)] + \cdots + a_1[T(v_1) + T(v_2)] \\ &+ a_0(v_1 + v_2) \\ &= p(T)(v_1) + p(T)(v_2) \end{aligned}$$

- Για κάθε $\lambda \in \mathbb{F}$ και $v \in V$ έχουμε

$$\begin{aligned} p(T)(\lambda v) &= a_nT^n(\lambda v) + \cdots + a_1T(\lambda v) + a_0Id(\lambda v) \\ &= \lambda(a_nT^n + \cdots + a_1T + a_0Id) = \lambda p(T)(v) \end{aligned}$$

(*ii*) Το σύνολο $\mathcal{A}$ είναι υποδακτύλιος του $\mathbb{F}[x]$ διότι εάν $p, q \in \mathcal{A}$ τότε $(p + q)(T) = p(T) + q(T) = 0$ και $(pq)(T) = p(T)q(T) = 0$.

Τέλος, λόγω της $(pf)(T) = p(T)f(T) = 0$ για κάθε $p \in \mathcal{A},\ f \in \mathbb{F}[X]$, το σύνολο $\mathcal{A}$ είναι ιδεώδες του $\mathbb{F}[x]$.

□

Ορισμός 1.4 *Έστω V, ένας n-διάστατος διανυσματικός χώρος πάνω από το σώμα $\mathbb{F}$. Το σύνολο όλων των γραμμικών απεικονίσεων από το V στο V το συμβολίζουμε με $\mathcal{L}(V,V)$ και είναι διανυσματικός χώρος πάνω από το σώμα $\mathbb{F}$ διάστασης n^2 αφού είναι ισόμορφος με το σύνολο $M_{n\times n}(\mathbb{F})$ των $n \times n$ πινάκων με στοιχεία από το $\mathbb{F}$.*

□

Πρόταση 1.6 *Έστω V, ένας n-διάστατος διανυσματικός χώρος πάνω από το σώμα $\mathbb{F}$ και $T : V \to V$ μία γραμμική απεικόνιση. Τότε υπάρχει μη μηδενικό πολυώνυμο $p(x) \in \mathbb{F}[x]$ τέτοιο, ώστε $p(T) = 0$.*

Απόδειξη:

Παίρνουμε τις n^2+1 γραμμικές απεικονίσεις $Id, T, T^2, \ldots, T^{n^2}$. Καθώς ο διανυσματικός χώρος $\mathcal{L}(V,V)$ των γραμμικών απεικονίσεων του V στο V έχει διάσταση n^2 πάνω από το $\mathbb{F}$, άρα πρέπει οι παραπάνω γραμμικές απεικονίσεις να είναι γραμμικώς εξαρτημένες. Δηλαδή για κάποια $c_0, c_1, \ldots, c_{n^2} \in \mathbb{F}$, όχι όλα μηδέν, ισχύει $c_{n^2}T^{n^2} + \cdots + c_1T + c_0Id = 0$. Τότε το πολυώνυμο

$$p(x) = c_{n^2}x^{n^2} + \cdots + c_1x + c_0,$$

είναι το ζητούμενο.

□

Πόρισμα 1.3 *Το ιδεώδες $\mathcal{A}$ του $\mathbb{F}[X]$ που ορίσαμε στην Πρόταση 1.12 δεν είναι το μηδενικό.*

□

Παρατήρηση: Εάν θεωρήσουμε το σύνολο όλων των βαθμών των πολυωνύμων του συνόλου $\mathcal{A}$, τότε αυτό είναι σύνολο φυσικών άρα περιέχει ελάχιστο στοιχείο το οποίο χρησιμοποιούμε όπως φαίνεται στον παρακάτω ορισμό.

Ορισμός 1.5 *Ας είναι V ένας πεπερασμένης διάστασης διανυσματικός χώρος πάνω από το σώμα $\mathbb{F}$ και $T : V \to V$ μία γραμμική απεικόνιση .*

Ελάχιστο πολυώνυμο *$m(x)$ της γραμμικής απεικόνισης T είναι ένα μονικό πολυώνυμο ελαχίστου βαθμού για το οποίο ισχύει $m(T) = 0$.*

□

Πρόταση 1.7 *Το ελάχιστο πολυώνυμο είναι μοναδικό.*

Απόδειξη:

Εάν υπήρχε $m'(x) \neq m(x)$ μονικό και τέτοιο, ώστε $m'(T) = 0$, τότε το $m'(x) - m(x)$ έχει μικρότερο βαθμό από το $m(x)$ και $(m' - m)(T) = m'(T) - m(T) = 0$, άρα $m' - m \in \mathcal{A}$, άτοπο λόγω της ελαχιστότητας του βαθμού του $m(x)$. Άρα το $m'(x) - m(x)$ είναι το μηδενικό πολυώνυμο, συνεπώς $m'(x) = m(x)$.

□

Πρόταση 1.8 *Ας είναι V ένας πεπερασμένης διάστασης διανυσματικός χώρος πάνω από το σώμα $\mathbb{F}$, $v \in V$ και $T : V \to V$ μία γραμμική απεικόνιση . Αν $m(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$ είναι το ελάχιστο πολυώνυμο της γραμμικής απεικόνισης T και $v_i = T^i(v),\ i = 0, 1, \ldots$ τότε κάθε ένα από τα διανύσματα $v_{k+i},\ i = 0, 1, \ldots$ είναι γραμμικός συνδυασμός των $v_0, v_1, \ldots, v_{k-1}$.*

Απόδειξη:

Θα εφαρμόσουμε τη μέθοδο της ισχυρής επαγωγής επί του i. Για $i = 0$ έχουμε $v_k = T^k(v) = -a_{k-1}T^{k-1}(v) - \cdots - a_1T(v) - a_0v$. Έστω $i \geq 1$ και υποθέτουμε ότι ισχύει για όλα τα $i \leq r$. Τότε

$$\begin{aligned} v_{k+r+1} &= T^{k+r+1}(v) = T\left(T^{k+r}(v)\right) \quad (\text{επαγωγική υπόθεση}) \\ &= T\left(b_{k-1}T^{k-1}(v) + \cdots + b_1T + b_0Id\right) \\ &= b_{k-1}T^k(v) + b_{k-2}T^{k-1} + \cdots + b_1T^2(v) + b_0T(v) \\ &= b_{k-1}\left(-a_{k-1}T^{k-1}(v) - \cdots - a_1T(v) - a_0v\right) \\ &+ b_{k-2}T^{k-1} + \cdots + b_1T^2(v) + b_0T(v) \\ &= (-a_{k-1}b_{k-1} + b_{k-2})T^{k-1}(v) + \cdots + (-a_1b_{k-1} + b_0)T(v) \\ &- a_0b_{k-1}v. \end{aligned}$$

□

Πρόταση 1.9 *Ας είναι V ένας πεπερασμένης διάστασης διανυσματικός χώρος πάνω από το σώμα $\mathbb{F}$ και $T : V \to V$ μία γραμμική απεικόνιση . Εάν $m(x)$ είναι το ελάχιστο πολυώνυμο της T και $p(x) \in \mathbb{F}[x]$ πολυώνυμο με $p(T) = 0$, τότε $m(x)|p(x)$.*

Απόδειξη:

Προκύπτει άμεσα εάν κάνουμε τη διαίρεση του $p(x)$ με το $m(x)$. Τότε, εάν το υπόλοιπο της διαίρεσης δεν είναι το μηδενικό πολυώνυμο, θα είχαμε ένα πολυώνυμο μικρότερου βαθμού από το $m(x)$ και το οποίο μηδενίζεται από την T, άτοπο λόγω της ελαχιστότητας του βαθμού του $m(x)$.

□

Ορισμός 1.6 *Ας είναι V ένας n-διάστατος διανυσματικός χώρος πάνω από το σώμα $\mathbb{F}$ και $T : V \to V$ μία γραμμική απεικόνιση .* ***Χαρακτηριστικό πολυώνυμο*** *της T με αντίστοιχο πίνακα $M_{n\times n}$ ονομάζουμε το πολυώνυμο $\det(xI - M)$, όπου I ο μοναδιαίος $n \times n$ πίνακας.*

□

Η ακόλουθη Πρόταση, γνωστή και ως Θεώρημα των **Cayley - Hamilton** , περιέχεται σε όλα τα βιβλία Γραμμικής Άλγεβρας στα οποία μπορεί να ανατρέξει ο αναγνώστης προκειμένου να διαβάσει την απόδειξη.

Πρόταση 1.10 *Ας είναι V ένας διανυσματικός χώρος πάνω από το σώμα $\mathbb{F}$ και $T : V \to V$ μία γραμμική απεικόνιση . Εάν $f(x)$ είναι το χαρακτηριστικό πολυώνυμο της T, τότε $f(T) = 0$ δηλαδή $m(x)|f(x)$, όπου $m(x)$ το ελάχιστο πολυώνυμο της T.*

□

Ορισμός 1.7 *Ας είναι V ένας διανυσματικός χώρος πάνω από το σώμα $\mathbb{F}$ και $T : V \to V$ μία γραμμική απεικόνιση . Ένα διάνυσμα $v \in V$ ονομάζεται* ***κυκλικό*** *εάν τα διανύσματα $T^k(v), \ \ k = 0, 1, \ldots$ παράγουν του V.*

□

Η απόδειξη του θεωρήματος ύπαρξης κανονικής βάσης σε πεπερασμένα σώματα θα προκύψει με τη βοήθεια των παρακάτω δύο λημμάτων.

Λήμμα 1.1 *Ας είναι V ένας διανυσματικός χώρος διάστασης n πάνω από το σώμα $\mathbb{F}$ και $T : V \to V$ μία γραμμική απεικόνιση . Τότε για την T υπάρχει κυκλικό διάνυσμα $v \in V$ αν και μόνο εάν το χαρακτηριστικό $\chi(x)$ και το ελάχιστο πολυώνυμο $m(x)$ της T ταυτίζονται.*

□

Λήμμα 1.2 ***(Λήμμα του Artin)*** *Εάν $\psi_1, \ldots, \psi_m$ είναι διακεκριμένοι ομομορφισμοί από μία ομάδα G στην πολλαπλασιαστική ομάδα των μη μηδενικών στοιχείων $\mathbb{F}^*$ ενός σώματος $\mathbb{F}$ και $\alpha_1, \ldots, \alpha_m$ στοιχεία του σώματος $\mathbb{F}$ όχι όλα μηδέν. Τότε για κάποιο $g \in G$ ισχύει*

$$\alpha_1\psi_1(g) + \cdots + \alpha_m\psi_m(g) \neq 0$$

Απόδειξη :

Η απόδειξη θα γίνει με τη μέθοδο της μαθηματικής επαγωγής επί του m. Για $m = 1$ είναι φανερή η ισχύς της πρότασης οπότε υποθέτουμε ότι $m > 1$ και ότι η πρόταση ισχύει για τυχαίους $m-1$ ομομορφισμούς. Ας πάρουμε $\psi_1, \ldots, \psi_m$ και $\alpha_1, \ldots, \alpha_m$ όπως στο Λήμμα. Εάν $\alpha_1 = 0$ τότε η επαγωγική υπόθεση δίνει το ζητούμενο αποτέλεσμα. Έστω λοιπόν ότι $\alpha_1 \neq 0$ και ας υποθέσουμε αντίθετα από το ζητούμενο, ότι

$$\alpha_1\psi_1(g) + \cdots + \alpha_m\psi_m(g) = 0, \quad \text{για κάθε} \quad g \in G. \tag{1.5}$$

Καθώς $\psi_1 \neq \psi_m$, άρα υπάρχει $h \in G$ τέτοιο ώστε $\psi_1(h) \neq \psi_m(h)$. Τότε, βάζοντας στη σχέση (1.5) στη θέση του g, το hg παίρνουμε

$$\alpha_1\psi_1(h)\psi_1(g) + \cdots + \alpha_m\psi_m(h)\psi_m(g) = 0, \quad \text{για κάθε} \quad g \in G.$$

Πολλαπλασιάζοντας την τελευταία με $\psi_m(h)^{-1}$ (το αντίστροφο αυτού του στοιχείου υπάρχει καθώς $\psi_m(h) \in \mathbb{F}^*$) παίρνουμε

$$b_1\psi_1(g) + \cdots + b_{m-1}\psi_{m-1}(g) + b_m\psi_m(g) = 0, \quad \text{για κάθε} \quad g \in G,$$

όπου $b_i = \alpha_i \psi_i(h)\psi_m(h)^{-1}$, $1 \leq i \leq m-1$. Αφαιρώντας την τελευταία από την σχέση (1.5) φτάνουμε στην

$$c_1\psi_1(g) + \cdots + c_{m-1}\psi_{m-1}(g) = 0, \quad \text{για κάθε} \quad g \in G,$$

όπου $c_i = a_1 - b_i$, $1 \leq i \leq m-1$. Όμως το $c_1 = a_1 - a_1\psi_1(h)\psi_m(h)^{-1} = a_1\left(1 - \psi_1(h)\psi_m(h)^{-1}\right) \neq 0$, που έρχεται σε αντίφαση με την επαγωγική υπόθεση.

□

Θεώρημα 1.1 *Για κάθε πεπερασμένο σώμα K και κάθε πεπερασμένη επέκταση F του K, υπάρχει κανονική βάση του F πάνω από το K.*

Απόδειξη:

Έστω $K = \mathbb{F}_q$ και $F = \mathbb{F}_{q^m}$, $m \geq 2$. Η επέκταση ως πεπερασμένη είναι $Galois$, άρα η αντίστοιχη ομάδα $Galois$ είναι κυκλική και παράγεται από ένα στοιχείο σ. Συνεπώς όλοι οι αυτομορφισμοί είναι οι $id, \sigma, \ldots, \sigma^{m-1}$ με $\sigma(\alpha) = \alpha^q$, $\alpha \in F$. Επειδή $\sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta)$ και $\sigma(c\alpha) = \sigma(c)\sigma(\alpha) = c\sigma(\alpha)$, για $\alpha, \beta \in F$ και $c \in K$, η απεικόνιση σ μπορεί να θεωρηθεί ως γραμμική απεικόνιση του διανυσματικού χώρου F πάνω από το σώμα K. Καθώς $\sigma^m = id$, άρα για το πολυώνυμο $p(x) = x^m - 1 \in K[x]$ ισχύει $p(\sigma) = 0$ και έτσι εάν εφαρμόσουμε το Λήμμα 1.2 στους $id, \sigma, \ldots, \sigma^{m-1}$ τους οποίους βλέπουμε ως ενδομορφισμούς του $\mathbb{F}^*$, βλέπουμε ότι κανένα μη μηδενικό πολυώνυμο στο $K[x]$ με βαθμό μικρότερο από m δεν μηδενίζεται από το σ. Συνεπώς το πολυώνυμο $x^m - 1$ είναι το ελάχιστο πολυώνυμο της γραμμικής απεικόνισης σ. Καθώς το χαρακτηριστικό πολυώνυμο του σ είναι μονικό βαθμού m που διαιρείται από το ελάχιστο, προκύπτει ότι το χαρακτηριστικό πολυώνυμο της γραμμικής απεικόνισης σ είναι επίσης

το $x^m - 1$. Τότε όμως, από το Λήμμα 1.1, υπάρχει στοιχείο $\alpha \in F$ τέτοιο ώστε τα $\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots$ να παράγουν τον F. Από την άλλη, τα στοιχεία $\sigma^k(\alpha)$ για $k \geq m$ ($\sigma^m(\alpha) = \alpha$) επαναλαμβάνονται και έτσι προκύπτει ότι τα $\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots, \sigma^{m-1}$ παράγουν τον F δηλαδή δίνουν μία βάση του F πάνω από το K. Καθώς αυτή η βάση περιέχει το α και όλα τα συζυγή του ως προς το K, άρα είναι κανονική βάση του F πάνω από το K.

□

1.3 Δυϊκή Βάση Επέκτασης

Ορισμός 1.8 *Ας είναι L/K μία πεπερασμένη επέκταση Galois με αντίστοιχη ομάδα Galois την G. Ονομάζουμε* **ίχνος** *του στοιχείου $\alpha \in L$ και το συμβολίζουμε με $\mathrm{Tr}(\alpha)$, το*

$$\mathrm{Tr}(\alpha) = \sum_{\sigma \in G} \sigma\alpha.$$

Σημείωση: $\mathrm{Tr}(\alpha) \in K$ διότι κάθε αυτομορφισμός $\rho \in G$ το σταθεροποιεί.

□

Πρόταση 1.11 *Εάν L/K διαχωρίσιμη επέκταση βαθμού n, η $\{a_1, \ldots, a_n\}$ είναι βάση της και $u_1, \ldots, u_n \in K$ τυχαία, τότε υπάρχει μοναδικό $\lambda \in L$, τέτοιο ώστε*

$$\mathrm{Tr}(\lambda \cdot a_i) = u_i,\ i = 1, \cdots, n$$

Απόδειξη:

Αναζητούμε $x_1 \cdots, x_n \in K$, $\lambda = x_1 a_1 + \cdots + x_n a_n$ τέτοια ώστε

$$\mathrm{Tr}\left((x_1 a_1 + \cdots + x_n a_n)\, a_i\right) = u_i,\ i = 1, \ldots, n$$

δηλαδή θέλω

$$\left(\mathrm{Tr}(a_i a_j)\right)_{i,j} \cdot (x_1, \ldots, x_n)^\top = (u_1, \ldots, u_n)^\top$$

Όμως ο πίνακας $\left(\mathrm{Tr}(a_i a_j)\right)_{i,j}$ είναι μη ιδιάζων άρα έχει ορίζουσα διάφορη του μηδενός. Συνεπώς υπάρχει μία ακριβώς λύση $(x_1, \ldots, x_n)$.

□

Πόρισμα 1.4 *Μπορούμε να βρούμε* $a_1^*, \ldots, a_n^*$ *τέτοια ώστε*

$$\mathrm{Tr}\,(a_i^* a_j) = \begin{cases} 1, \textit{αν } i = j \\ 0, \textit{αν } i \neq j \end{cases}$$

Μάλιστα τα $a_1^*, \ldots, a_n^*$ *είναι γραμμικώς ανεξάρτητα .*

Απόδειξη:

Λόγω της Πρότασης 1.11 μπορούμε να επιλέξουμε μοναδικά $a_i^*,\ i = 1, \ldots, n$ τέτοια ώστε

$$\begin{aligned} \mathrm{Tr}\,(a_1^* \cdot a_j) &= \delta_{1j} \quad (\text{Επιλέγω } \ u_j = \delta_{1j}) \\ \mathrm{Tr}\,(a_2^* \cdot a_j) &= \delta_{2j} \quad (\text{Επιλέγω } \ u_j = \delta_{2j}) \\ &\vdots \\ \mathrm{Tr}\,(a_n^* \cdot a_j) &= \delta_{nj} \quad (\text{Επιλέγω } \ u_j = \delta_{nj}) \end{aligned}$$

Για την γραμμική τους ανεξαρτησία, ας υποθέσουμε ότι υπάρχουν $k_1, \ldots, k_n \in K$ τέτοια ώστε

$$k_1 a_1^* + \ldots + k_n a_n^* = 0.$$

Τότε για κάθε $j = 1, \ldots, n$ έχω (πολλαπλασιάζω την παραπάνω με a_j)

$$\begin{aligned} k_1 a_1^* a_j + \ldots + k_j a_j^* a_j + \ldots + k_n a_n^* a_j &= 0 \Rightarrow \\ k_1 \delta_{1j} + \ldots + k_j \delta_{jj} + \ldots + k_n \delta_{nj} &= 0 \Rightarrow \\ k_j = 0, \quad \forall j = 1 \ldots n & \end{aligned}$$

□

Ορισμός 1.9 *Τα* $a_1^*, \ldots, a_n^* \in L$ *αποτελούν τη* ***δυϊκή βάση*** *της* $a_1, \ldots, a_n$.

□

Παράδειγμα 1.2 *Θα βρούμε τη δυϊκή βάση της συνήθους βάσης* $\{1, \sqrt{2}\}$ *της επέκτασης* $Galois$ $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ *με αντίστοιχη ομάδα* $Galois$ G *την* $G = \{id, \sigma\}$ *όπου* $\sigma(1) = 1$ *και* $\sigma(\sqrt{2}) = -\sqrt{2}$.

Εάν $a_1 = 1, a_2 = \sqrt{2}$ *και* $a_1^* = \lambda_{11}a_1 + \lambda_{12}a_2,\ a_2^* = \lambda_{21}a_1 + \lambda_{22}a_2$, *τότε*

$$\begin{aligned} a_1^*a_1 &= \lambda_{11} + \lambda_{12}\sqrt{2} \\ a_1^*a_2 &= 2\lambda_{12} + \lambda_{11}\sqrt{2} \\ a_2^*a_1 &= \lambda_{21} + \lambda_{22}\sqrt{2} \ \textit{και} \\ a_2^*a_2 &= 2\lambda_{22} + \lambda_{21}\sqrt{2} \end{aligned}$$

κι έτσι $\mathrm{Tr}\,(a_1^*a_1) = id(\lambda_{11} + \lambda_{12}\sqrt{2}) + \sigma(\lambda_{11} + \lambda_{12}\sqrt{2}) = 2\lambda_{11}$ *άρα πρέπει* $2\lambda_{11} = 1$ *απ'όπου* $\lambda_{11} = \frac{1}{2}$. *Όμοια* $\mathrm{Tr}\,(a_1^*a_2) = 4\lambda_{12},\ \mathrm{Tr}\,(a_2^*a_1) = 2\lambda_{21}$ *και* $\mathrm{Tr}\,(a_2^*a_2) = 4\lambda_{22}$ *και έτσι* $\lambda_{12} = \lambda_{21} = 0$ *ενώ* $\lambda_{22} = \frac{1}{4}$ *συνεπώς η ζητούμενη βάση είναι η*

$$\left\{\frac{1}{2}, \frac{1}{4}\sqrt{2}\right\}$$

□

Ας είναι L/K μία πεπερασμένη επέκταση $Galois$ με αντίστοιχη ομάδα $Galois$ την G και $\alpha \in L$ τέτοιο ώστε το $(\sigma\alpha)_{\sigma\in G}$ να είναι κανονική βάση για το L πάνω από το K. Έστω $d(\tau, \sigma) \in K$ για $\sigma, \tau \in G$ να είναι τέτοια ώστε

$$\alpha \cdot \sigma\alpha = \sum_{\tau\in G} d(\tau, \sigma)\tau\alpha, \quad \text{για κάθε } \sigma \in G \tag{1.6}$$

Εφαρμόζωντας και στα δύο μέλη της (1.6) τον αυτομορφισμό σ^{-1} το πρώτο και το δεύτερο μέλος γίνονται αντίστοιχα

$$\sigma^{-1}(\alpha \cdot \sigma\alpha) = \sigma^{-1}\alpha \cdot \sigma^{-1}\sigma\alpha = \sigma^{-1}\alpha \cdot \alpha = \sum_{\tau\in G} d(\tau, \sigma^{-1})\tau\alpha$$

$$\begin{aligned} \sigma^{-1}\left(\sum_{\tau\in G} d(\tau,\sigma)\tau\alpha\right) &= \sum_{\tau\in G} \sigma^{-1}(d(\tau,\sigma))\sigma^{-1}(\tau\alpha) \\ &\overset{d(\tau,\sigma)\in K}{=} \sum_{\tau\in G} d(\tau,\sigma)\sigma^{-1}\tau\alpha \\ &\overset{\text{Θέτω } \sigma^{-1}\tau=\rho}{=} \sum_{\rho\in G} d(\sigma\rho,\sigma)\rho\alpha = \sum_{\tau\in G} d(\sigma\tau,\sigma)\tau\alpha \end{aligned}$$

απ'τις δύο τελευταίες σχέσεις και λόγω της (1.6) παίρνουμε ότι

$$d(\tau, \sigma^{-1}) = d(\sigma\tau, \sigma)$$

δηλαδή

$$d(\tau,\sigma) = d(\sigma^{-1}\tau, \sigma^{-1}), \quad \text{για κάθε} \quad \sigma, \tau \in G \tag{1.7}$$

Λόγω της Πρότασης 1.11 μπορούμε να επιλέξουμε μοναδικό $\beta \in L$ τέτοιο ώστε $\mathrm{Tr}\,(\beta \cdot \alpha) = 1$ και $\mathrm{Tr}\,(\beta \cdot \sigma\alpha) = 0$, για κάθε $\sigma \in G$ με $\sigma \neq id$.

Πρόταση 1.12 *Για το παραπάνω β που εκλέξαμε, καθώς επίσης για $\sigma, \tau \in G$ έχουμε*

$$\mathrm{Tr}\,(\sigma\beta \cdot \tau\alpha) = \begin{cases} 1, \textit{αν } \sigma = \tau \\ 0, \textit{αν } \sigma \neq \tau \end{cases}$$

Απόδειξη:

$$\begin{aligned}
\mathrm{Tr}\,(\sigma\beta\cdot\tau\alpha) &= \sum_{\rho\in G}\rho(\sigma\beta\cdot\tau\alpha)=\sum_{\rho\in G}\rho\sigma\beta\cdot\rho\tau\alpha \\
&\overset{\rho\sigma=\pi}{=} \sum_{\pi\in G}\pi\beta\cdot\pi\sigma^{-1}\tau\alpha=\sum_{\pi\in G}\pi(\beta\cdot\sigma^{-1}\tau\alpha) \\
&= \mathrm{Tr}\left(\beta\cdot\sigma^{-1}\tau\alpha\right)=\begin{cases}\mathrm{Tr}\,(\beta\cdot\alpha)=1, \text{αν } \sigma=\tau\\ \mathrm{Tr}\,(\beta\cdot\sigma\alpha)=0, \text{αν } \sigma\neq\tau\end{cases}
\end{aligned}$$

□

Πρόταση 1.13 *Το σύνολο $(\sigma\beta)_{\sigma\in G}$ με το β όπως ορίστηκε παραπάνω, αποτελεί κανονική βάση της επέκτασης $Galois$ L/K.*

Απόδειξη:

Άρκεί να δείξουμε ότι το σύνολο $(\sigma\beta)_{\sigma\in G}=\{\sigma_1,\ldots,\sigma_n\}$ αποτελείται από γραμμικώς ανεξάρτητα στοιχεία, αφού η επέκταση L/K είναι βαθμού n. Τότε θα είναι βάση η οποία λόγω της μορφής της, θα είναι κανονική . Έστω λοιπόν $k_1,\ldots,k_n\in K$ τέτοια ώστε

$$k_1\sigma_1\beta+\cdots+k_j\sigma_j\beta+\cdots+k_n\sigma_n\beta=0.$$

Τότε πολλαπλασιάζοντας τα δύο μέλη της παραπάνω με $\sigma_j\alpha,\ j=1,\ldots,n$ παίρνουμε

$$k_1\sigma_1\beta\cdot\sigma_j\alpha+\cdots+k_j\sigma_j\beta\cdot\sigma_j\alpha+\cdots+k_n\sigma_n\beta\cdot\sigma_j\alpha=0$$

και παίρνοντας το ίχνος έχουμε

$$k_1\underbrace{\mathrm{Tr}\,(\sigma_1\beta\cdot\sigma_j\alpha)}_{\to 0}+\cdots+k_j\underbrace{\mathrm{Tr}\,(\sigma_j\beta\cdot\sigma_j\alpha)}_{\to 1}+\cdots+k_n\underbrace{\mathrm{Tr}\,(\sigma_n\beta\cdot\sigma_j\alpha)}_{\to 0}=0$$

και έτσι $k_j = 0,\ \forall j = 1, \ldots, n$ που δείχνει ότι τα $(\sigma\beta)_{\sigma\in G}$ είναι γραμμικώς ανεξάρτητα.

Σημείωση: Η βάση αυτή είναι η δυϊκή της $(\sigma\alpha)_{\sigma\in G}$.

□

Πρόταση 1.14 *Για τα α, β όπως ορίστηκαν παραπάνω, ισχύει*

$$\alpha \cdot \tau\beta = \sum_{\sigma\in G} d(\tau, \sigma)\sigma\beta \tag{1.8}$$

Απόδειξη:

Έστω $\alpha \cdot \tau\beta = \sum_{\sigma\in G} d\,'(\tau, \sigma)\sigma\beta$. Πολλαπλασιάζοντας με $\rho\alpha$ έχουμε $\alpha \cdot \tau\beta \cdot \rho\alpha = \sum_{\sigma\in G} d\,'(\tau, \sigma)\sigma\beta \cdot \rho\alpha$ και παίρνοντας ίχνος , το κάθε μέλος της τελευταίας γίνεται

$$\begin{aligned} \mathrm{Tr}\,(\alpha \cdot \tau\beta \cdot \rho\alpha) &= \mathrm{Tr}\left(\underbrace{\alpha \cdot \rho\alpha}\cdot\tau\beta\right) = \mathrm{Tr}\left(\left(\sum_{\sigma\in G} d(\sigma, \rho)\sigma\alpha\right) \cdot \tau\beta\right) \\ &= \sum_{\sigma\in G} d(\sigma, \rho)\mathrm{Tr}\,(\sigma\alpha \cdot \tau\beta) \overset{\text{Πρόταση } (1.12)}{=} d(\tau, \rho) \end{aligned}$$

και

$$\mathrm{Tr}\left(\sum_{\sigma\in G} d\,'(\tau, \sigma)\sigma\beta \cdot \rho\alpha\right) = \sum_{\sigma\in G} d\,'(\tau, \sigma)\mathrm{Tr}\,(\sigma\beta \cdot \rho\alpha) = d\,'(\tau, \rho)$$

και έτσι $d(\tau, \rho) = d\,'(\tau, \rho)$, απ'όπου προκύπτει το ζητούμενο.

Σημείωση: Παρατηρούμε ότι ο πίνακας $(d(\tau,\sigma))_{\tau,\sigma\in G}$ της γραμμικής απεικόνισης $m_\alpha : L \to L$ με $x \mapsto \alpha \cdot x$, ως προς τη βάση $(\sigma\beta)_{\sigma\in G}$, που βρήκαμε παραπάνω, είναι ο ανάστροφος του πίνακα $(d(\sigma,\tau))_{\sigma,\tau\in G}$ της γραμμικής απεικόνισης $m_\alpha : L \to L$ με $x \mapsto \alpha \cdot x$, ως προς τη βάση $(\sigma\alpha)_{\sigma\in G}$

□

1.4 Αριθμητική σε πεπερασμένα σώματα

Ας δούμε πώς γίνεται η πρόσθεση και ο πολλαπλασιασμός στο $\mathbb{F}_{q^n}$ γενικά. Παρακάτω θα θεωρούμε το $\mathbb{F}_{q^n}$ σαν διανυσματικό χώρο διάστασης n πάνω από το $\mathbb{F}_q$. Ας είναι $\alpha_0, \alpha_1, \ldots \alpha_{n-1} \in \mathbb{F}_{q^n}$ γραμμικώς ανεξάρτητα διανύσματα του $\mathbb{F}_q$. Τότε κάθε στοιχείο $A \in \mathbb{F}_{q^n}$, γράφεται στη μορφή

$$A = \sum_{i=0}^{n-1} a_i \alpha_i, a_i \in \mathbb{F}_q$$

και καθώς το $\mathbb{F}_{q^n}$ είναι διανυσματικός χώρος διάστασης n πάνω από το $\mathbb{F}_q$, δηλαδή ισόμορφο με το $\mathbb{F}_q^n$, άρα το A μπορεί να γραφτεί ως $A = (a_0, a_1, \ldots, a_{n-1})$. Έστω $B = (b_0, b_1, \ldots, b_{n-1})$ ένα ακόμη στοιχείο του $\mathbb{F}_{q^n}$. Τότε η **πρόσθεση** A+B των στοιχείων γίνεται εύκολα αθροίζοντας κατά συντεταγμένη τις παραπάνω διατεταγμένες n-άδες.

Ο **πολλαπλασιασμός** των στοιχείων A,B είναι δυσκολότερη υπόθεση υπό την έννοια της γραφής του γινομένου ως γραμμικού συνδυασμού των στοιχείων της κανονικής βάσης. Γράφουμε $A \cdot B = C = (c_0, c_1, \ldots, c_{n-1})$. Θέλουμε να εκφράσουμε τα c_i όσο απλούστερα γίνεται και σε σχέση με τα a_i, b_i. Ας υποθέσουμε ότι

$$\alpha_i \alpha_j = \sum_{k=0}^{n-1} t_{ij}^{(k)} \alpha_k, \quad t_{ij}^{(k)} \in \mathbb{F}_q. \tag{1.9}$$

Τότε ισχύει

$$c_k = \sum_{i,j} a_i b_j t_{ij}^{(k)} = A T_k B^\top, \quad 0 \leq k \leq n-1,$$

όπου $T_k = \left(t_{ij}^{(k)}\right)$ είναι ένας $n \times n$ πίνακας πάνω από το $\mathbb{F}_q$ και $B^\top$ είναι ο ανάστροφος του B.

Ορισμός 1.10 *Η συλλογή των πινάκων* $\{T_k\}$ *καλείται* ***πολλαπλασιαστικός πίνακας*** *για το* $\mathbb{F}_{q^n}$ *πάνω από το* $\mathbb{F}_q$.

□

Οι πίνακες αυτοί είναι ανεξάρτητοι από τα A,B. Εάν το n είναι μεγάλο τότε αυτός ο τρόπος πολλαπλασιασμού δεν είναι πρακτικός. Όμως από τις βάσεις του $\mathbb{F}_{q^n}$ πάνω από το $\mathbb{F}_q$, υπάρχουν κάποιες για τις οποίες οι αντίστοιχοι πολλαπλασιαστικοί πίνακες είναι απλούστεροι από κάποιους άλλους με την έννοια ότι μπορεί να περιέχουν λιγότερα μη μηδενικά στοιχεία ή να είναι τέτοιοι ώστε εάν κάποιος επιλέξει με κάποιο τρόπο ένα αλγόριθμο πολλαπλασιασμού, να φτιάξει ένα πεπερασμένο σώμα για κάποιο μεγάλο n. Για παράδειγμα, διάφοροι τρόποι πολλαπλασιασμού που κάνουν χρήση δυϊκών βάσεων βρίσκονται στα [9], [14], [17], [18]. Εμείς θα κάνουμε χρήση του σχήματος των *Massey-Omura* [13] που κάνει χρήση της συμμετρίας των κανονικών βάσεων.

Ας δούμε καταρχήν το πλεονέκτημα της χρήσης κανονικών βάσεων. Έστω $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ μία κανονική βάση του $\mathbb{F}_{q^n}$ πάνω από το $\mathbb{F}_q$ όπου $\alpha^{q^i} = \alpha_i$. Τότε $\alpha^{q^k} = \alpha_{i+k}$ για κάθε ακέραιο k, όπου οι δείκτες του α είναι ειλημμένοι $\pmod n$.

Ας δούμε αρχικά, την περίπτωση **ύψωσης στη δύναμη** q. Τότε

$$\left(\sum_{i=0}^{n-1} a_i\alpha_i\right)^q = \sum_{i=0}^{n-1} a_i\alpha_{i+1}$$

και

$$\alpha_n = \alpha^{q^n} = \alpha_0.$$

Τότε το αντίστοιχο διάνυσμα του στοιχείου A^q είναι το

$$(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$$

δηλαδή κυκλική μετάθεση κατά μία θέση των συντεταγμένων του A, δηλαδή δεν υπάρχει υπολογιστικό «κόστος» για την ύψωση στη δύναμη q. Φυσικά αυτό γενικεύεται για **ύψωση στην** q^i απλά με κυκλική μετάθεση κατά i θέσεις. Συνεπώς, εάν $q = 2$, η ύψωση σε οποιαδήποτε δύναμη, μπορεί να επιταχυνθεί με τη μέθοδο των διαδοχικών τετραγωνισμών. Κάτι τέτοιο είναι πολύ σημαντικό στην εφαρμογή του κρυπτοσυστήματος ElGamal και του συστήματος ανταλλαγής κλειδιού Diffie-Hellman στα οποία χρειαζόμαστε να υπολογίσουμε μεγάλες δυνάμεις στοιχείων σε πεπερασμένα σώματα.

Πρόταση 1.15 *Ας είναι* $t_{ij}^{(k)}$ *όπως ορίστηκαν στην σχέση* (1.9) *και τα* $\alpha_i = \alpha^{q^i}$ *όπως παραπάνω. Τότε*

$$t_{ij}^{(l)} = t_{(i-l,j-l)}^{(0)},$$

για κάθε $0 \leq i, j, l \leq n-1$.

Απόδειξη:

Υψώνουμε τα μέλη της σχέσης (1.9) εις την q^{-l} και από τη μία έχουμε

$$\begin{aligned}(\alpha_i\alpha_j)^{q^{-l}} &= \alpha_{i-l}\alpha_{j-l} = \sum_{k=0}^{n-1} t_{(i-l,j-l)}^{(k)}\alpha_k \\ &= \sum_{k=0}^{n-1} t_{(i-l,j-l)}^{(k-l)}\alpha_{k-l}\end{aligned}$$

και από την άλλη

$$\left(\sum_{k=0}^{n-1} t_{ij}^{(k)}\alpha_k\right)^{q^{-l}} = \sum_{k=0}^{n-1} t_{ij}^{(k)}\alpha_{k-l},$$

απ'όπου παίρνουμε

$$t_{ij}^{(k)} = t_{(i-l,j-l)}^{(k-l)}$$

δηλαδή τη ζητούμενη παίρνοντας $k = l$.

□

Συνεπώς, εάν με κάποια διαδικασία μπορέσουμε να υπολογίσουμε τον συντελεστή c_0 με εισόδους τα A, B τότε με την ίδια διαδικασία και με εισόδους τα $A^{q^{-l}}, B^{q^{-l}}$ παίρνουμε το συντελεστή c_l (Όπως αναφέραμε και παραπάνω, τα $A^{q^{-l}}, B^{q^{-l}}$ είναι απλές κυκλικές μεταθέσεις κατά l θέσεις των A, B και έτσι το C υπολογίζεται απλά με n κυκλικές μεταθέσεις).

Έτσι βλέπουμε ότι στη διαδικασία αυτή θα θέλαμε να έχουμε όσο το δυνατόν λιγότερα μη μηδενικά στοιχεία στον πίνακα T_0. Αυτό μπορεί να γίνει εάν διαλέξουμε μία «κατάλληλη» κανονική βάση η οποία θα περιέχει όσο το δυνατόν λιγότερα μη μηδενικά στοιχεία στον T_0.

Θεωρούμε

$$\alpha\alpha_i = \sum_{j=0}^{n-1} t_{ij}\alpha_j, \;\; 0 \leq i \leq n-1, \; t_{ij} \in \mathbb{F}_q$$

και ας είναι T ο $n \times n$ πίνακας (t_{ij}). Τότε με όμοια διαδικασία όπως στην παραπάνω πρόταση (ύψωση αυτή τη φορά στη δύναμη k), παίρνουμε

$$t_{ij}^{(k)} = t_{i-j,k-j}$$

για κάθε i, j, k. Συνεπώς, ο αριθμός των μη μηδενικών στοιχείων του πίνακα T_0 ισούται με τον αριθμό των μη μηδενικών στοιχείων του πίνακα T που δεν είναι άλλος από τον πίνακα της γραμμικής απεικόνισης

$$\begin{aligned} m_\alpha : \mathbb{F}_{q^n} &\rightarrow \mathbb{F}_{q^n} \\ x &\mapsto \alpha \cdot x \end{aligned}$$

Παράδειγμα 1.3 *Θεωρούμε το σώμα* $\mathbb{F}_{2^5}$, α *μία ρίζα του αναγώγου πολυωνύμου* $f(x) = x^5 + x^2 + 1 \in \mathbb{F}_{2^5}$ *και παίρνουμε* $\beta = \alpha^3$. *Τότε το σύνολο* $N = \{\beta, \beta^2, \beta^4, \beta^8, \beta^{16}\}$ *είναι μία κανονική βάση του* $\mathbb{F}_{2^5}$ *πάνω από το* $\mathbb{F}_2$ *και ο πίνακας πολλαπλασιασμού των στοιχείων* $\beta^{2^i}\beta^{2^j}$, $0 \leq i, j \leq 4$ *γραμμένων ως προς την παραπάνω βάση φαίνεται στον πίνακα 1 και ο αντίστοιχος πίνακας* T_0 *της γραμμικής απεικόνισης* m_β *περιέχει 15 μη μηδενικά στοιχεία.*

2^i	2^j	β	β^2	β^4	β^8	β^{16}
1	1	0	1	0	0	0
1	2	0	1	1	1	0
1	4	1	1	1	0	1
1	8	1	0	1	1	1
1	16	1	1	1	0	0
2	1	0	1	1	1	0
2	2	0	0	1	0	0
2	4	0	0	1	1	1
2	8	1	1	1	1	0
2	16	1	1	0	1	1
4	1	1	1	1	0	1
4	2	0	0	1	1	1
4	4	0	0	0	1	0
4	8	1	0	0	1	1
4	16	0	1	1	1	1
8	1	1	0	1	1	1
8	2	1	1	1	1	0
8	4	1	0	0	1	1
8	8	0	0	0	0	1
8	16	1	1	0	0	1
16	1	1	1	1	0	0
16	2	1	1	0	1	1
16	4	0	1	1	1	1
16	8	1	1	0	0	1
16	16	1	0	0	0	0

Πίνακας 1: Πίνακας πολλαπλασιασμού της κανονικής βάσης N του παραδείγματος 1.3

Παράδειγμα 1.4 *Εάν πάρουμε και πάλι το ίδιο σώμα $\mathbb{F}_{2^5}$, α μία ρίζα του αναγώγου πολυωνύμου $f(x) = x^5 + x^2 + 1 \in \mathbb{F}_{2^5}$ και διαλέξουμε αυτή τη φορά $\beta = \alpha^5$, τότε το σύνολο $M = \{\beta, \beta^2, \beta^4, \beta^8, \beta^{16}\}$ είναι και πάλι μία κανονική βάση του $\mathbb{F}_{2^5}$ πάνω από το $\mathbb{F}_2$ και ο πίνακας πολλαπλασιασμού των στοιχείων $\beta^{2^i}\beta^{2^j},\ 0 \leq i, j \leq 4$ γραμμένων ως προς*

την παραπάνω βάση φαίνεται στον πίνακα 2 και ο αντίστοιχος πίνακας T_0 της γραμμικής απεικόνισης m_β περιέχει τώρα 9 μη μηδενικά στοιχεία. Όπως θα δείξουμε στην επόμενη παράγραφο, ο αριθμός αυτός των μη μηδενικών στοιχείων στον πίνακα T_0 είναι και ο ελάχιστος δυνατός.

2^i	2^j	β	β^2	β^4	β^8	β^{16}
1	1	0	1	0	0	0
1	2	1	0	0	1	0
1	4	0	0	0	1	1
1	8	0	1	1	0	0
1	16	0	0	1	0	1
2	1	1	0	0	1	0
2	2	0	0	1	0	0
2	4	0	1	0	0	1
2	8	1	0	0	0	1
2	16	0	0	1	1	0
4	1	0	0	0	1	1
4	2	0	1	0	0	1
4	4	0	0	0	1	0
4	8	1	0	1	0	0
4	16	1	1	0	0	0
8	1	0	1	1	0	0
8	2	1	0	0	0	1
8	4	1	0	1	0	0
8	8	0	0	0	0	1
8	16	0	1	0	1	0
16	1	0	0	1	0	1
16	2	0	0	1	1	0
16	4	1	1	0	0	0
16	8	0	1	0	1	0
16	16	1	0	0	0	0

Πίνακας 2: Πίνακας πολλαπλασιασμού της κανονικής βάσης M του παραδείγματος 1.4

Θα υπολογίσουμε τώρα το υπολογιστικό «κόστος» σε πράξεις, όταν δουλεύουμε σε κανονική βάση.

Θεωρούμε την κανονική βάση $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ όπως στα προηγούμενα και ας είναι T ο πίνακας της γραμμικής απεικόνισης ο οποίος θεωρούμε ότι έχει k σε πλήθος μη μηδενικά στοιχεία (άρα n^2-k

μηδενικά).

Τότε λόγω της σχέσης

$$\begin{aligned} m_\alpha(X) &= \alpha \cdot X = \sum_{i=0}^{n} x_i \alpha \alpha^{q^i} \\ &= (\alpha\ \alpha^q\ \ldots \alpha^{q^{n-1}}) \cdot T \cdot (x_0\ x_1\ \ldots x_{n-1})^\top, \\ &\quad \text{όπου}\ \ \mathbb{F}_{q^n} \ni X = \sum_{i=0}^{n} x_i \alpha^{q^i}, \end{aligned}$$

παίρνουμε ότι για την εύρεση του γινομένου $\alpha \cdot X$ (με την προϋπόθεση ότι γνωρίζουμε τον πίνακα T), απαιτούνται 2 πράξεις λιγότερες για κάθε μηδενικό που υπάρχει στον πίνακα T (ένας πολλαπλασιασμός και μία πρόσθεση).

Συνολικά λοιπόν έχουμε $2(n^2 - k)$ πράξεις λιγότερες δηλαδή θα εκτελέσουμε $2n^2 - 2(n^2 - k) = 2k$ πράξεις.

Ας θεωρήσουμε τα στοιχεία

$$A = \sum_{i=0}^{n-1} a_i \alpha^{q^i}, a_i \in \mathbb{F}_q, \quad B = \sum_{i=0}^{n-1} b_i \alpha^{q^i}, b_i \in \mathbb{F}_q$$

όπου τώρα το X είναι το B. Τότε

$$AB = \sum_{i=0}^{n-1} a_i X \alpha^{q^i}.$$

Λόγω της σχέσης

$$\alpha^{q^i} \cdot x = \alpha^{q^i} \cdot x^{q^i q^{n-i}} = \left(\alpha \cdot x^{q^{n-i}}\right)^{q^i},$$

και θεωρώντας ότι η κυκλική μετάθεση των συντεταγμένων δεν έχει κάποιο υπολογιστικό «κόστος», συμπεραίνουμε ότι για τον υπολογισμό του $X\alpha^{q^i}$ χρειάζονται $2k$ πράξεις οι οποίες μαζί με τον πολλαπλασιασμό με a_i, δίνουν σύνολο $2k+n$ πράξεων. Αυτό το κάνουμε για κάθε όρο του αθροίσματος (οπότε σύνολο έως τώρα $(2k+n)n$ πράξεις) και έτσι κάθε τέτοιο όρο τον γράφουμε σαν γραμμικό συνδυασμό στοιχείων της κανονικής βάσης. Για την ομαδοποίηση των στοιχείων χρειάζονται επιπλέον $n-1$ προσθέσεις για να βρούμε τον συντελεστή καθενός από τα α^{q^i} και συνολικά έχουμε να υπολογίσουμε n σε πλήθος τέτοιους συντελεστές. Άρα τελικά, έχουμε σύνολικά

$$(2k+n)n + n(n-1) \text{ πράξεις},$$

για να υπολογίσουμε ένα και μόνο γινόμενο δύο στοιχείων της βάσης και να το γράψουμε σαν γραμμικό συνδυασμό των στοιχείων της κανονικής βάσης.

Στην περίπτωση βέλτιστης κανονικής βάσης χρειαζόμαστε

$$(2(2n-1)+n)\,n + n(n-1) = 6n^2 - 3n = O(n^2) \text{ πράξεις}$$

ενώ εάν έχουμε πολυπλοκότητα n^2 ή $\dfrac{n^2}{2}$ (δηλαδή όλα ή τα μισά στοιχεία στον πίνακα T είναι μη μηδενικά αντίστοιχα) τότε χρειαζόμαστε $(2n^2+n)n+n(n-1) = 2n^3+2n^2-n$ ή $\left(2\dfrac{n^2}{2}+n\right)n+n(n-1) = n^3+2n^2-n$ αντίστοιχα δηλαδή και στις δύο περιπτώσεις $O(n^3)$ πράξεις.

Η διαφορά αυτή αρχίζει να γίνεται αισθητή όταν αυξάνεται το n πράγμα που συμβαίνει στην Κρυπτογραφία.

Για παράδειγμα στο σώμα $\mathbb{F}_{2^{508}}$, στο οποίο όπως θα δούμε παρακάτω υπάρχει βέλτιστη κανονική βάση, χρειαζόμαστε $6 \cdot 508^2 - 3 \cdot 508 = 1.546.860$ πράξεις για να εκτελέσουμε τον πολλαπλασιασμό μεταξύ δύο

μόνο στοιχείων με τη χρήση βέλτιστης κανονικής βάσης. Εάν λοιπόν θέλουμε να κάνουμε κρυπτογράφηση ενός μηνύματος, χρειαζόμαστε μερικές δεκάδες εκατομμύρια πράξεις! Πόσες πράξεις θα είχαμε άραγε εάν αντί για βέλτιστη κανονική βάση, χρησιμοποιούσαμε μία κανονική βάση που μάλιστα έχει πολλά μη μηδενικά στοιχεία στον πίνακα T της αντίστοιχης γραμμικής απεικόνισης (π.χ. αν τα μισά στοιχεία ήταν μη μηδενικά θα χρειαζόμασταν $508^3 + 2 \cdot 508^2 - 508 = 131.612.132$ πράξεις για τον πολλαπλασιασμό μεταξύ δύο και μόνο στοιχείων!!!);

Στα παραδείγματα 1.3, 1.4 παραπάνω, δεν είναι αισθητή η διαφορά των πράξεων που πρέπει να εκτελεστούν για την εύρεση του γινομένου δύο στοιχείων του $\mathbb{F}_{2^5}$ και είναι λογικό αφού το n είναι μικρό.

2 Χαρακτηρισμός βέλτιστων κανονικών βάσεων Πεπερασμένων επεκτάσεων Galois

2.1 Βέλτιστες κανονικές Βάσεις

Θεωρούμε την γραμμική απεικόνιση

$$\begin{aligned} m_\alpha : L &\rightarrow L \\ x &\mapsto \alpha \cdot x, \end{aligned}$$

και μία κανονική βάση $(\sigma\alpha)_{\sigma\in G}$ του L πάνω από το K και ας υποθέσουμε ότι τα $d(\tau,\sigma) \in K$ με $\sigma,\tau \in G$ είναι τέτοια ώστε

$$\alpha \cdot \sigma\alpha = \sum_{\tau\in G} d(\tau,\sigma)\tau\alpha, \quad \text{για κάθε } \sigma \in G \text{ [2]} \tag{2.1}$$

Ορισμός 2.1 *Το πλήθος των μη μηδενικών στοιχείων του πίνακα της απεικόνισης m_α ονομάζεται* ***πολυπλοκότητα*** *του α.*

□

Παράδειγμα 2.1 *Η βάση N του παραδείγματος 1.3 έχει πολυπλοκότητα* 15.

□

[2] Ουσιαστικά ο $(d(\tau,\sigma))$ για $\tau,\sigma \in G$ είναι ο πίνακας της γραμμικής απεικόνισης m_α ως προς την κανονική βάση $(\sigma\alpha)_{\sigma\in G}$.

Πρόταση 2.1 *Η πολυπλοκότητα του α ως προς την κανονική βάση $(\sigma\alpha)_{\sigma\in G}$, είναι τουλάχιστον $2n-1$ δηλαδή*

$$\sharp\{(\sigma,\tau)\in G\times G : d(\tau,\sigma)\neq 0\}\geq 2n-1$$

Απόδειξη:

Αθροίζοντας την (2.1) ως προς σ, το πρώτο μέλος γίνεται

$$\sum_{\sigma\in G}\alpha\cdot\sigma\alpha=\alpha\cdot\sum_{\sigma\in G}\sigma\alpha=\alpha\cdot\mathrm{Tr}\,(\alpha)$$

και από την άλλη το δεύτερο μέλος γίνεται

$$\sum_{\sigma\in G}\sum_{\tau\in G}d(\tau,\sigma)\tau\alpha=\sum_{\tau\in G}\underbrace{\left(\sum_{\sigma\in G}d(\tau,\sigma)\right)}_{\in K}\tau\alpha$$

Έτσι έχουμε

$$\alpha\cdot\mathrm{Tr}\,(\alpha)=\sum_{\tau\in G}\left(\sum_{\sigma\in G}d(\tau,\sigma)\right)\tau\alpha$$

Όμως το α είναι κάποιο στοιχείο της βάσης $(\sigma\alpha)_{\sigma\in G}$ καθώς μέσα σε αυτή υπάρχει ο ταυτοτικός αυτομορφισμός id άρα η τελευταία ισότητα είναι ισότητα μεταξύ γραμμικών συνδυασμών στοιχείων της βάσης και έτσι προκύπτει ότι

$$\sum_{\sigma\in G}d(id,\sigma)=\mathrm{Tr}\,(\alpha)\tag{2.2}$$

και

$$\sum_{\sigma\in G}d(\tau,\sigma)=0,\quad\text{για }\tau\neq id\tag{2.3}$$

Χωρίς βλάβη της γενικότητος υποθέτουμε ότι το πρώτο διάνυσμα της κανονικής βάσης είναι το α. Ισχυριζόμαστε ότι κάθε γραμμή έχει τουλάχιστον ένα μη μηδενικό στοιχειο διότι εάν υπήρχε μία γραμμή που να ήταν όλα τα στοιχεία της μηδενικά τότε η ορίζουσα της γραμμικής απεικόνισης m_α θα ήταν ίση με το μηδέν, πράγμα αδύνατο αφού τότε η απεικόνιση δεν θα ήταν ένα προς ένα. Από την άλλη η ισότητα (2.3) δείχνει ότι σε κάθε γραμμή, πλην της πρώτης, θα πρέπει να υπάρχουν τουλάχιστον δύο μη μηδενικά στοιχεία (αν μάλιστα υπάρχουν ακριβώς δύο, τότε έχουν αντίθετο πρόσημο) άρα συνολικά $n-1$ γραμμές έχουν τουλάχιστον $2(n-1) = 2n-2$ μη μηδενικά στοιχεία. Τέλος, στην πρώτη γραμμή έχω ένα τουλάχιστον μη μηδενικό στοιχείο (Εάν υπήρχε ακριβώς ένα τότε θα ήταν το $\mathrm{Tr}\,(\alpha)$). Συνολικά λοιπόν, έχουμε τουλάχιστον $2n-2+1 = 2n-1$ μη μηδενικά στοιχεία.

□

Ορισμός 2.2 *Η κανονική βάση $(\sigma\alpha)_{\sigma\in G}$ ονομάζεται* **βέλτιστη**, *εάν η πολυπλοκότητα του α είναι ακριβώς $2n-1$ δηλαδή ισχύει η ισότητα στην Πρόταση 2.1.*

□

Παράδειγμα 2.2 *Έστω p πρώτος και ζ μία p ρίζα της μονάδος διαφορετική του 1. Τότε το σύνολο $\left\{\zeta^i, 1 \le i \le p-1\right\}$ αποτελεί μία βέλτιστη κανονική βάση της επέκτασης $\mathbb{Q}(\zeta)/\mathbb{Q}$.*

Απόδειξη:

Αφού ζ μία p ρίζα της μονάδος διαφορετική του 1 άρα $\zeta^p = 1,\ \zeta \neq 1$. Από το Λήμμα 4.1, το πολυώνυμο $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$

είναι ανάγωγο πάνω από το $\mathbb{Q}$ *και η επέκταση* $\mathbb{Q}(\zeta)/\mathbb{Q}$ *είναι* $Galois$ *με αντίστοιχη ομάδα* $Galois$ *την*

$$G = \left\{\sigma_i,\ 1 \leq i \leq p-1 : \sigma_i(\zeta) = \zeta^i\right\}.$$

Το ότι κάθε στοιχείο του $\mathbb{Q}(\zeta)$ *γράφεται ως συνδυασμός των* ζ^i *είναι προφανές ενώ για την γραμμική ανεξαρτησία αυτών υποθέτουμε ότι υπάρχουν* $\lambda_1, \cdots, \lambda_{p-1} \in \mathbb{Q}$ *όχι όλα μηδέν ώστε* $\lambda_1\zeta + \lambda_2\zeta^2 + \cdots + \lambda_{p-1}\zeta^{p-1} = 0$. *Εάν* λ_k *είναι το «μέγιστο» μη μηδενικό* $\lambda_i,\ 1 \leq i \leq p-1$, *υπό την έννοια ότι το* k *είναι μέγιστο, τότε αφού* $\zeta \neq 0$, *άρα* $\lambda_1 + \lambda_2\zeta + \cdots + \lambda_k\zeta^{k-1} = 0$. *Εάν* $k = 1$ *τελειώσαμε ενώ εάν* $k \geq 2$ *τότε το* ζ *είναι ρίζα ενός πολυωνύμου βαθμού* $k-1$. *Συνεπώς πρέπει το ανάγωγο του* ζ, *που είναι το* $f(x)$ *να το διαιρεί, άτοπο. Άρα* $\lambda_k = 0$, *άτοπο. Συνεπώς* $\lambda_i = 0,\ \forall i \in \{1, 2, \ldots, p-1\}$. *Άρα το σύνολο* $\left\{\zeta^i,\ 1 \leq i \leq p-1\right\}$ *αποτελεί βάση της παραπάνω επέκτασης και μάλιστα κανονική λόγω της μορφής της.*

Για την γραμμική απεικόνιση

$$\begin{aligned} m_\zeta : \mathbb{Q}(\zeta) &\rightarrow \mathbb{Q}(\zeta) \\ x &\mapsto \zeta \cdot x \end{aligned}$$

έχουμε

$m_\zeta(\zeta) = \zeta \cdot \zeta = \zeta^2 = [0, 1, 0, 0 \ldots, 0, 0] \cdot A$

$m_\zeta(\zeta^2) = \zeta \cdot \zeta^2 = \zeta^3 = [0, 0, 1, 0 \ldots, 0, 0] \cdot A$

$\vdots$

$m_\zeta(\zeta^{p-2}) = \zeta \cdot \zeta^{p-2} = \zeta^{p-1} = [0, 0, 0, 0 \ldots, 0, 1] \cdot A$

$$\begin{aligned} m_\zeta(\zeta^{p-1}) &= \zeta \cdot \zeta^{p-1} = \zeta^p = 1 = -1 - \zeta - \cdots - \zeta^{p-1} \\ &= [-1, -1, -1, -1 \ldots, -1, -1] \cdot A \end{aligned}$$

όπου $A := [\zeta, \zeta^2, \ldots, \zeta^{p-1}]^\top$

και έτσι ο αντίστοιχος πίνακας της γραμμικής απεικόνισης είναι ο

$$\left[\begin{array}{cccc|c} 0 & 0 & \cdots & 0 & -1 \\ \hline & & & & -1 \\ & & & & -1 \\ & I_{p-1} & & & \vdots \\ & & & & -1 \end{array}\right]$$

απ'όπου φαίνεται ότι η κανονική βάση που επιλέξαμε είναι βέλτιστη .

Σημείωση : Παρατηρήστε ότι το άνω δεξιά στοιχείο της πρώτης γραμμής είναι το μοναδικό μη μηδενικό εκείνης της γραμμής και είναι ίσο με το $\mathrm{Tr}\,(\zeta)$.

□

Παράδειγμα 2.3 *Η βάση* M *του παραδείγματος 1.4, είναι βέλτιστη κανονική βάση της επέκτασης* $\mathbb{F}_{2^5}/\mathbb{F}_2$ *αφού η πολυπλοκότητά της είναι* $2 \cdot 5 - 1 = 9$.

□

Πόρισμα 2.1 *Εάν η* $(\sigma\alpha)_{\sigma\in G}$ *είναι βέλτιστη κανονική βάση της επέκτασης* $Galois\ L/K$*, τότε*

(*i*) *Για κάθε* $\tau \in G,\ \tau \neq id$*, υπάρχουν ακριβώς δύο στοιχεία* $\sigma_1, \sigma_2 \in G$ *για τα οποία* $d(\tau, \sigma_1), d(\tau, \sigma_2) \neq 0$ *και* $d(\tau, \sigma_1) + d(\tau, \sigma_2) = 0$.

(*ii*) *Υπάρχει ακριβώς ένα στοιχείο* $\mu \in G$ *για το οποίο* $d(id, \mu) \neq 0$*, και γι' αυτό το στοιχείο ισχύει*

$$d(id, \mu) = \mathrm{Tr}\,(\alpha)\,.$$

□

Παρατήρηση: Στο εξής η $(\sigma\alpha)_{\sigma\in G},\ \alpha \in L$ είναι βέλτιστη κανονική βάση της επέκτασης $Galois\ L/K$ και το $\beta \in L$ που θα χρησιμοποιείται παρακάτω, είναι το στοιχείο για το οποίο η $(\sigma\beta)_{\sigma\in G}$ είναι η αντίστοιχη δυϊκή βάση όπως ορίστηκε στην παράγραφο 1.3.

Πόρισμα 2.2 *Για κάθε $\tau \in G,\ \tau \neq id$, το $\alpha \cdot \tau\beta$ ισούται με ένα στοιχείο του K^* επί τη διαφορά δύο διακεκριμένων συζυγών του β, ενώ $\alpha \cdot \beta = \mathrm{Tr}\,(\alpha) \cdot \mu\beta$.*

Απόδειξη:

Όπως αναφέραμε στην πρώτη περίπτωση του παραπάνω πορίσματος, για κάθε $\tau \in G,\ \tau \neq id$, υπάρχουν ακριβώς δύο στοιχεία $\sigma_1, \sigma_2 \in G$ για τα οποία $d(\tau, \sigma_1), d(\tau, \sigma_2) \neq 0$ και $d(\tau, \sigma_1) + d(\tau, \sigma_2) = 0$. Άρα

$$\begin{aligned} \alpha \cdot \tau\beta &= \sum_{\sigma\in G} d(\tau,\sigma)\sigma\beta = d(\tau,\sigma_1)\sigma_1\beta + d(\tau,\sigma_2)\sigma_2\beta \\ &= d(\tau,\sigma_1)(\sigma_1\beta - \sigma_2\beta) \end{aligned}$$

Τέλος, όταν βρισκόμαστε στη δεύτερη περίπτωση του παραπάνω πορίσματος, έχουμε

$$\alpha \cdot \beta = \sum_{\sigma\in G} d(id,\sigma)\sigma\beta = d(id,\mu)\mu\beta = \mathrm{Tr}\,(\alpha) \cdot \mu\beta$$

□

Σημείωση: Αντικαθιστώντας το α με $c\alpha$, $c = -\frac{1}{\mathrm{Tr}(\alpha)}$, μπορούμε χωρίς βλάβη της γενικότητος, να υποθέτουμε στο εξής ότι $\mathrm{Tr}(\alpha) = -1$. Συνεπώς

$$\alpha \cdot \beta = -\mu\beta \tag{2.4}$$

Πρόταση 2.2 *Ισχύει* $(\mathrm{Tr}(\alpha))(\mathrm{Tr}(\beta)) = 1$

Απόδειξη:

$$\begin{aligned} (\mathrm{Tr}(\alpha))(\mathrm{Tr}(\beta)) &= \mathrm{Tr}(\mathrm{Tr}(\alpha)\cdot\beta) = \mathrm{Tr}(\mathrm{Tr}(\alpha)\cdot\mu\beta) \\ (\text{Πόρισμα } 2.2) &= \mathrm{Tr}(\alpha\cdot\beta) = 1 \end{aligned}$$

□

Πόρισμα 2.3 *Από την υπόθεση ότι* $\mathrm{Tr}(\alpha) = -1$ *και την παραπάνω Πρόταση, παίρνουμε* $\mathrm{Tr}(\beta) = -1$.

Λήμμα 2.1 *Ισχύει*

$$d(id,\sigma) = \begin{cases} -1, & \text{αν } \sigma = \mu \\ 0, & \text{αν } \sigma \neq \mu \end{cases}$$

Απόδειξη:

Από τη σχέση (1.8) έχουμε

$$-\mu\beta = \alpha\cdot\beta = \alpha\cdot id\beta = \sum_{\sigma\in G} d(id,\sigma)\sigma\beta = d(id,\mu)\mu\beta + \sum_{\substack{\sigma\in G\\ \sigma\neq\mu}} d(id,\sigma)\sigma\beta$$

□

Πόρισμα 2.4 *Βάσει της σχέσης* (1.7) *έχουμε*

$$d(\sigma,\sigma)=\begin{cases} -1, & \text{αν } \sigma=\mu^{-1} \\ 0, & \text{αν } \sigma\neq\mu^{-1} \end{cases} \tag{2.5}$$

□

Πόρισμα 2.5 *Εάν τα* α,β *είναι όπως έχουν οριστεί παραπάνω και* $\mu^{-1}\neq id$*, τότε υπάρχει* $\lambda\in G$ *με* $\lambda\neq\mu^{-1}$*, τέτοιο ώστε*

$$\alpha\cdot\mu^{-1}\beta=-\mu^{-1}\beta+\lambda\beta \tag{2.6}$$

Απόδειξη:

Αφού υποθέσαμε ότι $\mu^{-1}\neq id$ *(δηλαδή* $\mu\neq id$*), άρα*

$$\alpha\cdot\mu^{-1}\beta=\sum_{\sigma\in G}d(\mu^{-1},\sigma)\sigma\beta=d(\mu^{-1},\mu^{-1})\mu^{-1}\beta+\sum_{\substack{\sigma\in G\\ \sigma\neq\mu^{-1}}}d(\mu^{-1},\sigma)\sigma\beta$$

και από την άλλη

$$\alpha\cdot id\beta=\alpha\cdot\beta\overset{2.4}{=}-\mu\beta.$$

Άρα πρέπει $d(id,\mu)=-1$ *και* $d(id,\sigma)=0,\ \forall\,\sigma\in G$*, με* $\sigma\neq\mu$ [3]

Λόγω του παραπάνω πορίσματος (2.4) *έχουμε* $d(\mu^{-1},\mu^{-1})=-1$ *και συνεπώς από το πόρισμα* (2.1) *υπάρχει* $\lambda\in G$ *με* $\lambda\neq\mu^{-1}$ *ώστε* $d(\mu^{-1},\lambda)=1$*, ενώ* $d(\mu^{-1},\sigma)=0,\ \forall\,\sigma\in G$*, με* $\sigma\neq\lambda,\mu^{-1}$*. Άρα τελικά*

$$\alpha\cdot\mu^{-1}\beta=-\mu^{-1}\beta+\lambda\beta$$

□

[3]Διότι βρισκόμαστε στην πρώτη γραμμή του πίνακα της γραμμικής απεικόνισης συνεπώς όλοι οι συντελεστές είναι μηδέν εκτός επό εκείνο που έχει συντελεστή το $d(id,\mu)=-1$.

2.2 Τρείς χρήσιμες σχέσεις

Πρόταση 2.3 *Έστω L/K επέκταση $Galois$ με αντίστοιχη ομάδα $Galois$ την G και $\alpha \in L$, τέτοιο ώστε $(\sigma\alpha)_{\sigma\in G}$ να είναι βέλτιστη κανονική βάση, $\mathrm{Tr}\,(\alpha) = -1$, ενώ $\beta \in L$ τέτοιο ώστε, η $(\sigma\beta)_{\sigma\in G}$ να είναι η αντίστοιχη δυϊκή βάση και τέλος τα $\mu, \lambda \in G$ να ικανοποιούν τις σχέσεις*

$$\alpha \cdot \beta = -\mu\beta, \tag{2.7}$$

$$\alpha \cdot \mu^{-1}\beta = -\mu^{-1}\beta + \lambda\beta, \;\; \lambda \neq \mu^{-1}, \tag{2.8}$$

και

$$\mu^2 \neq id.$$

Τότε ισχύουν τα εξής:

$$\mathrm{char}K = 2 \tag{2.9}$$

$$\alpha \cdot \mu\beta = \lambda\mu\beta + \beta \tag{2.10}$$

$$\lambda\mu = \mu\lambda \tag{2.11}$$

Απόδειξη:

Η κύρια τεχνική που θα ακολουθήσουμε βασίζεται στην προφανή ταυτότητα

$$\rho\alpha\,(\sigma\alpha \cdot \tau\beta) = \sigma\alpha\,(\rho\alpha \cdot \tau\beta)$$

για διάφορες επιλογές των $\rho, \sigma, \tau \in G$. Με τον τρόπο αυτό θα γράφουμε με δύο διαφορετικούς τρόπους το γινόμενο των αυτομορφισμών και θα συνδυάζουμε τα τελικά αποτελέσματα.

Πολλαπλασιάζουμε τη σχέση (2.7) επί $\mu\alpha$ και παίρνουμε

$$\mu\alpha(\alpha\cdot\beta)=\mu\alpha(-\mu\beta)=-\mu(\alpha\cdot\beta)\overset{(2.7)}{=}-\mu(-\mu\beta)=\mu^2\beta \qquad (2.12)$$

Από την άλλη, το $\mu\alpha(\alpha\cdot\beta)$ γραμμένο διαφορετικά ως $\alpha(\mu\alpha\cdot\beta)$ δίνει

$$\begin{aligned}\alpha(\mu\alpha\cdot\beta) &= \alpha\cdot\mu(\alpha\cdot\mu^{-1}\beta)\overset{(2.8)}{=}\alpha\cdot\mu(\lambda\beta-\mu^{-1}\beta)\\ &= \alpha\cdot\mu\lambda\beta-\alpha\cdot\beta=\alpha\cdot\mu\lambda\beta+\mu\beta \qquad (2.13)\end{aligned}$$

Συνεπώς από τις σχέσεις $(2.12), (2.13)$, έχουμε

$$\alpha\cdot\mu\lambda\beta=\mu^2\beta-\mu\beta \qquad (2.14)$$

Από το ότι $\mu\neq\mu^{-1}$ και την (2.38) παίρνουμε $d(\mu,\mu)=0$ άρα από την (2.14) έχουμε ότι $\lambda\neq id$ διότι διαφορετικά θα είχαμε $\alpha\cdot\mu\beta=\mu^2\beta-\mu\beta$. Όμως

$$\begin{aligned}\alpha\cdot\mu\beta &= \sum_{\sigma\in G}d(\mu,\sigma)\sigma\beta=\cancelto{0}{d(\mu,\mu)}\mu\beta+\sum_{\substack{\sigma\in G\\ \sigma\neq\mu}}d(\mu,\sigma)\sigma\beta\\ &= \sum_{\substack{\sigma\in G\\ \sigma\neq\mu}}d(\mu,\sigma)\sigma\beta,\ \text{άτοπο}\end{aligned}$$

$$\text{Άρα}\quad \lambda\neq id. \qquad (2.15)$$

Από την σχέση (2.8) έχουμε $\alpha\cdot\mu^{-1}\beta=\lambda\beta-\mu^{-1}\beta$, όμως

$$\alpha\cdot\mu^{-1}\beta=\sum_{\sigma\in G}d(\mu^{-1},\sigma)\sigma\beta=d(\mu^{-1},\lambda)\lambda\beta+\sum_{\substack{\sigma\in G\\ \sigma\neq\lambda}}d(\mu^{-1},\sigma)\sigma\beta \qquad (2.16)$$

Άρα $d(\mu^{-1},\lambda)=1$ και $d(\mu^{-1},\mu^{-1})=-1$, το οποίο σημαίνει επίσης ότι $\lambda\neq\mu^{-1}$ δηλαδή $\lambda^{-1}\mu^{-1}\neq id$. Συνεπώς από την (1.7) προκύπτει ότι

$$d(\lambda^{-1}\mu^{-1},\lambda^{-1})=d(\mu^{-1},\lambda)=1. \tag{2.17}$$

Επίσης, αφού $\lambda^{-1}\mu^{-1}\neq id$, άρα λόγω της

$$\begin{aligned}\alpha\cdot\lambda^{-1}\mu^{-1}\beta &= \sum_{\sigma\in G} d(\lambda^{-1}\mu^{-1},\sigma)\sigma\beta = \cancelto{1}{d(\lambda^{-1}\mu^{-1},\lambda^{-1})}\lambda^{-1}\beta \\ &+ \sum_{\substack{\sigma\in G\\ \sigma\neq\lambda^{-1}}} d(\lambda^{-1}\mu^{-1},\sigma)\sigma\beta \end{aligned}\tag{2.18}$$

πρέπει να υπάρχει $\kappa\in G,\ \kappa\neq\lambda^{-1}$ τέτοιο ώστε $d(\lambda^{-1}\mu^{-1},\kappa)=-1$ (οπότε $d(\lambda^{-1}\mu^{-1},\sigma)=0,\ \sigma\neq\lambda^{-1},\kappa$) συνεπώς έχουμε τελικά

$$\alpha\cdot\lambda^{-1}\mu^{-1}\beta=\lambda^{-1}\beta-\kappa\beta. \tag{2.19}$$

Από τη σχέση (2.15) έχουμε $\lambda^{-1}\mu^{-1}\neq\mu^{-1}$, άρα η σχέση (2.38) δίνει

$$d(\lambda^{-1}\mu^{-1},\lambda^{-1}\mu^{-1})=0,$$

που σημαίνει ότι

$$\kappa\neq\lambda^{-1}\mu^{-1}. \tag{2.20}$$

Επίσης

$$\begin{aligned} \lambda\alpha(\alpha\cdot\mu^{-1}\beta) &\overset{(2.8)}{=} \lambda\alpha(\lambda\beta-\mu^{-1}\beta)=\lambda(\alpha\cdot\beta-\alpha\cdot\lambda^{-1}\mu^{-1}\beta) \\ &\overset{(2.7),(2.19)}{=} \lambda(-\mu\beta+\kappa\beta-\lambda^{-1}\beta) \\ &= -\lambda\mu\beta+\lambda\kappa\beta-\beta \end{aligned} \tag{2.21}$$

και η παραπάνω παράσταση $\lambda\alpha(\alpha\cdot\mu^{-1}\beta)$ γραμμένη διαφορετικά, ως $\alpha\cdot(\lambda\alpha\cdot\mu^{-1}\beta)$, δίνει

$$\begin{aligned} \alpha\cdot(\lambda\alpha\cdot\mu^{-1}\beta) &= \alpha\cdot\lambda(\alpha\cdot\lambda^{-1}\mu^{-1}\beta)\overset{(2.19)}{=}\alpha\cdot\lambda(\lambda^{-1}\beta-\kappa\beta) \\ &= \alpha\cdot(\beta-\lambda\kappa\beta)\overset{(2.7)}{=}-\mu\beta-\alpha\cdot\lambda\kappa\beta \end{aligned} \tag{2.22}$$

και έτσι από τις σχέσεις $(2.38), (2.8)$ παίρνουμε

$$\alpha\cdot\lambda\kappa\beta=-\mu\beta+\lambda\mu\beta+\beta-\lambda\kappa\beta \tag{2.23}$$

Από τη σχέση (2.20), έχουμε $\lambda\kappa\neq\mu^{-1}$ άρα από την σχέση (2.38) έχουμε $d(\lambda\kappa,\lambda\kappa)=0$, συνεπώς ο όρος $-\lambda\kappa\beta$ δε θα έπρεπε να εμφανίζεται στο $\alpha\cdot\lambda\kappa\beta$ της σχέσης (2.23), συνεπώς πρέπει να απλοποιείται με κάποιον από τους υπόλοιπους όρους. Όμως από τη σχέση (2.19) έχουμε $\lambda\kappa\neq id$, άρα δεν διαγράφεται με το β. Συνεπώς διαγράφεται είτε με το $\lambda\mu\beta$ είτε με το $-\mu\beta$. Θα υποθέσουμε ότι διαγράφεται με το $\lambda\mu\beta$ και θα καταλήξουμε σε άτοπο.

Ας υποθέσουμε λοιπόν ότι $\lambda\kappa\beta=\lambda\mu\beta$. Τότε $\kappa=\mu$ άρα η σχέση (2.23) δίνει

$$\alpha\cdot\lambda\mu\beta=\beta-\mu\beta \tag{2.24}$$

Επίσης,

$$\alpha \cdot \lambda\mu\beta = \sum_{\sigma\in G} d(\lambda\mu,\sigma)\sigma\beta = d(\lambda\mu,\mu)\mu\beta + \sum_{\substack{\sigma\in G\\ \sigma\neq\mu}} d(\lambda\mu,\sigma)\sigma\beta,$$

άρα λόγω της σχέσης (2.24) πρέπει $d(\lambda\mu,\mu) = -1$ και λόγω της (1.7) έχουμε $d(\mu^{-1}\lambda\mu,\mu^{-1}) = d(\lambda\mu,\mu) = -1$.

Από την άλλη,

$$\begin{aligned}\alpha \cdot \mu^{-1}\lambda\mu\beta = \sum_{\sigma\in G} d(\mu^{-1}\lambda\mu,\sigma)\sigma\beta &= \cancelto{-1}{d(\mu^{-1}\lambda\mu,\mu^{-1})}\mu^{-1}\beta \\ &+ \sum_{\substack{\sigma\in G\\ \sigma\neq\mu^{-1}}} d(\mu^{-1}\lambda\mu,\sigma)\sigma\beta,\end{aligned}$$

και επειδή λόγω της (2.15) έχουμε ότι $\mu^{-1}\lambda\mu \neq id$, άρα υπάρχει $\nu \in G,\ \nu \neq \mu^{-1}$, τέτοιο ώστε

$$\alpha \cdot \mu^{-1}\lambda\mu\beta = -\mu^{-1}\beta + \nu\beta. \tag{2.25}$$

Έτσι, από τη μία έχουμε ότι

$$\begin{aligned}\alpha \cdot (\mu\alpha \cdot \lambda\mu\beta) &= \alpha \cdot \mu(\alpha \cdot \mu^{-1}\lambda\mu\beta) \overset{(2.25)}{=} \alpha \cdot \mu(\nu\beta - \mu^{-1}\beta) \\ &= \alpha \cdot \mu\nu\beta - \alpha \cdot \beta \overset{(2.7)}{=} \alpha \cdot \mu\nu\beta + \mu\beta \end{aligned} \tag{2.26}$$

ενώ από την άλλη, εάν γράψουμε το $\alpha \cdot (\mu\alpha \cdot \lambda\mu\beta) = \mu\alpha(\alpha \cdot \lambda\mu\beta)$, διαφορετικά έχουμε,

$$\begin{aligned} \mu\alpha(\alpha\cdot\lambda\mu\beta) &\overset{(2.24)}{=} \mu\alpha(\beta-\mu\beta)=\mu(\alpha\cdot\mu^{-1}\beta-\alpha\cdot\beta) \\ &\overset{(2.8),(2.7)}{=} \mu(\lambda\beta-\mu^{-1}\beta+\mu\beta)=\mu\lambda\beta-\beta+\mu^2\beta \end{aligned} \tag{2.27}$$

Έτσι, από τις δύο τελευταίες σχέσεις $(2.26), (2.27)$ έχουμε

$$\alpha\cdot\mu\nu\beta=\mu\lambda\beta-\beta+\mu^2\beta-\mu\beta. \tag{2.28}$$

Καθώς όμως εξ'υποθέσεως τα id, μ, μ^2 είναι διακεκριμένα [4] άρα αναγκαστικά ο όρος $\mu\lambda\beta$ θα είναι εκείνος που θα πρέπει να διαγράφεται με κάποιον από τους υπόλοιπους τρεις της σχέσης (2.28). Συνεπώς $\mu\lambda\beta\in\{\beta,\mu\beta,-\mu^2\beta\}$.

- Εάν $\mu\lambda\beta=\mu\beta$ τότε $\mu\lambda=\mu$ δηλαδή $\lambda=id$, άτοπο.
- Εάν $\mu\lambda\beta=\beta$ τότε $\mu\lambda=id$, άτοπο λόγω της (2.17).

Συνεπώς $\mu\lambda\beta=-\mu^2\beta\Rightarrow\mu\lambda\beta+\mu^2\beta=0$. Όμως οι αυτομορφισμοί $\mu\lambda,\mu^2\in G$ αποτελούν στοιχεία της βάσης άρα δεν μπορεί να είναι διακεκριμένοι διότι τότε θα είχαμε γραμμική εξάρτησή τους (οι συντελεστές είναι μη μηδενικοί). Συνεπώς πρέπει

$$\mu\lambda=\mu^2$$

και κατ'επέκτασιν

$$\mathrm{char}K=2\ ^{[5]}.$$

[4] Εάν για παράδειγμα ήταν $\mu^2=\mu$ τότε θα είχαμε $\mu=id$, άτοπο εξ'υποθέσεως.

[5] Διότι για κάθε $k\in K$ ισχύει $2k=2\mu\lambda k=2\mu\lambda(\beta\cdot\beta^{-1}\cdot k)=2\mu\lambda\beta\cdot2\mu\lambda\beta^{-1}\cdot2\mu\lambda k\overset{2\mu\lambda\beta=0}{=}0$, άρα $\mathrm{char}K=2$.

Άρα $\mu\lambda = \mu^2 \Rightarrow \mu = \lambda$. Συνεπώς $\lambda\mu = \mu^2$ και $\mu\lambda = \mu^2$ άρα $\lambda\mu = \mu\lambda$. Τότε, τα πρώτα μέλη των σχέσεων $(2.14), (2.24)$ είναι ίσα και έτσι οδηγούμαστε στην

$$\mu^2\beta - \mu\beta = \beta - \mu\beta \Rightarrow \mu^2\beta = \beta \overset{\mathrm{char}K=2}{\Rightarrow} \mu^2\beta + \beta = 0 \Rightarrow \mu^2 = id \; \acute{\alpha}\tau o\pi o$$

Συνεπώς ο όρος $-\mu\beta$ είναι εκείνος που διαγράφεται με τον $-\lambda\kappa\beta$ στη σχέση (2.23), δηλαδή $\mu\beta + \lambda\kappa\beta = 0$ και με όμοιο επιχείρημα όπως παραπάνω, παίρνουμε ότι

$$\mu = \lambda\kappa$$

και έτσι $2\mu\beta = 0$. Αυτές οι σχέσεις αποδεικνύουν την (2.9) και μέσω της (2.23) αποδεικνύουν και την (2.10).

Έτσι, από τη σχέση (2.19) παίρνουμε ότι

$$\alpha \cdot \lambda^{-1}\mu^{-1}\beta = \lambda^{-1}\beta + \lambda^{-1}\mu\beta. \tag{2.29}$$

Όμως

$$\begin{aligned} \alpha \cdot \lambda^{-1}\mu^{-1}\beta &= \sum_{\sigma\in G} d(\lambda^{-1}\mu^{-1}, \sigma)\sigma\beta = d(\lambda^{-1}\mu^{-1}, \lambda^{-1}\mu)\lambda^{-1}\mu\beta \\ &+ \sum_{\substack{\sigma\in G \\ \sigma\neq\lambda^{-1}\mu}} d(\lambda^{-1}\mu^{-1}, \sigma)\sigma\beta, \end{aligned}$$

άρα πρέπει $d(\lambda^{-1}\mu^{-1}, \lambda^{-1}\mu) = 1$ και σύμφωνα με τη (1.7), έχουμε τελικά ότι

$$d(\mu^{-2}, \mu^{-1}\lambda) = d(\lambda^{-1}\mu^{-1}, \lambda^{-1}\mu) = 1$$

και επειδή $\mu^{-2} \neq id$, άρα υπάρχει $\upsilon \in G,\ \upsilon \neq \mu^{-1}\lambda$ τέτοιο ώστε

$$\alpha \cdot \mu^{-2}\beta = \mu^{-1}\lambda\beta + \upsilon\beta \tag{2.30}$$

Αυτό δίνει ότι

$$\begin{aligned} \lambda\alpha \cdot (\mu\alpha \cdot \mu^{-1}\beta) &= \lambda\alpha \cdot \mu(\alpha \cdot \mu^{-2}\beta) \overset{(2.30)}{=} \lambda\alpha \cdot \mu(\mu^{-1}\lambda\beta + \upsilon\beta) \\ &= \lambda\alpha \cdot (\lambda\beta + \mu\upsilon\beta) = \lambda(\alpha\beta) + \lambda\alpha \cdot \mu\upsilon\beta \\ &\overset{(2.7),\ \mathrm{char}K=2}{=} \lambda\mu\beta + \lambda\alpha \cdot \mu\upsilon\beta \end{aligned} \tag{2.31}$$

ενώ το ίδιο με διαφορετική μορφή, δίνει

$$\begin{aligned} \mu\alpha \cdot (\lambda\alpha \cdot \mu^{-1}\beta) &= \mu\alpha \cdot \lambda(\alpha \cdot \lambda^{-1}\mu^{-1}\beta) \\ &\overset{(2.29)}{=} \mu\alpha \cdot \lambda(\lambda^{-1}\beta + \lambda^{-1}\mu\beta) \\ &= \mu\alpha \cdot \beta + \mu\alpha \cdot \mu\beta \\ &= \mu(\alpha \cdot \mu^{-1}\beta + \alpha \cdot \beta) \\ &\overset{(2.7),(2.8),(2.9)}{=} \mu(\lambda\beta + \mu^{-1}\beta + \mu\beta) \\ &= \mu\lambda\beta + \beta + \mu^2\beta. \end{aligned} \tag{2.32}$$

Συνεπώς, από τις δύο τελευταίες σχέσεις $(2.31), (2.32)$ παίρνουμε

$$\lambda\alpha \cdot \mu\upsilon\beta = \lambda\mu\beta + \mu\lambda\beta + \beta + \mu^2\beta \tag{2.33}$$

Όμως το $\lambda\alpha \cdot \mu\upsilon\beta$ είναι συζυγές του $\alpha \cdot \lambda^{-1}\mu\upsilon\beta$ συνεπώς δύο όροι στο δεξί μέλος της (2.33) θα πρέπει να διαγράφονται. Όμως $id \notin \{\lambda\mu, \mu\lambda, \mu^2\}$, άρα το β δεν διαγράφεται με κάποιο από τους υπόλοιπους όρους. Συνεπώς δύο εκ των $\lambda\mu\beta, \mu\lambda\beta, \mu^2\beta$ πρέπει να διαγράφονται, άρα $\lambda\mu = \mu\lambda, \mu\lambda = \mu^2$ ή $\mu^2 = \lambda\mu$. Σε κάθε περίπτωση έχουμε

$$\lambda\mu = \mu\lambda$$

που ολοκληρώνει την απόδειξη της Πρότασης.

□

2.3 Κεντρικό Θεώρημα

Πρόκεται για το κύριο μέρος της εργασίας που αποτελεί ερευνητική δημοσίευση των H. Lenstra και S. Gao, [8] καθώς προσδιορίζει ακριβώς τις (πεπερασμένες) επεκτάσεις Galois στις οποίες αναζητούμε βέλτιστη κανονική βάση. Το αποτέλεσμα της έρευνας αυτής διατυπώνεται στο ακόλουθο Θεώρημα.

Θεώρημα 2.1 *Έστω L/K μία πεπερασμένη επέκταση $Galois$ με αντίστοιχη ομάδα $Galois$ την G και $\alpha \in L$. Τότε, αν υπάρχει πρώτος αριθμός p, πρωταρχική $p-$ρίζα της μονάδος ζ σε κάποια αλγεβρική επέκταση του L και στοιχείο $c \in K^*$ έτσι ώστε μία από τις παρακάτω να αληθεύει:*

(i) *Το ανάγωγο πολυώνυμο του ζ πάνω από το K έχει βαθμό $p-1$, ισχύει $L = K(\zeta)$ και $\alpha = c\zeta$,*

(ii) $\mathrm{char}K = 2$, *το ανάγωγο πολυώνυμο του $\zeta + \zeta^{-1}$ πάνω από το K έχει βαθμό $\dfrac{p-1}{2}$ και ισχύει $L = K(\zeta + \zeta^{-1})$ και $\alpha = c(\zeta + \zeta^{-1})$.*

τότε η $(\sigma\alpha)_{\sigma \in G}$ είναι βέλτιστη κανονική βάση για το L πάνω από το K ***και το αντίστροφο****.*

Απόδειξη:

Σχόλιο: Λόγω της σημείωσης στο Πόρισμα 2.2, αρκεί να αποδείξουμε το θεώρημα για την περίπτωση όπου $c = 1$ καθώς εάν έχουμε βέλτιστη κανονική βάση που παράγεται από το στοιχείο $\alpha = \zeta$ ή το $\alpha = \zeta + \zeta^{-1}$, τότε και το στοιχείο $c\alpha$ παράγει μία βέλτιστη κανονική βάση.

Ευθύ:

- Ας υποθέσουμε ότι ισχύει η (i). Τότε η κατασκευή της βέλτιστης κανονικής βάσης, είναι εντελώς όμοια με εκείνη στο Παράδειγμα

(2.2) με μοναδική διαφορά ότι η επέκταση εδώ είναι η $K(\zeta)/K$ αντί της $\mathbb{Q}(\zeta)/\mathbb{Q}$ που είχαμε στο παράδειγμα.

- Ας υποθέσουμε ότι ισχύει η (ii) του Θεωρήματος δηλαδή $\mathrm{char}K = 2$, $\deg \min\left(\zeta+\zeta^{-1}, K\right) = \frac{p-1}{2}$ και $L = K\left(\zeta+\zeta^{-1}\right)$. Από το σχόλιο παραπάνω, παίρνουμε $\alpha = \zeta+\zeta^{-1}$. Σκοπός μας, είναι η κατασκευή μιας κανονικής βάσης που θα δείξουμε ότι είναι βέλτιστη. Για το λόγο αυτό θα χρησιμοποιήσουμε την συνήθη βάση $\{\alpha^0, \alpha, \alpha^2, \ldots, \alpha^{\frac{p-1}{2}-1}\}$ του L ως K διανυσματικού χώρου .

  Επειδή το ζ είναι ρίζα του $x^{p-1}+\cdots+x+1$, άρα το $\min(\zeta, K)$ είναι βαθμού το πολύ $p-1$. Επειδή όμως $[L:K] = \frac{p-1}{2}$ άρα $[K(\zeta), L] = 1$ ή 2.

  Και στις δύο περιπτώσεις, σκοπός μας είναι να δείξουμε ότι όλα τα συζυγή του α είναι της μορφής $\zeta^i+\zeta^{-i}$ για κάποιο $1 \le i \le \frac{p-1}{2}$.

  - Εάν $[K(\zeta), L] = 1$ τότε $K(\zeta) = L$ δηλαδή $\zeta \in L$ άρα έχει νόημα να μιλήσουμε για το $\sigma(\zeta)$ όπου $\sigma \in G(L/K)$. Η συνέχεια όπως στο $(\star)$ παρακάτω με $\tilde{\sigma}$ να είναι το ίδιο το σ.
  - Εάν $[K(\zeta), L] = 2$ τότε $p(x) = \min(\zeta, L) = x^2 - \left(\zeta+\zeta^{-1}\right)x + 1$ και επεκτείνουμε τον $\sigma \in G(L/K)$ σε έναν αυτομορφισμό $\tilde{\sigma} : K(\zeta) \to K(\zeta)$. Αρκεί να ορίσουμε το $\tilde{\sigma}(\zeta)$. Εάν

    $$p^{\sigma}(x) = \sigma\left(p(x)\right) = x^2 - \sigma\left(\zeta+\zeta^{-1}\right)x + 1,$$

    τότε

    $$\begin{aligned} p^{\sigma}\left(\tilde{\sigma}(\zeta)\right) &= \left(\tilde{\sigma}(\zeta)\right)^2 - \sigma\left(\zeta+\zeta^{-1}\right)\tilde{\sigma}(\zeta) + 1 \\ &\overset{\zeta+\zeta^{-1}\in L}{=} \tilde{\sigma}(\zeta^2) - \tilde{\sigma}\left(\zeta+\zeta^{-1}\right)\tilde{\sigma}(\zeta) + \tilde{\sigma}(1) \\ &= \tilde{\sigma}\left(\zeta^2 - \left(\zeta+\zeta^{-1}\right)\zeta + 1\right) = \tilde{\sigma}(0) = 0 \end{aligned}$$

άρα το $\tilde{\sigma}(\zeta)$ είναι μία από τις δύο ρίζες του $p^{\sigma}(x)$. Επειδή $\tilde{\sigma} \in G\left(K(\zeta)/K\right)$ και $K(\zeta)/K$ κυκλοτομική επέκταση, άρα το στοιχείο $\tilde{\sigma}(\zeta)$ είναι μία πρωταρχική $p-$ ρίζα της μονάδος.

Άρα για τον αυτομορφισμό $\tilde{\sigma} : K(\zeta) \to K(\zeta)$, εάν m_i είναι μία ρίζα του $p^{\sigma}(x)$, τότε ορίζουμε $\tilde{\sigma}|_L = \sigma$, $\tilde{\sigma}(\zeta) = m_i$ και εάν $b \in K(\zeta)$ τότε $b = f(\zeta)$ με $f(x) \in L[x]$ (Η επέκταση $K(\zeta)$ είναι εξ' υποθέσεως αλγεβρική πάνω από το L) και ορίζουμε $\tilde{\sigma}(b) = f^{\sigma}(m_i)$. Η απεικόνιση αυτή είναι καλώς ορισμένη καθώς εάν $b = f(a) = g(a)$ τότε $f^{\sigma}(m_i) = g^{\sigma}(m_i)$. Πράγματι, $(f-g)(\zeta) = 0$ άρα $p(x)|f(x) - g(x)$ συνεπώς $p^{\sigma}(x)|f^{\sigma}(x) - g^{\sigma}(x)$ και αφού $p^{\sigma}(m_i) = 0$, άρα τελικά $f^{\sigma}(m_i) - g^{\sigma}(m_i) = 0$

$(\star)$ Άρα σε κάθε περίπτωση, εάν γ είναι συζυγής του α πάνω από το K, δηλαδή $\gamma = \sigma(\alpha)$, για κάποιο $\sigma \in G(L/K)$, τότε

$$\begin{aligned} \gamma &= \sigma(\zeta + \zeta^{-1}) = \tilde{\sigma}(\zeta + \zeta^{-1}) \\ &= \tilde{\sigma}(\zeta) + \tilde{\sigma}(\zeta^{-1}) = \tilde{\sigma}(\zeta) + \tilde{\sigma}(\zeta)^{-1}. \end{aligned}$$

Άρα κάποια ρίζα η του $x^2 - \gamma x + 1$ (οι ρίζες αυτού είναι οι $\tilde{\sigma}(\zeta)$ και $\tilde{\sigma}(\zeta^{-1})$ διότι έχουν άθροισμα γ και γινόμενο 1), είναι συζυγής του ζ ή του ζ^{-1} (προφανές, αφού $\eta = \tilde{\sigma}(\zeta)$ ή $\eta = \tilde{\sigma}(\zeta^{-1})$), άρα το η είναι κάποια $p-$ρίζα της μονάδος κι έτσι $\eta = \zeta^i$, για κάποιο i που δεν είναι διαιρετό από το p (εάν $p|i$, τότε $i = pk$ για κάποιο $k \in \mathbb{Z}$, άρα $\zeta^i = \zeta^{pk} = 1$, άτοπο αφού το 1 δεν είναι πρωταρχική $p-$ρίζα της μονάδος). Άρα $\gamma = \eta + \eta^{-1} = \zeta^i + \zeta^{-i} = a_i$, για κάποιο i, με $0 \leq i \leq \frac{p-1}{2}$ (εάν $\frac{p+1}{2} \leq i \leq p-1$, τότε $\zeta^i + \zeta^{-i} = \zeta^{i-p} + \zeta^{p-i}$, οπότε περιοριζόμαστε μόνο σε εκείνα τα i για τα οποία $0 \leq i \leq \frac{p-1}{2}$).

Αφού ο βαθμός του α είναι $\frac{p-1}{2}$, ο p είναι περιττός πρώτος και τα συζυγή του α, είναι ακριβώς τα στοιχεία $a_i = \zeta^i + \zeta^{-i}$, με

$1 \leq i \leq \frac{p-1}{2}$ [6] . Λόγω του Λήμματος 4.2, για $0 < j < \frac{p-1}{2}$ έχουμε ότι

$$\alpha^j = \sum_{i=0}^{\left[\frac{j-1}{2}\right]} \binom{j}{i} a_{j-2i} \quad \text{και} \quad \alpha^0 = \sum_{i=0}^{\frac{p-1}{2}} a_i$$

Καθώς λοιπόν κάθε στοιχείο της συνήθους βάσης του L, που γράψαμε στην αρχή γράφεται ως γραμμικός συνδυασμός στοιχείων του συνόλου $\{a_1, a_2, \ldots, a_{\frac{p-1}{2}}\}$, άρα το τελευταίο σύνολο (που περιέχει $\frac{p-1}{2}$ στοιχεία), είναι γραμμικώς ανεξάρτητο και αποτελεί βάση της επέκτασης L/K που μάλιστα είναι κανονική εξ' ορισμού των a_i [7]. Επίσης για την γραμμική απεικόνιση

$$\begin{aligned} m_\alpha : L &\to L \\ x &\mapsto \alpha \cdot x \end{aligned}$$

έχουμε

$$\begin{aligned} m_\alpha(a_1) &= \alpha \cdot a_1 = \alpha^2 = \left(\zeta + \zeta^{-1}\right)^2 \overset{\mathrm{char}K=2}{=} \zeta^2 + \zeta^{-2} = a_2. \\ m_\alpha(a_i) &= \alpha \cdot a_i = \left(\zeta + \zeta^{-1}\right)\left(\zeta^i + \zeta^{-i}\right) \\ &= \zeta^{i+1} + \zeta^{1-i} + \zeta^{i-1} + \zeta^{-1-i} \\ &= \left(\zeta^{i-1} + \zeta^{-(i-1)}\right) + \left(\zeta^{i+1} + \zeta^{-(i+1)}\right) \\ &= a_{i-1} + a_{i+1}, \quad \text{για } 1 < i < \frac{p-1}{2}. \\ m_\alpha\left(a_{\frac{p-1}{2}}\right) &= \alpha \cdot a_{\frac{p-1}{2}} = a_{\frac{p-3}{2}} + a_{\frac{p-1}{2}} \end{aligned}$$

[6] εάν είχαμε $\zeta^i + \zeta^{-i} = \zeta^j + \zeta^{-j}$ για $i \neq j$ και $0 \leq i, j \leq \frac{p-1}{2}$, τότε καταλήγουμε στη σχέση $(\zeta^{j-i} - 1)(\zeta^{j+i} - 1) = 0$ που δεν γίνεται διότι τότε θα είχαμε $\zeta^{j-i} = 1$ ή $\zeta^{j+i} = 1$ και οι εκθέτες είναι και οι δύο μικρότεροι του p ενώ ταυτόχρονα το ζ είναι $p-$ρίζα της μονάδος.

[7] Παρατηρήστε ότι κάθε συζυγές γ του α έχει τη μορφή - όπως δείξαμε στην αρχή - $\gamma = a_i$.

Φαίνεται λοιπόν, λόγω της μορφής της, ότι η βάση αυτή είναι βέλτιστη.

Αντίστροφο:

Ας υποθέσουμε ότι η $(\sigma\alpha)_{\sigma\in G}$ είναι βέλτιστη κανονική βάση και $(\sigma\beta)_{\sigma\in G},\ \beta\in L$ η δυϊκή της. Λόγω της σχέσης (2.4) διακρίνουμε τις εξής περιπτώσεις:

(i) $\mu = id$. Τότε από την σχέση (2.4) παίρνουμε $\alpha = -1$. Άρα η $(\sigma\alpha)_{\sigma\in G} = \{-1\}$, είναι η βάση της L/K άρα $[L:K]=1$, συνεπώς κάθε στοιχείο $\lambda\in L$, γράφεται ως $(-1)\cdot k = -k,\ k\in K$ άρα $L\subseteq K$ και αφού εξ'υποθέσεως $K\subseteq L$, άρα $L=K$.

- $\mathrm{char}K\neq 2$. Τότε για $p=2$, η $\zeta=-1$ είναι πρωταρχική $2-$ρίζα της μονάδος και τότε $L=K(-1)=K$ και το ανάγωγο πολυώνυμο του ζ πάνω από το K είναι το $x+1$ βαθμού $p-1=1$ άρα είμαστε στην περίπτωση (i) του θεωρήματος.
- $\mathrm{char}K=2$. Για $p=3$, οι $\zeta=\omega,\omega^2$ είναι πρωταρχικές 3-ρίζες της μονάδος και σε κάθε περίπτωση (είτε $\zeta=\omega$ είτε $\zeta=\omega^2$) έχουμε
$$\zeta+\zeta^{-1}=\omega+\omega^2=-1\overset{\mathrm{char}K=2}{=}1,$$
άρα $K\left(\zeta+\zeta^{-1}\right)=K(1)=K=L$. Το ανάγωγο πολυώνυμο του 1 πάνω από το K, είναι το $x-1$ με βαθμό $\frac{p-1}{2}=1$ δηλαδή είμαστε στην περίπτωση (ii) του θεωρήματος.

(ii) $\mu\neq id$ και $\mu^2=id$. Τότε λόγω της σχέσης 2.4, έχουμε $\alpha=(-\mu\beta)\cdot\beta^{-1}$ και εφαρμόζωντας στην τελευταία τον αυτομορφισμό μ έχουμε

$$\begin{aligned}\mu\alpha &= \mu\left((-\mu\beta)\cdot\beta^{-1}\right)=-\mu^2\beta\cdot\mu\beta^{-1}\overset{\mu^2=id}{=}-\beta\cdot(\mu\beta)^{-1}\\ &\overset{(2.4)}{=} -\beta\cdot(-\alpha\beta)^{-1}=\beta\cdot\beta^{-1}\cdot\alpha^{-1}=\alpha^{-1}\end{aligned}$$

Άρα

$$\alpha \cdot \mu\alpha = 1 = -\mathrm{Tr}\,(\alpha) = \sum_{\sigma \in G}(-\sigma\alpha) \tag{2.34}$$

και έτσι σύμφωνα με τη σχέση (2.1), παίρνουμε τελικά

$$d(\sigma, \mu) = -1, \;\; \forall \sigma \in G$$

που δείχνει ότι τα στοιχεία της στήλης του πίνακα της γραμμικής απεικόνισης m_α που αντιστοιχεί στον αυτομορφισμό μ, είναι όλα ίσα με -1.

Λόγω της σχέσης (1.8), έχουμε

$$\begin{aligned} \alpha \cdot \sigma\beta &= \sum_{\tau \in G} d(\sigma, \tau)\tau\beta = d(\sigma, \mu)\mu\beta + \sum_{\substack{\tau \in G \\ \tau \neq \mu}} d(\sigma, \tau)\tau\beta \\ &= -\mu\beta + \sum_{\substack{\tau \in G \\ \tau \neq \mu}} d(\sigma, \tau)\tau\beta \end{aligned} \tag{2.35}$$

Όμως, λόγω του Πορίσματος (2.1) ισχύει ότι για κάθε $\sigma \in G$ με $\sigma \neq id$ υπάρχουν ακριβώς δύο στοιχεία $\tau \in G$ με $d(\sigma, \tau)$ μη μηδενικά, των οποίων το άθροισμα κάνει μηδέν. Αφού λοιπόν ο ένας αυτομορφισμός είναι το $\mu \neq id$ (διότι $d(\sigma, \mu) = -1 \neq 0$), άρα για κάποιο άλλο μοναδικό $\sigma^* \in G$ με $\sigma^* \neq \mu$ ισχύει ότι

$$d(\sigma, \sigma^*) = 1 \tag{2.36}$$

και κατ'επέκτασιν $d(\sigma, \tau) = 0, \; \forall \; \tau \neq \mu, \sigma^*$. Συνεπώς λόγω της σχέσης (2.35), παίρνουμε τελικά ότι

$$\alpha \cdot \sigma\beta = \sigma^*\beta - \mu\beta, \;\; \forall \; \sigma \in G, \sigma \neq id$$

Επίσης $\alpha \cdot \sigma^* \alpha = \sum_{\tau \in G} d(\tau, \sigma^*) \tau\alpha = d(\sigma, \sigma^*)\sigma\alpha + \sum_{\substack{\tau \in G \\ \tau \neq \mu}} d(\tau, \sigma^*)\tau\alpha$

Όμως η γραμμική απεικόνιση m_x είναι ισομορφισμός άρα ο αντίστοιχος πίνακας είναι αντιστρέψιμος συνεπώς η ορίζουσα είναι διαφορετική του μηδενός άρα καμία στήλη δεν περιέχει όλα τα στοιχεία ίσα με μηδέν. Από την άλλη, εάν μία στήλη πλην εκείνης που αντιστοιχεί στον αυτομορφισμό μ (που έχει n σε πλήθος στοιχεία ίσα με -1), είχε δύο μη μηδενικά στοιχεία, τότε θα είχαμε ακόμη να συμπληρώσουμε $2n - 1 - (n + 2) = n - 3$ θέσεις με μη μηδενικά στοιχεία. Όμως έχουμε $n - 2$ στήλες στις οποίες πρέπει να συμπληρώσουμε στοιχεία μη μηδενικά άρα σίγουρα κάποια έχει μόνο μηδενικά, άτοπο. Άρα

$$d(\tau, \sigma^*) = 0, \quad \forall\, \tau \in G, \tau \neq \mu, \tau \neq \sigma \tag{2.37}$$

Συνεπώς από τις σχέσεις (2.36),(2.37), η απεικόνιση

$$\begin{aligned} \phi : G \setminus \{\mu\} &\rightarrow G \setminus \{\mu\} \\ \sigma &\mapsto \sigma^* \end{aligned}$$

είναι 1-1 άρα τελικά έχουμε

$$\alpha \cdot \sigma^* \alpha = \sigma\alpha, \ \sigma^* \neq \mu,$$

και από την σχέση (2.34) παίρνουμε

$$\alpha \cdot \mu\alpha = 1.$$

Συνεπώς το σύνολο $A = \{1\} \cup \{\sigma\alpha : \sigma \in G\}$ είναι κλειστό ως προς τον πολλαπλασιασμό με το α αφού

$$\begin{aligned} \alpha \cdot 1 &= \alpha = id\alpha \in A \\ \alpha\sigma^*\alpha &= \sigma\alpha \in A,\ \sigma^* \neq \mu \\ \alpha\mu\alpha &= 1 \in A \end{aligned}$$

Θα δείξουμε τώρα ότι το A είναι πολλαπλασιαστική ομάδα . Προφανώς το ουδέτερο ανήκει στο A. Αρκεί λοιπόν να δείξω την κλειστότητα.

$$\begin{aligned} 1 \cdot \tau\alpha &= \tau\alpha \in A \\ \sigma\alpha \cdot \tau\alpha &= \sigma(\alpha \cdot \sigma^{-1}\tau\alpha) \overset{\sigma^{-1}\tau=\rho}{=} \sigma(\alpha \cdot \rho\alpha) \\ &= \begin{cases} \sigma 1 = 1 \in A, \text{αν } \ \rho = \mu \\ \sigma(\tau\alpha) = \pi\alpha \in A, \text{αν } \ \rho \neq \mu \end{cases} \end{aligned}$$

συνεπώς η A είναι ομάδα τάξης $n+1$ εκτός εάν $\alpha = 1$ που αποκλείεται διότι εάν ήταν $\alpha = 1$ τότε $\sigma\alpha = 1,\ \forall\, \sigma \in G$ άρα $(\sigma\alpha)_{\sigma\in G} = \{1\}$ άρα $L = K$, οπότε $G = \{id\}$, δηλαδή $\mu = id$, άτοπο.

Άρα $\alpha^{n+1} = 1$ [8]. Επίσης $\alpha \neq 1$ άρα το α είναι ρίζα του πολυωνύμου

$$f(x) = x^n + \cdots + x + 1.$$

Αν $m(x)$ είναι το ελάχιστο πολυώνυμο του α, τότε αυτό έχει ρίζες όλα τα $\sigma\alpha$ δηλαδή τις $(n+1)-$ρίζες της μονάδος και λόγω του ότι και το $f(x)$ έχει τις ίδιες ρίζες, είναι και τα δύο μονικά και ίδιου βαθμού, συνάγουμε ότι $f(x) \equiv m(x)$ απ'όπου το $f(x)$ είναι ανάγωγο .

[8] διότι για $\sigma = id$, από το Θεώρημα του *Lagrange* έχουμε ότι $(id\alpha)^{n+1} = 1$ δηλαδή $\alpha^{n+1} = 1$.

Το σύνολο A περιέχει όλες τις $(n+1)-$ρίζες της μονάδος (διότι είναι ομάδα τάξης $n+1$ και άρα κάθε στοιχείο υψωμένο στη δύναμη $n+1$ ισούται με 1) άρα και τις πρωταρχικές . Θα δείξουμε ότι όλες οι $\sigma\alpha, \sigma \in G$ είναι πρωταρχικές οπότε θα συμπεράνουμε ότι ο $n+1$ θα είναι πρώτος. Εάν $\rho\alpha$ πρωταρχική $(n+1)-$ ρίζα της μονάδος τότε εάν k είναι ο ελάχιστος φυσικός αριθμός για τον οποίο $(\sigma\alpha)^k = 1$, τότε έχουμε διαδοχικά

$$\begin{aligned}(\sigma\alpha)^k = 1 \;&\Rightarrow\; \underbrace{\sigma\alpha \cdot \cdots\cdot \sigma\alpha}_{k} = 1 \Rightarrow \sigma(\underbrace{\alpha \cdot \cdots\cdot \alpha}_{k}) = 1 \\ &\Rightarrow\; \sigma\alpha^k = 1 \Rightarrow \rho\sigma^{-1}(\sigma\alpha^k) = \rho\sigma^{-1}(1) \Rightarrow \rho\alpha^k = 1 \\ &\Rightarrow\; (\rho\alpha)^k = 1 \Rightarrow k = n+1\end{aligned}$$

διότι το $\rho\alpha$ είναι μία πρωταρχική ρίζα της μονάδος συνεπώς η τάξη του είναι $n+1$.

Άρα ο $n+1$ είναι πρώτος οπότε είμαστε στην πρώτη περίπτωση του θεωρήματος (Το $f(x)$ πράγματι είναι ανάγωγο βαθμού $p-1 = n+1-1 = n$ και ισχύει $L = K(\alpha)$.)

(iii) $\underline{\mu \neq id \text{ και } \mu^2 \neq id.}$

Από το Λήμμα 2.1 έχουμε $d(id, \sigma) = -1$ ή 0, αναλόγως εάν $\sigma = \mu$ ή $\sigma \neq \mu$ και λόγω της σχέσης (1.7) έχουμε,

$$d(\sigma,\sigma) = \begin{cases} -1, & \text{αν } \sigma = \mu^{-1} \\ 0, & \text{αν } \sigma \neq \mu^{-1}. \end{cases} \tag{2.38}$$

Λόγω της σχέσης (1.8), έχουμε

$$\alpha \cdot \mu^{-1}\beta = \sum_{\sigma\in G} d(\mu^{-1},\sigma)\sigma\beta = d(\mu^{-1},\mu^{-1})\mu^{-1}\beta + \sum_{\substack{\sigma\in G \\ \sigma\neq\mu^{-1}}} d(\mu^{-1},\sigma)\sigma\beta$$

και από τη σχέση (2.38),

$$d(\mu^{-1}, \mu^{-1}) = -1.$$

Επειδή όμως $\mu^{-1} \neq id$, άρα πρέπει να υπάρχει $\lambda \in G$ τέτοιο, ώστε $d(\mu^{-1}, \lambda) = 1$ ενώ $d(\mu^{-1}, \sigma) = 0$, για κάθε $\sigma \in G$ με $\sigma \neq \lambda, \mu^{-1}$. Άρα τελικά

$$\alpha \cdot \mu^{-1}\beta = -\mu^{-1}\beta + \lambda\beta, \quad \lambda \neq \mu^{-1}. \tag{2.39}$$

Εφαρμόζουμε τον αυτομορφισμό μ στην σχέση (2.39) και παίρνω

$$\mu(\alpha \cdot \mu^{-1}\beta) = \mu\alpha \cdot \beta \ \text{ και } \ \mu(\lambda\beta - \mu^{-1}\beta) = \mu\lambda\beta - \beta,$$

άρα

$$\mu\alpha\beta = \mu\lambda\beta - \beta \overset{(2.9),(2.11)}{\Rightarrow} \mu\alpha \cdot \beta = \lambda\mu\beta + \beta.$$

Όμως σε συνδυασμό με την (2.10) παίρνουμε

$$\mu\alpha \cdot \beta = \alpha \cdot \mu\beta \Rightarrow \mu\alpha \cdot (\mu\beta)^{-1} = \alpha \cdot \beta^{-1},$$

δηλαδή

$$\mu(\alpha \cdot \beta^{-1}) = \alpha \cdot \beta^{-1}. \tag{2.40}$$

Εάν πολλαπλασιάσουμε κατά μέλη την τελευταία με την $-\mu\beta = \alpha \cdot \beta$, παίρνουμε διαδοχικά

$$\begin{aligned} -\mu(\alpha \cdot \beta^{-1}) \cdot \mu\beta = \alpha^2 \ &\Rightarrow \ -\mu(\alpha \cdot \beta^{-1} \cdot \beta) = \alpha^2 \\ &\Rightarrow \ \alpha^2 = -\mu\alpha \overset{(2.9)}{\Rightarrow} \mu\alpha = \alpha^2. \end{aligned}$$

Ισχυριζόμαστε ότι για κάθε $n \geq 0$ ισχύει

$$\mu^n \alpha = a^{2^n} \tag{2.41}$$

και θα το αποδείξουμε επαγωγικά.

Για $n = 0, 1$ ισχύει. Έστω ότι ισχύει για $n = k \geq 2$, δηλαδή ότι $\mu^k \alpha = \alpha^{2^k}$. Τότε

$$\mu^{k+1}\alpha = \mu(\mu^k \alpha) = \mu(\alpha^{2^k}) = \left(\alpha^{2^k}\right)^2 = \alpha^{2^{k+1}}$$

και η επαγωγή ολοκληρώθηκε.

Θέτοντας στη σχέση (2.41) $n = order\mu$ (άρα $\mu^n \alpha = \alpha$), παίρνουμε $\alpha^{2^n} = \alpha$, το οποίο σημαίνει ότι το α είναι αλγεβρικό πάνω από το $\mathbb{F}_2$ (αφού είναι ρίζα του πολυωνύμου $x^{2^n} - x \in \mathbb{F}_2[X]$). Άρα $\alpha \in \mathbb{F}_{2^n}$ συνεπώς ο βαθμός του, διαιρεί το n.

Άρα

$$n = order\mu \leq \sharp G = [L : K] = [K(\alpha) : K] \overset{(\star)}{\leq} n,$$

όπου η $(\star)$ ισχύει διότι $[K(\alpha) : K] = l$, όπου l ο βαθμός του αναγώγου πολυωνύμου του α πάνω από το K, ο οποίος είναι μικρότερος ή ίσος από το βαθμό του α πάνω από το $\mathbb{F}_2$ που διαιρεί το n άρα είναι μικρότερος από n.

Λόγω της παραπάνω σχέσης, ισχύει η ισότητα παντού κάτι που σημαίνει ότι το μ παράγει την ομάδα G.

Άρα

$$G = \{\alpha, \mu\alpha, \ldots, \mu^{n-1}\alpha\}$$

και το σύνολο αυτό είναι βάση της επέκτασης L/K.

Ισχυριζόμαστε τώρα ότι $\frac{\alpha}{\beta} \in K$. Λόγω της σχέσης $\mu\left(\frac{\alpha}{\beta}\right) = \frac{\alpha}{\beta}$ παίρνουμε επαγωγικά ότι

$$\mu^k \left(\frac{\alpha}{\beta}\right) = \frac{\alpha}{\beta}, \quad \text{για κάθε} \quad k = 1, \ldots, n-1. \tag{2.42}$$

Αφού $\frac{\alpha}{\beta} \in L$, υπάρχουν $k_1, \ldots, k_n \in K$ τέτοια, ώστε

$$\frac{\alpha}{\beta} = k_1\alpha + k_2\mu\alpha + \cdots + k_n\mu^{n-1}\alpha.$$

Εφαρμόζουμε διαδοχικά τις δυνάμεις των αυτομορφισμών μ και λόγω της σχέσης (2.42) παίρνουμε

$$\begin{aligned}
\frac{\alpha}{\beta} &= \mu\left(\frac{\alpha}{\beta}\right) = k_1\mu\alpha + k_2\mu^2\alpha + \cdots + k_n\alpha \\
\frac{\alpha}{\beta} &= \mu^2\left(\frac{\alpha}{\beta}\right) = k_1\mu^2\alpha + k_2\mu^3\alpha + \cdots + k_n\mu\alpha \\
&\vdots \\
\frac{\alpha}{\beta} &= \mu^{n-1}\left(\frac{\alpha}{\beta}\right) = k_1\mu^{n-1}\alpha + k_2\alpha + \cdots + k_n\mu^{n-2}\alpha
\end{aligned}$$

Λόγω της μοναδικότητος της γραφής του $\frac{\alpha}{\beta}$ ως προς τα στοιχεία της βάσης, θα πρέπει $k_2 = k_1 = k_n = \ldots = k_3$, άρα

$$\frac{\alpha}{\beta} = k_1\left(\alpha + \mu\alpha + \cdots + \mu^{n-1}\alpha\right) = k_1\sum_{\sigma\in G}\sigma\alpha = k_1\mathrm{Tr}\,(\alpha) \in K,$$

και η απόδειξη του ισχυρισμού ολοκληρώθηκε.

Για τη συνέχεια της απόδειξης, αφού $\mathrm{Tr}\,(\alpha) = -1$ άρα $\frac{\alpha}{\beta} = -k_1$ δηλαδή $\alpha = -k_1\beta$ και παίρνοντας ίχνος και στα δύο μέλη έχουμε

$$\mathrm{Tr}\,(\alpha) = -k_1\mathrm{Tr}\,(\beta) \overset{\mathrm{Tr}(\alpha)=\mathrm{Tr}(\beta)=-1}{\Longrightarrow} k_1 = -1.$$

Άρα $\frac{\alpha}{\beta} = 1$ και έτσι $\alpha = \beta$ που λόγω των σχέσεων (1.6), (1.8), έχουμε

$$d(\sigma,\tau) = d(\tau,\sigma), \quad \text{για κάθε} \quad \sigma,\tau \in G \tag{2.43}$$

Έστω ζ ρίζα του $X^2 - \alpha X + 1$ σε κάποια αλγεβρική επέκταση του L. Άρα $\zeta + \zeta^{-1} = \alpha$. Άρα λόγω του ότι το α είναι αλγεβρικό πάνω από το $\mathbb{F}_2$, το ίδιο θα συμβαίνει και με το ζ, δηλαδή η (πολλαπλασιαστική) τάξη του ζ είναι πεπερασμένη και περιττή έστω $2m+1$.

Για κάθε ακέραιο i, ας είναι $\gamma_i := \zeta^i + \zeta^{-i}$. Τότε $\gamma_0 = \zeta^0 + \zeta^0 = 1 + 1 = 0$ και λόγω των τύπων $Vieta$, $\gamma_1 = \alpha$. Επίσης έχουμε διαδοχικά

$$\begin{aligned}
\gamma_i = \gamma_j &\iff \zeta^i + \zeta^{-i} = \zeta^j + \zeta^{-j} \overset{\mathrm{char}K=2}{\iff} \zeta^{2i+j} + \zeta^j + 2^{i+j} + j^i = 0 \\
&\implies \zeta^{i+j}\left(\zeta^i + \zeta^j\right) + \left(\zeta^i + \zeta^j\right) = 0 \\
&\implies \left(\zeta^{i+j} + 1\right)\left(\zeta^i + \zeta^j\right) = 0 \\
&\implies \zeta^{i+j} + 1 = 0 \ \text{ή} \ \zeta^i + \zeta^j = 0 \\
&\implies i + j \equiv 0 \pmod{2m+1} \ \text{ή} \ i - j \equiv 0 \pmod{2m+1} \\
&\implies i \equiv \pm j \pmod{2m+1}
\end{aligned}$$

Συνεπώς υπάρχουν ακριβώς m διαφορετικά στοιχεία μεταξύ των γ_i, ας πούμε $\gamma_1, \ldots, \gamma_m$.

Κάθε ένα από τα n συζυγή του α είναι της μορφής

$$\mu^j\alpha = \alpha^{2^j} = \zeta^{2^j} + \zeta^{-2^j} = \gamma_{2^j}, \ \text{ για κάποιο ακέραιο } \ j,$$

συνεπώς υπάρχουν μεταξύ των γ_i. Άρα $n \leq m$. Θα δείξουμε ότι $n = m$ δείχνοντας, αντίστροφα, ότι κάθε μη μηδενικό γ_i είναι συζυγές του α.

Αυτό θα γίνει με ισχυρή έπαγωγή επί του i. Έχουμε $\gamma_1 = \alpha, \gamma_2 = \alpha^2 = \mu\alpha$, άρα για $i = 1, 2$ ισχύει. Έστω ότι το γ_j είναι συζυγές του α για κάθε $j < i$ με $3 \leq i \leq m$. Θα δείξουμε ότι και το γ_i είναι συζυγές του α. Όμως

$$\begin{aligned}\alpha \cdot \gamma_{i-2} &= \left(\zeta + \zeta^{-1}\right) \cdot \left(\zeta^{i-2} + \zeta^{2-i}\right) \\ &= \zeta^{i-1} + \zeta^{3-i} + \zeta^{i-3} + \zeta 1 - i = \gamma_{i-1} + \gamma_{i-3}, \quad (2.44)\end{aligned}$$

όπου λόγω της επαγωγικής υπόθεσης τα $\gamma_{i-2}, \gamma_{i-1}$ είναι συζυγή του α ενώ το γ_{i-3} είναι είτε συζυγές του α είτε ίσο με μηδέν.

Άρα $\gamma_{i-2} = \sigma\alpha$ και $\gamma_{i-1} = \tau\alpha$ για κάποια $\sigma, \tau \in G$, συνεπώς λόγω της παραπάνω σχέσης (2.44), όταν το $\alpha \cdot \sigma\alpha$ εκφράζεται στην κανονική βάση, το γ_{i-1} εμφανίζεται με συντελεστή 1 και λόγω της σχέσης (2.43), όταν το $\alpha \cdot \gamma_{i-1}$ εκφράζεται ως προς την ίδια βάση, τότε το $\sigma\alpha = \gamma_{i-2}$ εμφανίζεται με συντελεστή 1. Συνεπώς από το Πόρισμα 2.1, αφού $\beta = \alpha$ και $\gamma_{i-1} \neq \alpha$ [9], άρα το $\alpha \cdot \gamma_{i-1}$ είναι ίσο με το άθροισμα του γ_{i-2} και κάποιου άλλου συζυγούς του α. Όμως λόγω της σχέσης (2.44), έχουμε $\alpha \cdot \gamma_{i-1} = \gamma_{i-2} + \gamma_i$, άρα το άλλο συζυγές του α πρέπει να είναι το γ_i και αυτό ολοκληρώνει την επαγωγή.

Άρα $n = m$, συνεπώς τα $\gamma_1, \ldots, \gamma_m$ είναι τα στοιχεία της βάσης $(\sigma\alpha)_{\sigma \in G}$.

Από το γεγονός ότι κάθε μη μηδενικό γ_i ισούται με κάποιο συζυγές $\mu^j\alpha$ του α, άρα για κάθε i μη διαιρετό από το $2m+1$ ισχύει

$$\gamma_i = \mu^j\alpha = \gamma_{2^j} \Longrightarrow i \equiv \pm 2^j \pmod{2m+1}.$$

Πιο συγκεκριμένα, οποιοσδήποτε ακέραιος i μη διαιρετός από το $2m+1$ είναι πρώτος προς το $2m+1$, άρα ο $2m+1$ είναι πρώτος. Άρα για $p = 2m+1$ έχουμε $\frac{p-1}{2} = \frac{2m+1-1}{2} = m = n$ που είναι ο βαθμός του ανάγωγου πολυωνύμου του $\alpha = \zeta + \zeta^{-1}$ πάνω από το K και έτσι έχουμε ολοκληρώσει την απόδειξη και αυτής της περίπτωσης.

[9] Εάν $\gamma_{i-1} = \alpha = \gamma_1 \Rightarrow i - 1 \equiv \pm 1 \pmod{2m+1}$, άτοπο αφού $1 \leq i \leq m$.

3 Βέλτιστες κανονικές βάσεις Πεπερασμένων Σωμάτων

3.1 Τύπου I

Λήμμα 3.1 *Εάν το q είναι πρώτος ή δύναμη πρώτου και πρωταρχικό στοιχείο του $\mathbb{Z}_{n+1}$, τότε εάν α είναι μία $(n+1)-$ρίζα της μονάδος, υπάρχουν n διακεκριμένα συζυγή του α κάθε ένα από τα οποία είναι επίσης πρωταρχική $(n+1)-$ρίζα της μονάδος.*

Απόδειξη:

Έστω $\alpha^{q^i} = \alpha^{q^j}$ για κάποια i, j με $i \neq j$ και $0 \leq i < j \leq n-1$. Τότε $\alpha^{q^i - q^j} = 1$. Όμως το α είναι πρωταρχική $(n+1)-$ρίζα της μονάδος άρα πρέπει $n+1 | q^i - q^j$ δηλαδή $q^i \equiv q^j \pmod{n+1}$, απ'όπου $q^{i-j} \equiv 1 \pmod{n+1}$. Όμως λόγω της $1 \leq i-j \leq n-1$ καταλήγουμε σε άτοπο διότι το q είναι πρωταρχικό στοιχείο του $\mathbb{Z}_{n+1}$ άρα το n είναι το ελάχιστο k με την ιδιότητα $q^k \equiv 1 \pmod{n+1}$. Άρα τα α^{q^i} είναι διακεκριμένα για $0 \leq i \leq n-1$ και αφού

$$\left(\alpha^{q^i}\right)^{n+1} = \alpha^{(n+1)q^i} = \left(\alpha^{n+1}\right)^{q^i} = 1,$$

τα α^{q^i} είναι $(n+1)-$ρίζες της μονάδος και η απόδειξη ολοκληρώθηκε.

□

Θεώρημα 3.1 *Οι παρακάτω προτάσεις (i) και (ii) είναι ισοδύναμες*

(i) *Υπάρχει πρώτος p, πρωταρχική $p-$ ρίζα της μονάδος ζ τέτοια ώστε $\deg \min(\zeta, \mathbb{F}_q) = p-1$ και $\mathbb{F}_{q^n} = \mathbb{F}_q(\zeta)$.*

(ii) *Υπάρχει πρώτος p τέτοιος ώστε $n+1 = p$ και q να γεννάει την πολλαπλασιαστική ομάδα $\mathbb{Z}_{n+1}^{\star}$.*

Απόδειξη :

Ας υποθέσουμε ότι ισχύει η (i)*. Τότε ισοδύναμα*

$$\min(\zeta, \mathbb{F}_q) = x^{p-1} + \cdots + x + 1$$

το οποίο σε συνδυασμό με το ότι $\mathbb{F}_{q^n} = \mathbb{F}_q(\zeta)$ *σημαίνει ισοδύναμα ότι* $n = p-1$ *δηλαδή* $n+1 = p$*, πρώτος και μάλιστα λόγω της Πρότασης 1.2 έχουμε* $\mathrm{ord}_p(q) = p-1$*, δηλαδή το* q *παράγει την πολλαπλασιαστική ομάδα* $\mathbb{Z}^\star_{n+1}$*. Άρα ισοδύναμα έχουμε το* (ii)*.*

□

Είναι φανερή η σχέση του Θεωρήματος αυτού με το Κεντρικό Θεώρημα 2.1 του προηγουμένου κεφαλαίου, με την οποία κατασκευάζουμε βέλτιστες κανονικές βάσεις. Έτσι έχουμε το επόμενο

Πόρισμα 3.1 *Εάν ο* $n+1$ *είναι πρώτος και το* q *είναι πρωταρχικό στοιχείο του* $\mathbb{Z}_{n+1}$ *και πρώτος ή δύναμη πρώτου, τότε οι πρωταρχικές* $(n+1)-$*ρίζες της μονάδος είναι γραμμικώς ανεξάρτητες και αποτελούν μία βέλτιστη κανονική βάση του* $\mathbb{F}_{q^n}$ *πάνω από το* $\mathbb{F}_q$*.*

□

Ορισμός 3.1 *Κάθε τέτοια βέλτιστη κανονική βάση που προκύπτει από την παραπάνω κατασκευή την ονομάζουμε* ***Τύπου I*** *.*

□

3.2 Τύπου II

Θεώρημα 3.2 *Ας υποθέσουμε ότι ο αριθμός* $p = 2n+1$ *είναι πρώτος. Τότε οι παρακάτω προτάσεις* (i) *και* (ii) *είναι ισοδύναμες*

(i) *Υπάρχει μία $p-$ρίζα της μονάδος, έστω ζ για την οποία ισχύει* $\deg\min\left(\zeta+\zeta^{-1},\mathbb{F}_2\right)=\frac{p-1}{2}$ *και* $\mathbb{F}_{2^n}=\mathbb{F}_2\left(\zeta+\zeta^{-1}\right)$.

(ii) *Ισχύει είτε*

- (a) *το 2 είναι πρωταρχικό στοιχείο του* $\mathbb{Z}_{2n+1}$ *είτε*
- (b) $2n+1\equiv 3 \pmod 4$ *και το 2 παράγει τα τετραγωνικά υπόλοιπα του* $\mathbb{Z}_{2n+1}$

Απόδειξη:

Ας υποθέσουμε ότι ισχύει η (i). Επειδή

$$\mathbb{F}_2\leq\underbrace{\mathbb{F}_2\left(\zeta+\zeta^{-1}\right)}_{\mathbb{F}_{2^n}}\leq\mathbb{F}_2\left(\zeta\right)$$

και το $\zeta+\zeta^{-1}$ είναι ρίζα του πολυωνύμου $x^2-\left(\zeta+\zeta^{-1}\right)x+1$, άρα η επέκταση $\mathbb{F}_2\left(\zeta+\zeta^{-1}\right)\leq\mathbb{F}_2\left(\zeta\right)$ είναι βαθμού 1 ή 2.

- Εάν είναι βαθμού 2 τότε $\left[\mathbb{F}_2\left(\zeta\right):\mathbb{F}_2\right]=p-1$ και το ζ είναι ρίζα του κυκλοτομικού πολυωνύμου Φ_p [10] με $\deg\Phi_p=p-1$. Άρα το ελάχιστο πολυώνυμο του ζ πάνω από το $\mathbb{F}_2$ είναι το Φ_p οπότε $\mathrm{ord}_p\left(2\right)=p-1$ οπότε είμαστε στην περίπτωση (α) του (ii).
- Εάν είναι βαθμού 1, τότε $\mathbb{F}_2\left(\zeta\right)=\mathbb{F}_{2^n}$ άρα $\deg\min\left(\zeta,\mathbb{F}_2\right)=n$. Το ζ είναι ρίζα του Φ_p που έχει βαθμό $p-1=2n$ άρα πρέπει να αναλύεται σε δύο πολυώνυμα βαθμού n. Συνεπώς $\mathrm{ord}_p\left(2\right)=n=\frac{p-1}{2}$ κι έτσι το 2 παράγει τα τετραγωνικά υπόλοιπα του $\mathbb{Z}_{2n+1}$. Επιπλέον, εάν υποθέσουμε ότι $2n+1\equiv 1 \pmod 4$ και θέσουμε $\alpha=\zeta+\zeta^{-1}$, τότε

$$\alpha^{2^{\frac{p-1}{4}}}=\left(\zeta+\zeta^{-1}\right)^{2^{\frac{p-1}{4}}}=\zeta^{2^{\frac{p-1}{4}}}+\zeta^{-2^{\frac{p-1}{4}}}=\zeta^{-1}+\zeta=\alpha$$

[10] Ξέρουμε ότι $x^p-1=\Phi_1\Phi_p$

διότι $2^{\frac{p-1}{4}} \equiv -1 \pmod{p}$ αφού $\mathrm{ord}_p(2) = \frac{p-1}{2}$. Άρα $\alpha \in \mathbb{F}_{2^{\frac{n}{2}}}$, άτοπο διότι $\alpha \in \mathbb{F}_{2^n}$ και δεν ανήκει σε κανένα μικρότερο υπόσωμά του. Άρα $2n+1 \equiv 3 \pmod{4}$.

Αντίστροφα, ας υποθέσουμε ότι ισχύει η (ii). Διακρίνουμε τις εξής περιπτώσεις:

- Εάν το 2 είναι πρωταρχικό στοιχείο του $\mathbb{Z}_{2n+1}$ τότε $\mathrm{ord}_p(2) = p-1$ άρα το Φ_p είναι ανάγωγο οπότε $\mathbb{F}_2(\zeta) = \mathbb{F}_{2^{p-1}} = \mathbb{F}_{2^{2n}}$. Επίσης η επέκταση $\mathbb{F}_2\left(\zeta+\zeta^{-1}\right) \leq \mathbb{F}_2(\zeta)$ είναι βαθμού 1 ή 2. Εάν θέσουμε $\alpha = \zeta + \zeta^{-1}$, τότε

$$\alpha^{2^{\frac{p-1}{2}}} = \zeta^{2^{\frac{p-1}{2}}} + \zeta^{-2^{\frac{p-1}{2}}} = \zeta^{-1} + \zeta = \alpha,$$

διότι $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Άρα $\zeta + \zeta^{-1} \in \mathbb{F}_{2^{\frac{p-1}{2}}} = \mathbb{F}_{2^n}$, δηλαδή $\left[\mathbb{F}_2(\zeta) : \mathbb{F}_2\left(\zeta+\zeta^{-1}\right)\right] = 2$. Συνεπώς αναγκαστικά παίρνουμε $\left[\mathbb{F}_{2^n} : \mathbb{F}_2\left(\zeta+\zeta^{-1}\right)\right] = 1$ άρα $\left[\mathbb{F}_2\left(\zeta+\zeta^{-1}\right) : \mathbb{F}_2\right] = \frac{p-1}{2}$ κι έτσι ισχύει το (i) του Θεωρήματος.

- Εάν $2n+1 \equiv 3 \pmod{4}$ και το 2 παράγει τα τετραγωνικά υπόλοιπα του $\mathbb{Z}_{2n+1}$, δηλαδή $\mathrm{ord}_p(2) = \frac{p-1}{2}$, τότε το κυκλοτομικό πολυώνυμο Φ_p αναλύεται σε γινόμενο 2 αναγώγων πολυωνύμων βαθμού n. Άρα $\deg \min(\zeta, \mathbb{F}_2) = n = \frac{p-1}{2}$. Επίσης εάν θέσουμε $\alpha = \zeta + \zeta^{-1}$, τότε

$$\alpha^{2^{\frac{p-1}{2}}} = \zeta^{2^{\frac{p-1}{2}}} + \zeta^{-2^{\frac{p-1}{2}}} = \zeta + \zeta^{-1} = \alpha$$

άρα $\zeta + \zeta^{-1} \in \mathbb{F}_{2^{\frac{p-1}{2}}} = \mathbb{F}_{2^n}$.

Όμως ξέρουμε ότι $\left[\mathbb{F}_2(\zeta) : \mathbb{F}_2\left(\zeta+\zeta^{-1}\right)\right] = 1$ ή 2, άρα αν υποθέσουμε ότι $\left[\mathbb{F}_2(\zeta) : \mathbb{F}_2\left(\zeta+\zeta^{-1}\right)\right] = 2$ τότε θα είχαμε $\mathbb{F}_2\left(\zeta+\zeta^{-1}\right) = \mathbb{F}_{2^k}$ με $k|n$ και το n θα ήταν άρτιος, άτοπο διότι από την υπόθεση

$2n+1 \equiv 3 \pmod 4$. Συνεπώς $\left[\mathbb{F}_2(\zeta) : \mathbb{F}_2\left(\zeta+\zeta^{-1}\right)\right] = 1$, άρα $\mathbb{F}_{2^n} = \mathbb{F}_2\left(\zeta+\zeta^{-1}\right)$, δηλαδή και πάλι ισχύει το (i) του Θεωρήματος.

□

Ορισμός 3.2 *Κάθε τέτοια βέλτιστη κανονική βάση που προκύπτει από την παραπάνω κατασκευή την ονομάζουμε* ***Τύπου II*** .

□

Όπως και στην προηγούμενη παράγραφο, έτσι κι εδώ υπάρχει μία φυσιολογική κατασκευή βέλτιστων κανονικών βάσεων με τη βοήθεια του Κεντρικού Θεωρήματος και του παραπάνω Θεωρήματος. Την κατασκευή αυτή διατυπώνουμε στο επόμενο

Πόρισμα 3.2 *Εάν ο $2n+1$ είναι πρώτος και υποθέσουμε ότι είτε*

(a) *το 2 είναι πρωταρχικό στοιχείο του $\mathbb{Z}_{2n+1}$ είτε*

(ii) $2n+1 \equiv 3 \pmod 4$ *και το 2 παράγει τα τετραγωνικά υπόλοιπα του $\mathbb{Z}_{2n+1}$*

τότε το $\alpha = \zeta + \zeta^{-1}$ παράγει μία βέλτιστη κανονική βάση του $\mathbb{F}_{2^n}$ πάνω από το $\mathbb{F}_2$, όπου το ζ είναι μία πρωταρχική $(2n+1)-$ρίζα της μονάδος.

Ορισμός 3.3 *Κάθε τέτοια βέλτιστη κανονική βάση που προκύπτει από την παραπάνω κατασκευή την ονομάζουμε* ***Τύπου II*** .

□

Παρατήρηση: Για πρακτικές εφαρμογές χρειαζόμαστε βέλτιστες κανονικές βάσεις πάνω από το $\mathbb{F}_2$. Θα ήταν πολύ χρήσιμο εάν είχαμε κάποιους κανόνες με τους οποίους να ελέγχουμε εάν οι υποθέσεις των παραπάνω Πορισμάτων 3.1 και 3.2. Έτσι το επόμενο αποτέλεσμα που υπάρχει στο [11], είναι πολύ χρήσιμο.

Πρόταση 3.1 (i) *Το 2 είναι πρωταρχικό στοιχείο του* $\mathbb{Z}_r$ *για κάποιο πρώτο* r*, εάν* $r = 4s + 1$ *και το* s *είναι περιττός πρώτος.*

(ii) *Το 2 είναι πρωταρχικό στοιχείο του* $\mathbb{Z}_r$ *για κάποιο πρώτο* r*, εάν* $r = 2s + 1$ *και το* s *είναι πρώτος ισότιμος με* $1 \pmod 4$.

(iii) *Το 2 παράγει τα τετραγωνικά υπόλοιπα του* $\mathbb{Z}_r$ *για κάποιο πρώτο* r*, εάν* $r = 2s + 1$ *και το* s *είναι πρώτος ισότιμος με* $3 \pmod 4$.

□

Θα εξετάσουμε τώρα το ελάχιστο πολυώνυμο βέλτιστων κανονικών βάσεων Τύπου I και II.

Για την Τύπου I βέλτιστη κανονική βάση, το ελάχιστο πολυώνυμο είναι προφανώς το $x^n + \cdots + x + 1$, το οποίο είναι και ανάγωγο πάνω από το $\mathbb{F}_q$ αν και μόνο αν ο $n+1$ είναι πρώτος και το q είναι πρωταρχικό στοιχείο του $\mathbb{Z}_{n+1}$.

Για την εύρεση του ελαχίστου πολυωνύμου μίας βέλτιστης κανονικής βάσης Τύπου II θα περιγράψουμε τη διαδικασία παρακάτω. Ας είναι n ένας θετικός ακέραιος και ζ μία πρωταρχική $(2n+1)-$ρίζα της μονάδος σε κάποιο σώμα. Θεωρούμε το πολυώνυμο

$$f_n(x) = \prod_{j=1}^{n} \left(x - \zeta^j - \zeta^{-j}\right) \quad [11]. \tag{3.1}$$

[11] Ας σημειωθεί, ότι το $f_n(x)$ είναι το ελάχιστο πολυώνυμο του $\alpha = \zeta + \zeta^{-1}$ κάτω από τις προϋποθέσεις του Πορίσματος 3.2

Από τον τύπο του $Waring$ για κάθε θετικό ακέραιο k, έχουμε

$$\left(\zeta^j\right)^k + \left(\zeta^j\right)^{-k} = \sum_{i=0}^{[k/2]} \frac{k}{k-i}\binom{k-i}{i}(-1)^i \left(\zeta^j + \zeta^{-j}\right)^{k-2i}.$$

Ορίζουμε

$$D_k(x) = \sum_{i=0}^{[k/2]} \frac{k}{k-i}\binom{k-i}{i}(-1)^i x^{k-2i},$$

το οποίο είναι μία ειδική περίπτωση πολυωνύμου του Dickson . Τότε από την (3.1), βλέπουμε ότι το $\zeta^j + \zeta^{-j}$ είναι ρίζα του $D_{n+1}(x) - D_n(x)$, για $j = 0, 1, \ldots, n$. Καθώς το $D_{n+1}(x) - D_n(x)$ έχει βαθμό $n+1$ και τα $\zeta^j + \left(\zeta^j\right)^{-1}$ είναι διαφορετικά για $j = 0, 1, \ldots, n$, έχουμε ότι

$$D_{n+1}(x) - D_n(x) = f_n(x)(x-2).$$

Άρα

$$f_n(x) = \sum_{j=0}^{[(n-1)/2]} (-1)^j \binom{n-1-j}{j} x^{n-(2j+1)} + \sum_{j=0}^{[n/2]} (-1)^j \binom{n-j}{j} x^{n-2j}.$$

Ας σημειωθεί ότι το $f_n(x)$ είναι ανάγωγο πάνω από το $\mathbb{F}_q$ αν και μόνο αν η πολλαπλασιαστική ομάδα $\mathbb{Z}^\star_{2n+1}$ παράγεται από το q και το -1, και είναι ανάγωγο πάνω από το σώμα των ρητών αριθμών όταν το $2n+1$ είναι πρώτος.

3.3 Επίλογος

Στις προηγούμενες 2 παραγράφους είδαμε δύο κατασκευές βέλτιστων κανονικών βάσεων οι οποίες μάλιστα χαρακτηρίζουν τις βέλτιστες

κανονικές βάσεις (δηλαδή αν έχουμε κάποια βέλτιστη κανονική βάση, τότε αυτή θα είναι Τύπου I ή Τύπου II) αφού είναι άμεσο πόρισμα του Κεντρικού Θεωρήματος 2.1 και των αντίστοιχων Θεωρημάτων 3.1 και 3.2. Για την ιστορία να αναφέρουμε ότι στο άρθρο [15], με τη βοήθεια υπολογιστή δεν βρέθηκαν βέλτιστες κανονικές βάσεις στο $\mathbb{F}_{2^n}$ για $2 \leq n \leq 30$. Το γεγονός αυτό οδήγησε τους συγγραφείς του να ισχυριστούν ότι εάν το n δεν ικανοποιεί τις προϋποθέσεις των Πορισμάτων 3.1 και 3.2, τότε το $\mathbb{F}_{2^n}$ δεν περιέχει βέλτιστη κανονική βάση.Ο Lenstra στο άρθρο [10] απέδειξε ότι πράγματι αυτό ισχύει. Εάν το κατώτερο σώμα $\mathbb{F}_q$ δεν είναι το $\mathbb{F}_2$ τότε έχουμε άλλες βέλτιστες κανονικές βάσεις. Ας υποθέσουμε ότι τα στοιχεία του συνόλου N αποτελούν βέλτιστη κανονική βάση του $\mathbb{F}_{q^n}$ πάνω από το $\mathbb{F}_q$ και ας είναι $\alpha \in \mathbb{F}_q$. Τότε το σύνολο

$$\alpha N = \{\alpha a : a \in N\}$$

αποτελεί επίσης μία βέλτιστη κανονική βάση του $\mathbb{F}_{q^n}$ πάνω από το $\mathbb{F}_q$. Τότε λέμε ότι οι βάσεις N και αN είναι **ισοδύναμες** .

Ένας άλλος τρόπος εύρεσης βέλτιστων κανονικών βάσεων δίνεται από το Λήμμα (3.2) παρακάτω και το οποίο βρίσκεται στο άρθρο [8] των Gao και Lenstra.Για κάθε θετικό ακέραιο s με $(n, s) = 1$, τα στοιχεία του συνόλου N μένει να αποτελούν μία βάση του $\mathbb{F}_{q^{ns}}$ πάνω από το $\mathbb{F}_{q^s}$ και τότε θα αποτελούν μία βέλτιστη κανονική βάση του $\mathbb{F}_{q^{ns}}$ πάνω από το $\mathbb{F}_{q^s}$.

Λήμμα 3.2 *Έστω s, n πρώτοι μεταξύ τους πρώτοι αριθμοί. Εάν τα στοιχεία του συνόλου $\tilde{B} = \{\alpha_0, \cdots, \alpha_{n-1}\}$ αποτελούν βάση του $\mathbb{F}_{q^n}$ πάνω από το $\mathbb{F}_q$, τότε το $\tilde{B}$ είναι επίσης βάση του $\mathbb{F}_{q^{sn}}$ πάνω από το $\mathbb{F}_{q^s}$.*

□

Το πρόβλημα τώρα, ήταν εάν υπήρχαν ή όχι άλλες βέλτιστες κανονικές βάσεις. Ο Mullin στο άρθρο [16] απέδειξε ότι εάν η κατανομή των

μη μηδενικών στοιχείων του πίνακα πολλαπλασιασμού μίας βέλτιστης κανονικής βάσης είναι όμοια με μία Τύπου I ή Τύπου II βέλτιστη κανονική βάση τότε η βάση αυτή θα πρέπει να είναι Τύπου I ή Τύπου II. Αργότερα, ο Gao στο άρθρο [7] απέδειξε ότι κάθε βέλτιστη κανονική βάση πεπερασμένου σώματος πρέπει να είναι ισοδύναμη με μία Τύπου I ή Τύπου II βέλτιστη κανονική βάση. Τελικά, οι Gao και Lenstra στο άρθρο τους [8] επέκτειναν το αποτέλεσμα σε κάθε πεπερασμένη επέκταση Galois τυχαίου σώματος απόδειξη που ολοκληρώσαμε στο προηγούμενο κεφάλαιο.

Τελειώνουμε την εργασία αυτή με τον πίνακα 3, που δείχνει την ύπαρξη βέλτιστων κανονικών βάσεων του $\mathbb{F}_{2^n}$ πάνω από το $\mathbb{F}_2$ για $n \leq 1000$. Το * υποδηλώνει την ύπαρξη βέλτιστης κανονικής βάσης τύπου I, το ✠ υποδηλώνει την ύπαρξη βέλτιστης κανονικής βάσης τύπου I και τύπου II, διαφορετικά υπάρχει βέλτιστη κανονική βάση τύπου II.

2✠	53	135	231	338	431	546*	653	772*	876*
3	58*	138*	233	346*	438	554	658*	774	879
4*	60*	146	239	348*	441	556*	659	779	882*
5	65	148*	243	350	442*	558	660*	783	891
6	66*	155	245	354	443	561	676*	785	893
9	69	158	251	359	453	562*	683	786*	906*
10*	74	162*	254	371	460*	575	686	791	911
11	81	172*	261	372*	466*	585	690	796*	923
12*	82*	173	268*	375	470	586*	700*	803	930
14	83	174	270	378✠	473	593	708*	809	933
18✠	86	178*	273	378*	483	606	713	810	935
23	89	179	278	386	490*	611	719	818	938
26	90	180*	281	388*	491	612*	723	820*	939
28*	95	183	292*	393	495	614	725	826*	940*
29	98	186	293	398	508*	615	726	828*	946*
30	99	189	299	410	509	618✠	741	831	950
33	100*	191	303	411	515	629	743	833	953
35	105	194	306	413	519	638	746	834	965
36*	106*	196*	309	414	522*	639	749	846	974
39	113	209	316*	418*	530	641	755	852*	975
41	119	210	323	419	531	645	756*	858*	986
50	130*	221	326	420*	540*	650	761	866	989
51	131	226*	329	426	543	651	765	870	993
52*	134	230	330	429	545	652*	771	873	998

Πίνακας 3: Τιμές του $n \leq 1000$ για τις οποίες υπάρχει βέλτιστη κανονική βάση του $\mathbb{F}_{2^n}$ πάνω από το $\mathbb{F}_2$.

4 Παράρτημα

Λήμμα 4.1 *Έστω p πρώτος. Τότε το πολυώνυμο $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ είναι ανάγωγο πάνω από το $\mathbb{Q}$.*

Απόδειξη:

Επειδή για $x \neq 1$ ισχύει $f(x) = \dfrac{x^p - 1}{x - 1}$, οι ρίζες του $f(x)$ είναι ρίζες του $x^p - 1 = 0,\ x \neq 1$ δηλαδή οι $p-$ρίζες της μονάδος οι οποίες είναι οι $\zeta^i, 1 \leq i \leq p-1$ όπου ζ μια $p-$ρίζα της μονάδος. Επειδή p πρώτος, όλες οι ρίζες είναι πρωταρχικές και ανήκουν στην ίδια επέκταση του $\mathbb{Q}$, την $\mathbb{Q}(\zeta)$. Εάν λοιπόν $p(x) = \mathrm{Irr}\,(\zeta, \mathbb{Q})$ και $\deg p(x) = d$, τότε $p(x) | f(x)$ απ'όπου $d \leq p - 1$. Η επέκταση $\mathbb{Q}(\zeta)/\mathbb{Q}$ είναι επέκταση $Galois$ διότι είναι κανονική (αφού όλες οι ρίζες του $p(x)$ είναι ρίζες και του $f(x)$ του οποίου όλες οι ρίζες ανήκουν στο $\mathbb{Q}(\zeta)$) και είναι διαχωρίσιμη (αφού το $p(x)$ έχει μόνο απλές ρίζες λόγω του ότι διαιρεί το $f(x)$ που έχει απλές ρίζες). Άρα $d = p - 1$ οπότε αφού τα $p(x), f(x)$ είναι και τα δύο μονικά, ταυτίζονται. Συνεπώς το $f(x)$ είναι ανάγωγο αφού είναι το $p(x)$ το οποίο εξ'υποθέσεως είναι ανάγωγο.

□

Λήμμα 4.2 *Έστω L/K μία πεπερασμένη επέκταση. Εάν ζ είναι μία p-ρίζα της μονάδος και για $1 \leq i \leq \frac{p-1}{2}$ ορίσουμε $a_i = \zeta^i + \zeta^{-i}$ καθώς επίσης $\alpha := a_1$, τότε*

(i) *για* $1 < j < \frac{p-1}{2}$ *ισχύει* $\alpha^j = \displaystyle\sum_{i=0}^{\left[\frac{j-1}{2}\right]} \binom{j}{i} a_{j-2i}$

(ii) *εάν* $\mathrm{char} K = 2$, *τότε* $\alpha^0 = \displaystyle\sum_{i=0}^{\frac{p-1}{2}} a_i$

Απόδειξη:

(i)

$$\begin{aligned}
\alpha^j &= \left(\zeta+\zeta^{-1}\right)^j = \sum_{i=0}^{j}\binom{j}{i}\zeta^i\zeta^{j-i} = \sum_{i=0}^{j}\binom{j}{i}\zeta^{2i-j} \\
&= \sum_{i=0}^{\left[\frac{j-1}{2}\right]}\binom{j}{i}\zeta^{2i-j} + \sum_{i=\left[\frac{j-1}{2}\right]+1}^{j}\binom{j}{i}\zeta^{2i-j} \\
&\overset{\text{Θέτω } i\to j-i}{=} \sum_{i=0}^{\left[\frac{j-1}{2}\right]}\binom{j}{i}\zeta^{2i-j} + \sum_{i=0}^{\left[\frac{j-1}{2}\right]}\binom{j}{j-i}\zeta^{2(j-i)-j} \\
&\overset{\binom{j}{j-i}=\binom{j}{i}}{=} \sum_{i=0}^{\left[\frac{j-1}{2}\right]}\binom{j}{i}\left(\zeta^{2i-j}+\zeta^{j-2i}\right) = \sum_{i=0}^{\left[\frac{j-1}{2}\right]}\binom{j}{i}a_{j-2i}
\end{aligned}$$

(ii)

$$\begin{aligned}
\alpha^0 &= 1 = \sum_{i=0}^{p-1}\left(-\zeta^i\right) \overset{\mathrm{char}K=2}{=} \sum_{i=0}^{p-1}\zeta^i = \sum_{i=0}^{\frac{p-1}{2}}\zeta^i + \sum_{i=\frac{p-1}{2}+1}^{p-1}\zeta^i \\
&\overset{\text{Θέτω } i\to p-i}{=} \sum_{i=0}^{\frac{p-1}{2}}\zeta^i + \sum_{i=0}^{\frac{p-1}{2}}\zeta^{p-i} = \sum_{i=0}^{\frac{p-1}{2}}\zeta^i + \sum_{i=0}^{\frac{p-1}{2}}\zeta^{-i} \\
&= \sum_{i=0}^{\frac{p-1}{2}}\left(\zeta^i+\zeta^{-i}\right) = \sum_{i=0}^{\frac{p-1}{2}}a_i
\end{aligned}$$

□

Αναφορές

[1] Ανδρεαδάκη Σ., *Θεωρία Galois*, Εκδόσεις Συμμετρία, 1999

[2] Πουλάκη Δ., *Θεωρία Αριθμών, Μία σύγχρονη θεώρηση της κλασικής Θεωρίας Αριθμών*, Εκδόσεις Ζήτη, 1998

[3] Artin, E. *Galois Theory,* Second Edition, 1944

[4] Ash, R. *Abstract Algebra, The Basic Graduate Year,* 2000

[5] Coutinho, S.C. *The Mathematics of Ciphers,* Num. th., RSA

[6] Elgamal, T. *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,* IEEE Trans. Info. Th. 31 (1985). 469-472

[7] S. Gao, *The determination of optimal normal bases over Finite Fields*, CORR 92-01, Department of Combinatorics and Optimization, University of Waterloo, 1992.

[8] Gao, S. and Lenstra, H.W., *Optimal Normal Bases*, Designs, Codes and Cryptography. 2 (1992),315-323.

[9] Hsu, I.S., Truong, T.K., Deutsch, L.J., and Reed, I.S., *A Comparison of VLSI Architecture of Finite Field Multipliers Using Dual, Normal, or Standard Bases,* IEEE Trans. Comp. vol.C-37. No.6 (1988). 735-739

[10] Lenstra, H.W., Jr. *Optimal Normal Bases Over the Field of Two Elements*. preprint. 1991

[11] Leveque W.J., *Topics in Number Theory*, (2 volumes), Addison-Wesley, Reading, Mass., 1956.

[12] Lidl, R., and Niederreiter, H. *Introduction to Finite Fields and Their Applications*. Cambridge University Press. 1986

[13] Massey, J.L., and Omura, J.K. *Computational Method and Apparatus for Finite Field Arithmetic,* U.S.patent 4,587,627,. May 1986

[14] Morii, M., Kasahara, M., and Whiting, D., *Efficient Bit-serial Multiplication and the Discrete-time Wiener-Hopf Equation Over Finite Fields*. IEEE Trans. Info. Th. bf 35 (1989). 1177-1183

[15] Mullin, R.C., Onyszchuk, I., Vanstone, S., and Wilson, R. *Optimal Normal Bases in GF(pn)*. Discrete Applied Math. 22 (1988 / 1989). 149-161

[16] Mullin R.C., *A characterization of the extremal distributions of optimal normal bases*, to appear in Proc. Marshall Hall Memorial Conference, Burlington, Vermont, 1990.

[17] Stinson, D.H., *On Bit-serial Multiplication and Dual Bases in GF(2m),* IEEE Trans. Info. Th. 37 (1991). 1733-1736

[18] Wang, M., and Blake, I.F. *Bit-serial Multiplication in Finite Fields*. SIAM J. Disc. Math. 3 (1990). 140-148

Ευρετήριο

Artin's lemma , 17
Lenstra , 75
Galois
    επέκταση, 21, 23, 40, 45, 54
    ομάδα, 5, 21, 40, 45, 54

απεικόνιση
    γραμμική, 11, 12, 14–16, 25, 37, 40, 44, 57, 59, 60
    πίνακας, 25, 33, 41
αυτομορφισμός, 19
    ταυτοτικός, 38
αυτομορφισμοί, 18

βάσεις
    ισοδύναμες, 75
βάση, 19
    βέλτιστη, 35, 37, 39, 41, 42, 45, 54, 58
    δυϊκή, 19, 21, 24, 42, 45, 58
    κανονική, 7, 18, 23, 27, 33, 37–40
    συνήθης, 55, 57
    Τύπου I, 69, 73
    Τύπου II, 72, 73, 76

διανυσματικός χώρος, 11, 12, 14–16, 18, 55

επέκταση, 7, 78
    αλγεβρική, 54
    διαχωρίσιμη, 19, 78
    κανονική, 78
    πεπερασμένη, 18

γραμμική ανεξαρτησία, 20, 23

ιδεώδες, 12
ιχνος, 19, 23, 24

κρυπτοσύστημα
    Diffie-Hellman, 28
    El-Gamal, 28
κυκλικό διάνυσμα, 16

ομάδα, 61
    κυκλική, 18
    πολλαπλασιαστική, 17, 61
ομομορφισμός, 17
ορίζουσα, 39

πίνακας
    ανάστροφος, 25, 26
    ιδιάζων, 19
    μοναδιαίος, 16
    πολλαπλασιαστικός, 27
πολυώνυμο
    ανάγωγο, 2–4, 54, 61, 78
    ελάχιστο, 16, 61

ελάχιστο (γραμμικής απεικόνισης), 14, 18
μονικό, 61
χαρακτηριστικό, 16, 18
πολυπλοκότητα, 35, 37, 38
πρωταρχική ρίζα μονάδος, 54, 62, 78

ρίζες της μονάδος, 78

σώμα
πεπερασμένο, 11, 18
πρώτο, 1
σχήμα
Massey-Omura, 27
συζυγής, 18, 42, 56

υπολογιστικό «κόστος», 28, 33, 35