Γιάννη Α. Αντωνιάδη
Τμήμα Μαθηματικών,
Πανεπιστήμιο Κρήτης

Εφαρμοσμένη Άλγεβρα

Σημειώσεις
Μάριου Μαγιολαδίτη

Έκδοση ΕΠΕΑΕΚ «Μαθηματικά για το 2001»
Ηράκλειο, 2000

Εισαγωγή

Η θεωρία των πεπερασμένων σωμάτων αποτελεί, παραδοσιακά, μέρος της Θεωρίας του Galois. Ιδιαίτερα στο πρόγραμμα σπουδών του Τμήματός μας, αποτελεί μέρος του περιεχομένου του αντίστοιχου μεταπτυχιακού μαθήματος.

Η θεωρία όμως είναι πάρα πολύ χρήσιμη τόσο στη Θεωρία Κωδίκων όσο και στην Κρυπτολογία, δυο σχετικά καινούριους κλάδους των μαθηματικών με τεράστια ανάπτυξη τα τελευταία χρόνια. Είναι συνεπώς απαραίτητη η διδασκαλία της σε προπτυχιακό επίπεδο. Αυτό θα πρέπει να γίνει με τέτοιο τρόπο ώστε να είναι κατανοητή από το ακροατήριο, χωρίς τη χρήση πολλών τεχνικών όρων, ιδιαίτερα δε διότι, συνήθως, το ακροατήριο αποτελείται και από φοιτητές άλλων τμημάτων, όπως αυτό της Επιστήμης των Υπολογιστών.

Οι παρούσες σημειώσεις ασχολούνται με την μελέτη των **πεπερασμένων σωμάτων** και την ανάλυση σε γινόμενο αναγώγων παραγόντων των **κυκλοτομικών πολυωνύμων.**

Έχει χρησιμοποιηθεί αποκλειστικά το βιβλίο του Robert J. McEliece, "Finite Fields for Computer Scientists and Engineers", Kluwer Academic Publishers. Λόγω έλλειψης χρόνου μερικά θεωρήματα δεν αποδείχθηκαν.

Σημειώσεις κράτησε ο φοιτητής Μάριος Μαγιολαδίτης ο οποίος είχε και την ηλεκτρονική επεξεργασία του κειμένου. Τον ευχαριστώ θερμά.

Επίσης ευχαριστώ τον επιστημονικό υπεύθυνο του ΕΠΕΑΕΚ «Μαθηματικά για το 2001» και Επ. Καθηγητή του Τμήματος κύριο Χρήστο Κουρουνιώτη με τη βοήθεια του οποίου εκδίδονται οι παρούσες σημειώσεις.

Γιάννης Α. Αντωνιάδης, Καθηγητής
Ηράκλειο, Μάρτης 2000

Κεφάλαιο 0

Εισαγωγικά

(0.1) Έστω ένα μη κενό σύνολο Α. Μια (διμελής) **πράξη** $*$ ή αλλιώς ένας **νόμος εσωτερικής σύνθεσης** είναι μια απεικόνιση $* : A \times A \to A$.

(0.2) Ορισμός Ένα σύνολο G εφοδιασμένο με μία διμελή πράξη $*$ θα λέγεται **ομάδα**, και θα συμβολίζεται $(G, *)$, όταν ισχύουν τα εξής αξιώματα:

(i) Η πράξη * είναι προσεταιριστική.
(ii) Υπάρχει ένα στοιχείο e στο G τέτοιο ώστε $e * x = x * e = x$ για κάθε x στο G.
(iii) Για κάθε α στο G υπάρχει ένα στοιχείο β στο G με την ιδιότητα $\alpha * \beta = \beta * \alpha = e$.

Αν, επιπλέον, η πράξη είναι αντιμεταθετική η ομάδα θα λέγεται **αντιμεταθετική** ή **αβελιανή**.

Αποδεικνύεται ότι αν G ομάδα, τότε υπάρχει μοναδικό e με αυτή την ιδιότητα. Θα το ονομάζουμε **μοναδιαίο** ή **ουδέτερο** στοιχείο.

Επίσης αν μας δοθεί ένα α στην ομάδα G τότε το β που ορίσαμε πιο πάνω είναι μοναδικό. Θα το ονομάζουμε **αντίστροφο** ή **αντίθετο** του α.

(0.3) Παραδείγματα

Το $(\mathbb{Z}, +)$ είναι αβελιανή ομάδα ενώ το $(\mathbb{Z}, \cdot)$ δεν αποτελεί ομάδα.

(0.4) Ορισμός Έστω Η ένα υποσύνολο ενός συνόλου G. Αν $(G, *)$ και $(H, *)$ είναι ομάδες για κάποια διμελή πράξη $*$ τότε λέμε ότι η $(H, *)$ **είναι υποομάδα της** $(G, *)$. Θα γράφουμε $(H, *) \leq (G, *)$.

(0.5) Παράδειγμα

$(\mathbb{Z}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$

(0.6) Ορισμός Ένα σύνολο R εφοδιασμένο με δυο πράξεις + και $\cdot$ θα λέγεται **δακτύλιος**, όταν ισχύουν τα ακόλουθα αξιώματα:

(i) Η ομάδα (R,+) είναι αβελιανή
(ii) Για το $(R, \cdot)$ ισχύουν
(1) προσεταιρισμός: $\alpha(\beta\gamma) = (\alpha\beta)\gamma$, για κάθε $\alpha, \beta, \gamma \in R$
(2) επιμερισμός: $\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma$, για κάθε $\alpha, \beta, \gamma \in R$
$(\alpha+\beta)\gamma = \alpha\gamma + \beta\gamma$, για κάθε $\alpha, \beta, \gamma \in R$

Αν υπάρχει ένα στοιχείο, $1 \in R$ τέτοιο ώστε $1 \cdot a = a \cdot 1 = a$, για κάθε $a \in R$ τότε αυτό θα λέγεται **μοναδιαίο** στοιχείο του δακτυλίου και ο δακτύλιος λέγεται **δακτύλιος με μοναδιαίο**. Αν ισχύει $\alpha\beta = \beta\alpha$ για κάθε $\alpha, \beta \in R$ τότε ο δακτύλιος λέγεται **αντιμεταθετικός**. Αν, τέλος ένας δακτύλιος R έχει μοναδιαίο και ισχύει η αντιμεταθετικότητα του πολλαπλασιασμού θα λέγεται **αντιμεταθετικός δακτύλιος με μοναδιαίο**.

(0.7) Ορισμός Ένα μη μηδενικό στοιχεία a του δακτυλίου $(R,+,\cdot)$ θα λέγεται **διαιρέτης του μηδενός** αν υπάρχει μη μηδενικό στοιχείο b του δακτυλίου τέτοιο ώστε $ab = 0$.

(0.8) Ορισμός Ένας αντιμεταθετικός δακτύλιος με μοναδιαίο, χωρίς διαιρέτες του μηδενός, λέγεται **ακεραία περιοχή**.

Για παράδειγμα, ο δακτύλιος $(\mathbf{Z}, +, \cdot)$ των ακεραίων αριθμών είναι ακεραία περιοχή.

(0.9) Ορισμός Ένα σύνολο K εφοδιασμένο με δυο πράξεις + και $\cdot$ θα λέγεται **σώμα**, όταν ισχύουν τα εξής αξιώματα:

(i) Η ομάδα $(K,+)$ είναι αβελιανή.
(ii) Η ομάδα $(K^*,\cdot)$, όπου $K^* = K\backslash\{0\}$, είναι αβελιανή.
(iii) $\alpha(\beta+\gamma) = \alpha\beta+\alpha\gamma$, για κάθε $\alpha, \beta, \gamma \in K$

(0.10) Παρατήρηση Ένα σώμα είναι ένας αντιμεταθετικό δακτύλιος με μοναδιαίο όπου κάθε μη-μηδενικό στοιχείο έχει αντίστροφο ως προς την πράξη του πολλαπλασιασμού.

Για παράδειγμα τα σύνολα $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{R}$ εφοδιασμένα με τις πράξεις της συνήθης πρόσθεσης και του συνήθη πολλαπλασιασμού είναι σώματα και μάλιστα με άπειρα στοιχεία.

Αυτά τα σώματα δεν μας ενδιαφέρουν στο παρών μάθημα. Εμείς ενδιαφερόμαστε για τα πεπερασμένα σώματα.

(0.11) Ορισμός Ένα σώμα θα λέγεται **πεπερασμένο** όταν έχει πεπερασμένο πλήθος στοιχείων.

Για παράδειγμα το σύνολο $\mathbf{F}_2=\{0,1\}$ με πράξεις:

+	**0**	**1**
0	0	1
1	1	0

Και

$\otimes$	**1**
1	1

αποτελεί πεπερασμένο σώμα με δύο στοιχεία.

(0.12) Ορισμός Έστω n φυσικός αριθμός, $n > 1$. Αν $a, b \in \mathbb{Z}$ θα λέμε ότι το a είναι **ισοδύναμο** (ή **ισότιμο**) modulo n αν το n διαιρεί το $a - b$.

Θα συμβολίζουμε ότι το a είναι ισοδύναμο modulo n με το b με $a \equiv b \pmod n$. Αυτή είναι μια σχέση ισοδυναμίας στο $\mathbb{Z}$ αφού ισχύουν

i) $a \equiv a \pmod n$ διότι $n \mid a-a = 0$ για κάθε $a \in R$ (*ανακλαστική*)
ii) $a \equiv b \Rightarrow m \mid a - b \Rightarrow m \mid -(a - b) \Rightarrow m \mid b - a \Rightarrow b \equiv a$ (*συμμετρική*)
iii) $a \equiv b \wedge b \equiv c \Rightarrow a \equiv c$ (*μεταβατική*)

άρα χωρίζει το $\mathbb{Z}$ σε κλάσεις ισοδυναμίας. Την κλάση ενός στοιχείου $a \in \mathbb{Z}$ θα την συμβολίζουμε με [a] ή με a mod n ή με K_a. Δηλαδή $[a] = \{ b \in \mathbb{Z} \mid b \equiv a \pmod n\}$. Το σύνολο των κλάσεων mod n θα το συμβολίζουμε με $\mathbb{Z}_n$. Μπορούμε λοιπόν να γράψουμε ότι $\mathbb{Z}_n = \{ [0], [1], \ldots, [n-1] \}$.

Για παράδειγμα για $n = 4$ έχουμε 4 κλάσεις ισοδυναμίας:

$$[0] = \{0, \pm 4, \pm 8 \pm 12, \pm 16, \ldots\} \qquad [2] = \{\ldots, -14, -10, -6, -2, 2, 6, 10, \ldots\}$$
$$[1] = \{\ldots, -7, -3, 1, 5, 9, \ldots\} \qquad [3] = \{\ldots, -9, -5, -1, 3, 7, 11, 15, \ldots\}$$

Ορίζουμε στο σύνολο των κλάσεων $\mathbb{Z}_n$ πράξεις πρόσθεσης + και πολλαπλασιασμού $\otimes$ ως εξής:

$$[a] + [b] = [a + b]$$
$$[a] \otimes [b] = [a\, b]$$

Εύκολα αποδεικνύεται ότι οι πράξεις είναι καλά ορισμένες και ότι η τριάδα $(\mathbb{Z}_n, +, \otimes)$ αποτελεί αντιμεταθετικό δακτύλιο με μοναδιαίο στοιχείο.

Ξεχωρίζουμε δύο περιπτώσεις:

(I) Ο n είναι σύνθετος. Δηλαδή υπάρχουν $a, b \in \mathbb{N}$, $a > 1$, $b > 1$ τέτοια ώστε $n = ab$. Τότε όμως $[a] \neq [0]$, $[b] \neq [0]$ αφού $a, b < n$ αλλά $[a] \otimes [b] = [ab] = [n] = [0]$. Δηλαδή ο δακτύλιος $(\mathbb{Z}_n, +, \otimes)$ έχει διαιρέτες το 0.

(II) Ο n είναι πρώτος. Τότε αν υπήρχαν $a, b \in \mathbb{N}$ τέτοιοι ώστε $[a] \otimes [b] = [0]$ ή αλλιώς $[ab] = [0]$ θα σήμαινε ότι το n θα διαιρούσε το ab ή επειδή ο n είναι πρώτος ότι θα διαιρούσε ή το a ή το b δηλαδή ή $[a] = [0]$ ή $[b] = [0]$. Επομένως, ο $(\mathbb{Z}_n, +, \otimes)$ δεν έχει διαιρέτες το 0. Είναι δηλαδή ακέραια περιοχή. Πιο συγκεκριμένα είναι σώμα διότι για κάθε [a] με $[a] \neq [0]$ αυτό σημαίνει ότι το n δεν διαιρεί το a δηλαδή μκδ(a, n) = 1, δηλαδή η ισοδυναμία $ax \equiv 1 \pmod n$ έχει μοναδική λύση, έστω b. Επομένως, $[a] \otimes [b] = [ab] = [1]$ άρα κάθε μη-μηδενική κλάση ισοδυναμίας έχει αντίστροφο.

Ώστε για κάθε πρώτο p η $(Z_p, +, \otimes)$ είναι σώμα με p στοιχεία. Θα το συμβολίζουμε με $\mathbf{F}_p$.

Για παράδειγμα το $\mathbf{F}_3 = Z_3 = \{[0], [1], [2]\}$ αποτελεί σώμα με πίνακες πρόσθεσης και πολλαπλασιασμού:

+	**[0]**	**[1]**	**[2]**
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

Και

⊗	**[1]**	**[2]**
[1]	[1]	[2]
[2]	[2]	**[1]**

Επειδή το 4 είναι σύνθετος, δείξαμε προηγουμένως ότι ο δακτύλιος Z_4 δεν είναι σώμα. Για παράδειγμα το [2] δεν έχει πολλαπλασιαστικό αντίστροφο. Ωστόσο, υπάρχει σώμα με **4** στοιχεία. Αν συμβολίσουμε τα στοιχεία του με 0, 1, 2, 3 τότε οι πίνακες πρόσθεσης και πολλαπλασιασμού είναι οι εξής:

+	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

·	**1**	**2**	**3**
1	1	2	3
2	2	3	1
3	3	1	2

Εντελώς φυσιολογικά τίθενται τα ακόλουθα δύο ερωτήματα:

(I) Έστω $n \in \mathbb{N}$, υπάρχει σώμα με n στοιχεία;

(II) Υποθέτουμε ότι για κάποιο $n \in \mathbb{N}$ υπάρχει τουλάχιστον ένα σώμα με n στοιχεία. Πόσα μη ισόμορφα μεταξύ τους σώματα με n στοιχεία υπάρχουν;

Οι απαντήσεις σε αυτά τα ερωτήματα αποτελούν το πρώτο μέρος του βιβλίου και θα είναι οι εξής:

(I) Αν ο n είναι δύναμη πρώτου αριθμού, δηλαδή $n = p^\lambda$ για κάποιο πρώτο p και κάποιο ακέραιο λ τότε υπάρχει πάντοτε ένα σώμα με n στοιχεία. Αλλιώς, αν ο n δεν είναι δύναμη πρώτου δεν υπάρχει κανένα με n στοιχεία.

(II) Αν υπάρχει πεπερασμένο σώμα με n στοιχεία τότε αυτό είναι μοναδικό. Δηλαδή δύο πεπερασμένα σώματα με n στοιχεία είναι μεταξύ τους ισόμορφα.

Κεφάλαιο 1

Ευκλείδειες περιοχές και Ευκλείδειος αλγόριθμος

Όπως ειπώθηκε στο προηγούμενο κεφάλαιο το (**Z, +,** ·) είναι μια ακέραια περιοχή, Επίσης γνωρίζουμε ότι στους ακέραιους μπορούμε να ορίσουμε την έννοια του μέγιστου κοινού διαιρέτη δυο (ή και περισσότερων) ακεραίων.

(1.1) Ορισμός Αν a, b$\in$**Z** ο φυσικός αριθμός d είναι ο **μέγιστος κοινός διαιρέτης** (ΜΚΔ) των a και b όταν:

(i) d|a και d|b (είναι δηλαδή ένας κοινός τους διαιρέτης)
(ii) Αν d′ ακέραιος τέτοιος ώστε d′|a και d′|b τότε d′|d (είναι δηλαδή μέγιστος)

Για παράδειγμα:

ΜΚΔ(6,15) = 3
ΜΚΔ(24,36) = 12

Επίσης στο **Z**, μπορούμε να διαιρέσουμε δυο ακεραίους, δηλαδή αν a, b $\in$ **Z**, b$\neq$0 τότε υπάρχουν q και r τέτοιοι ώστε a = bq + r όπου $0 \le r < |b|$.

Το q ονομάζεται **πηλίκο της διαίρεσης των a και b** και το r ονομάζεται **υπόλοιπο** και είναι μονοσήμαντα ορισμένα**.**

Εδώ βλέπουμε ότι στον ορισμό της διαιρετότητας χρησιμοποιείται η έννοια της απόλυτης τιμής. Η απόλυτη τιμή ενός ακεραίου είναι μη-αρνητικός ακέραιος. Επίσης, η διαιρετότητα χρησιμοποιείται για την εύρεση του μέγιστου κοινού διαιρέτη δύο ακεραίων.

Για παράδειγμα:

36 = 24 + 12
24 = 2 · 12 + 0
Δηλαδή ΜΚΔ(36,24)=12

Αυτή η διαδικασία λέγεται αλγόριθμος του Ευκλείδη.

Όταν το υπόλοιπο γίνει μηδέν το τελευταίο πηλίκο είναι ο ΜΚΔ. Μάλιστα ακολουθώντας την αντίθετη πορεία, ο ΜΚΔ(a, b) γράφεται σαν γραμμικός συνδυασμός των a, b.

Θα προσπαθήσουμε τώρα να δώσουμε κατάλληλο ορισμό, σε δακτυλίους που έχουν ιδιότητες ανάλογες με αυτές του **Z** που μόλις περιγράψαμε.

(1.2) Ορισμός **Ευκλείδεια περιοχή** (ή ευκλείδειος δακτύλιος) R είναι μια ακέραια περιοχή εφοδιασμένη με μια συνάρτηση $g : R^* \to \{0,1,2,3,\ldots\}$, $R^* = R \setminus \{0\}$, τέτοια ώστε:

(i) g(a) ≤ g(ab) για κάθε μη μηδενικά στοιχεία a, b του R.

(ii) Για κάθε a, b $\in$ R με b $\neq 0$ υπάρχουν q, r $\in$ R (ονομάζονται πηλίκο και υπόλοιπο αντίστοιχα) τέτοια ώστε a = bq + r όπου r = 0 ή αλλιώς g(r) < g(b).

Σημείωση: Αν χρειαστεί ορίζουμε $g(0) = -\infty$

Κλασικό παράδειγμα (το πρότυπο) είναι $(\mathbf{Z}, |\,.\,|)$ (όπου $|\,.\,|$ η συνήθης απόλυτη τιμή).

Ας πάρουμε το δακτύλιο $R = \mathbf{Z}[i] = \mathbf{Z} + \mathbf{Z}i = \{a + bi \mid a, b \in \mathbf{Z}\}$

Η ομάδα (R,+) είναι αβελιανή και μάλιστα υποομάδα της (C,+)

Διότι αν πάρουμε x, y $\in$ R τότε $\begin{cases} x = a + bi \mid a, b \in Z \\ y = c + di \mid c, d \in Z \end{cases}$ οπότε

$x - y = (a - c) + (b - d)i \in R$ αφού $(a - c \in \mathbf{Z})$ και $(b - d \in \mathbf{Z})$.

Ισχύει επίσης $(R^*, \cdot) \leq (C^*, \cdot)$

Ο προσεταιρισμός, οι επιμερισμοί και η αντιμεταθετικότητα ισχύουν διότι ισχύουν για όλα τα στοιχεία του $C^* = C\backslash\{0\}$. Το μοναδιαίο στοιχείο του R είναι το 1+0i και επίσης ο R δεν έχει διαιρέτες του μηδενός διότι είναι υποδακτύλιος του C ο οποίος είναι σώμα και συνεπώς δεν έχει διαιρέτες του μηδενός. Επομένως ο δακτύλιος $R = \mathbf{Z}[i]$ είναι ακέραια περιοχή. Θα αποδείξουμε ότι ο R αποτελεί **ευκλείδεια περιοχή** ως προς την συνάρτηση $g : \mathbf{Z}[i]\backslash 0 \to \{0,1,2,3,\ldots\}$ η οποία ορίζεται ως εξής:
Αν x = a+bi τότε $g(x) = a^2 + b^2 = (a+bi)(a-bi)$.

Έστω x = a + bi, y = c + di $\in \mathbf{Z}[i]$, όπου a, b, c, d$\in \mathbf{Z}$ και $y \neq 0$
Τότε $g(x) = a^2 + b^2$ και xy = (ac – bd) + (ad + bc)i οπότε
$g(xy) = (ac - bd)^2 + (ad + bc)^2 = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = a^2 (c^2 + d^2) + b^2 (c^2 + d^2) =$
$= (a^2 + b^2)(c^2 + d^2) = g(x)\, g(y)$.

Επειδή $c^2 + d^2 \geq 1$ έχουμε ότι $g(xy) \geq g(x)$, έτσι αποδείξαμε την (i).

Τώρα θα αποδείξουμε την (ii).

Έστω x = a + bi, y = c + di$\in \mathbf{Z}[i]$ (a, b, c, d$\in \mathbf{Z}$) $y \neq 0 \Rightarrow (c,d) \neq (0, 0)$

Επειδή x, y $\in$ C μπορούμε να διαιρέσουμε.

Έστω $q' := xy^{-1} = \frac{x}{y} = \frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd}{c^2+d^2} + \frac{cb-ad}{c^2+d^2}i \in Q[i]$.

Γράφουμε, $q' = x' + y'i \mid x', y' \in Q$.

Διαλέγουμε ένα σημείο με ακέραιες συντεταγμένες που βρίσκεται πιο κοντά στο σημείο (x', y').

Έστω (z, w) αυτό το σημείο.
Τότε $|x' - z| \le \frac{1}{2}, |y' - w| \le \frac{1}{2}$.
Έστω $q = z + wi \in \mathbf{Z}[i]$. Οπότε
$g(q' - q) = |q' - q|^2 = |(x' - z) + (y' - w)i|^2 \le |x' - z|^2 + |y' - w|^2 \le \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$.
Έστω $r := x - qy \in \mathbf{Z}[i]$. Τότε $r = q'y - qy = (q' - q)y$.

Αν $q' = q$ έπεται ότι $r = 0$

Αλλιώς $g(r) = g((q' - q)y) = |q' - q|^2 |y|^2 \le \frac{1}{2}|y|^2 < |y|^2 = g(y)$. (αποδείξαμε και την (ii)).

□

Αν K σώμα τότε ο δακτύλιος R = K[X] των πολυωνύμων μιας μεταβλητής με συντελεστές από το σώμα K με την συνάρτηση $g : R \setminus \{0\} \to \{0,1,2,3,\ldots\}$ με τύπο $g(f(X)) = \deg f$, όπου deg f ο βαθμός του πολυωνύμου f(X), είναι ευκλείδεια περιοχή.

(i) Έστω $f_1, f_2 \in K[X]$ με $\deg f_1 = k_1 \ge 0, \deg f_2 = k_2 \ge 0$
$g(f_1 \cdot f_2) = \deg(f_1 \cdot f_2) = k_1 + k_2 \ge k_1 = \deg(f_1) = g(f_1)$

(ii) Έστω $f_1, f_2 \in K[X], f_2 \ne 0$ τότε υπάρχουν μοναδικά πολυώνυμα $q, r \in R$ τέτοια ώστε: $f_1 = f_2 q + r$ όπου $r = 0$ ή $g(r) = \deg(r) < \deg(f_2) = g(f_2)$.

<u>Απόδειξη του (ii):</u>

Έστω $h = h_0 + h_1 X + \ldots + h_m X^m \in K[X] \quad (h_m \ne 0)$
και $f = f_0 + f_1 X + \ldots + f_n X^n \in K[X] \quad (f_n \ne 0)$
- Αν $n < m$ τότε παίρνουμε $q = 0$ και $r = f$.

Δηλαδή $f = h \cdot 0 + f$ και $\deg r = \deg f = n < m = \deg h$.
- Αν $n \ge m$ θα εφαρμόσουμε επαγωγή ως προς n.

Για $n = 0$ το θεώρημα ισχύει διότι $0 \ge m$ οπότε και $m = 0$.
Δηλαδή $h = h_0$ και $f = f_0$. Οπότε $f = h_0 (h_0^{-1} f) + 0$. Επομένως, $q = h_0^{-1} f$ και $r = 0$.
Υποθέτουμε ότι ισχύει για όλα τα πολυώνυμα βαθμού μικρότερου του n και θεωρούμε το πολυώνυμο $f^* = f - f_n h_m^{-1} X^{n-m} h$. Επειδή ο $\deg f^*$ είναι μικρότερος του degf λόγω της υπόθεσης της μαθηματικής επαγωγής έπεται ότι υπάρχουν μοναδικά (q^*, r) πολυώνυμα του K[X] τέτοια ώστε $r = 0$ ή $\deg r < \deg h$ και $f^* = hq + r$.
Επομένως,

$f = f^* + f_n h_m^{-1} X^{n-m} h =$
$= q^* h + r + f_n h_m^{-1} X^{n-m} h =$
$= h(q^* + f_n h_m^{-1} X^{n-m}) + r =$

$= hq + r$

Όπου $q = q^* + f_n h_m^{-1} X^{n-m}$.

Έστω τώρα ότι για τα δοσμένα πολυώνυμα f και h υπάρχουν δύο ζευγάρια (q, r) και $(\bar{q}, \bar{r})$ τέτοια ώστε:

$f = hq + r \mid r = 0$ είτε $\deg r < \deg h$

$f = h\bar{q} + \bar{r} \mid \bar{r} = 0$ είτε $\deg \bar{r} < \deg h$.

Θα αποδείξουμε ότι $q = \bar{q}$ και $r = \bar{r}$.

Πράγματι: $hq + r = h\bar{q} + \bar{r}$ ή $h(q - \bar{q}) = \bar{r} - r$

Αν $q \neq \bar{q}$ τότε $\deg\big(h(q - \bar{q})\big) \geq \deg h$.

Ενώ $\deg\big(h(q - \bar{q})\big) = \deg(\bar{r} - r) < \deg h$. Άτοπο

Συνεπώς $q = \bar{q}$. Οπότε και $r = \bar{r}$.

□

(1.3) Άσκηση: Να αποδείξετε ότι ο $\mathbf{Z}[\sqrt{-3}] = \left\{a + b\sqrt{-3} \,\middle|\, a, b \in Z\right\}$ είναι ευκλείδειος δακτύλιος ως προς την συνάρτηση $g : \mathbf{Z}[\sqrt{-3}] \to \{0,1,2,3,\ldots\}$ με $g\left(a + b\sqrt{-3}\right) = \left|a + b\sqrt{-3}\right|^2 = a\text{^}2 + 3b^2$.

(1.4) Ορισμοί Έστω R Ευκλείδεια περιοχή. Το ε λέγεται **μονάδα** (ή **αντιστρέψιμο στοιχείο**) του R όταν υπάρχει $\varepsilon' \in R$ τέτοιο ώστε $\varepsilon \cdot \varepsilon' = 1$.

Το σύνολο $E(R) := \{\varepsilon \in R \,/\, \exists\, \varepsilon' \in R \text{ τ.ω. } \varepsilon \cdot \varepsilon' = 1\}$ είναι το **σύνολο των μονάδων** του R.

(1.5) Παράδειγμα Για $R = \mathbf{Z}$ έχουμε ότι $E(R) = \{-1, 1\}$

(1.6) Ορισμός Δυο στοιχεία $a, b \in R$ θα λέγονται **συνεταιρικά** όταν υπάρχει $\varepsilon \in E(R)$ τέτοιο ώστε $a = b\varepsilon$.

Θα το συμβολίζουμε $a \cong b$.

(1.7) Παραδείγματα:

(i) Το 3 και το –3 είναι συνεταιρικά στοιχεία της ευκλείδειας περιοχής **Z.**

(ii) Το πολυώνυμο $X^2 + 2X + 9$ είναι συνεταιρικό του $5X^2 + 10X + 45$ στην Ευκλείδεια περιοχή K[X] διότι $5X^2 + 10X + 45 = 5(X^2 + 2X + 9)$ και $5 \in E(K[X]) = K^*$.

(iii) Τα στοιχεία $1 + i$ και $1 - i$ της ευκλείδειας περιοχής $\mathbf{Z}[i]$ είναι συνεταιρικά αφού $-i(1 + i) = -i - i^2 = -i - (-1) = 1 - i$ και $-i \in E(Z[i])$.

(1.8) Παρατήρηση Έστω $(R, +, \cdot)$ ένας δακτύλιος. Τότε η $(E(R), \cdot)$ αποτελεί πολλαπλασιαστική ομάδα.

Σε κάθε ευκλείδεια περιοχή μπορούμε να ορίσουμε την έννοια του μεγίστου κοινού διαιρέτη (ΜΚΔ) δύο ή περισσοτέρων (πεπερασμένου όμως πλήθους) στοιχείων της περιοχής.

(1.9) Ορισμός: Αν R Ευκλείδεια περιοχή και a, b ∈ R ένα στοιχείο d ∈ R θα είναι ένας **ΜΚΔ** των a, b όταν ισχύουν:

(i) d|a και d|b (είναι δηλαδή ένας κοινός τους διαιρέτης)
(ii) Αν $d' \in R$ τέτοιο ώστε $d'|a$ και $d'|b$ τότε $d'|d$ (είναι δηλαδή μέγιστος)

Αν τώρα d_1, d_2 δύο ΜΚΔ των a, b τότε έχουμε:

$$\begin{cases} d_1 \mid d_2 \\ d_2 \mid d_1 \end{cases} \Rightarrow \begin{cases} d_2 = rd_1 \ (r \in R) \\ d_1 = sd_2 \ (s \in R) \end{cases} \Rightarrow d_2 = rsd_2 \Rightarrow d_2(1 - rs) = 0 \Rightarrow rs = 1 \Rightarrow r \in E(R).$$

Επομένως, τα d_1 και d_2 είναι **συνεταιρικά** (διαφέρουν δηλαδή κατά μια μονάδα του δακτυλίου R).

Επομένως, ο ΜΚΔ των a και b ορίζεται κατά προσέγγιση μονάδας του R.

- Αν d = ΜΚΔ(a, b) τότε υπάρχουν x και y στοιχεία του R τέτοια ώστε ax + by = d.
  (Η απόδειξη είναι εντελώς όμοια με το **Z**).
- Αν s, t, r ∈ **Z** τότε ΜΚΔ(s, t) = ΜΚΔ(s, t – rs).

Απόδειξη

Στο **Z** έχουμε τα εξής.

Έστω d_1 := ΜΚΔ(s, t) και d_2 = ΜΚΔ(s, t – rs). Έχουμε ότι

$$\left.\begin{array}{l} \left.\begin{array}{l} d_1|s \wedge d_1|t \\ d_1|s \Rightarrow d_1|rs \end{array}\right\} \Rightarrow d_1|s \wedge d_1|(t - rs) \Rightarrow d_1|d_2 \\ \left.\begin{array}{l} d_2|s \wedge d_2|(t - rs) \\ d_1|s \Rightarrow d_1|rs \end{array}\right\} \Rightarrow d_2|s \wedge d_2|t \Rightarrow d_2|d_1 \end{array}\right\} \Rightarrow d_1 = d_2$$

□

Εντελώς όμοια είναι η απόδειξη σε οποιοδήποτε Ευκλείδειο δακτύλιο R.

Η ιδιότητα αυτή χρησιμοποιείται στον λεγόμενο αλγόριθμο του Ευκλείδη.

Πρόκειται για έναν αλγόριθμο υπολογισμού του μέγιστου κοινού διαιρέτη.

Ο αλγόριθμος του Ευκλείδη

Ζητείται ο ΜΚΔ των ακεραίων a, b.

Γράφουμε:

$a = bq_1 + r_1 \quad 0 \le r_1 < |b|$

$b = r_1q_2 + r_2 \quad 0 \le r_2 < r_1$

Συνεχίζουμε...

Τελικά: $r_{n-1} = r_n\, q_{n+1} + 0$ και $0 = r_{n+1}$

Τότε ΜΚΔ(α, b) = r_n

(1.10) Παράδειγμα:

Αν πάρουμε a = 45 και b = 19 τότε

$45 = 19 \cdot 2 + 7 \Rightarrow 19 = 7 \cdot 2 + 5 \Rightarrow 7 = 1 \cdot 5 + 2 \Rightarrow 5 = 2 \cdot 2 + 1 \Rightarrow 2 = 1 \cdot 2 + 0$

Επομένως ΜΚΔ(a, b) = 1.

Το 1 μπορεί να γραφεί σαν γραμμικός συνδυασμός των α και b με τον παρακάτω τρόπο:

$1 = 5 - 2 \cdot 2 \Rightarrow 1 = 5 - 2 \cdot (7 \cdot 5) \Rightarrow 1 = 3 \cdot 5 - 2 \cdot 7 \Rightarrow 1 = -2 \cdot 7 + 3 \cdot (19 - 7 \cdot 2) \Rightarrow$
$1 = 3 \cdot 19 - 8 \cdot 7 \Rightarrow 1 = 3 \cdot 19 - 8 \cdot (45 - 19 \cdot 2) \Rightarrow 1 = 19 \cdot 19 - 8 \cdot 45$

Δηλαδή $1 = 19 \cdot 19 + (-8) \cdot 45$

(1.11) Πρόταση Έστω R μια ευκλείδεια περιοχή και $t \in R$, m, n θετικοί ακέραιοι.

Τότε ΜΚΔ($t^n - 1, t^m - 1$) = $t^{\text{ΜΚΔ}(n,m)} - 1$

Απόδειξη

Θα κάνουμε την απόδειξη επαγωγικά ως προς το max{n, m}.

- Αν max{n, m} = 1 τότε m = n = 1.

  Οπότε έχουμε ότι $\text{ΜΚΔ}(t^n - 1, t^m - 1) = \text{ΜΚΔ}(t - 1, t - 1) = t - 1 = t^{\text{ΜΚΔ}(1,1)} - 1$ δηλαδή η πρόταση ισχύει.

- Επίσης αν m = n τότε ΜΚΔ(n, m) = n = m
  Οπότε ΜΚΔ($t^n - 1, t^m - 1$) = ΜΚΔ($t^n - 1, t^n - 1$) = $t^n - 1$. Η πρόταση ισχύει και πάλι.

- Έστω τώρα m < n.

Παρατηρούμε ότι $(t^n - 1) - t^{n-m}(t^m - 1) = t^{n-m} - 1$.

Επομένως $ΜΚΔ(t^n - 1, t^m - 1) = ΜΚΔ(t^m - 1, t^{n-m} - 1)$

Οπότε λόγω της μαθηματικής επαγωγής
$ΜΚΔ(t^n - 1, t^{n-m} - 1) = t^{ΜΚΔ(m,n-m)} - 1 = t^{ΜΚΔ(m,n)} - 1$

Άρα αποδείξαμε τη πρόταση.

□

(1.12) Πόρισμα: $ΜΚΔ(X^{q^n} - X, X^{q^d} - X) = X^{q^{ΜΚΔ(n,d)}} - X \quad (q \in N)$

(1.13) Παραδείγματα

$ΜΚΔ(2^{15} - 1, 2^{20} - 1) = 2^{ΜΚΔ(15,20)} - 1 = 2^5 - 1 = 31.$
$ΜΚΔ(X^{15} - 1, X^{20} - 1) = X^5 - 1$

Κεφάλαιο 2

Μονοσήμαντη ανάλυση σε Ευκλείδειες περιοχές

Στην Ευκλείδεια περιοχή **Z**, ισχύει το λεγόμενο Θεμελιώδες Θεώρημα της Αριθμητικής. Δηλαδή ότι κάθε ακέραιος α, $\alpha \notin \{0, 1, -1\}$ γράφεται μονοσήμαντα στη μορφή

$$\alpha = \varepsilon\, p_1 p_2 \ldots p_s$$

όπου $\varepsilon \in \{1, -1\}$ και $p_1, p_2, \ldots, p_s$ είναι πρώτοι αριθμοί.

Υπενθυμίζουμε και την βασική ιδιότητα που πληρούν οι πρώτοι: Αν p πρώτος και a, b ακέραιοι τέτοιοι ώστε p | ab τότε p | a ή p | b.

Σκοπός μας είναι να γενικεύσουμε το Θεμελιώδες Θεώρημα της Αριθμητικής για κάθε Ευκλείδεια περιοχή R.

Έστω R οποιαδήποτε Ευκλείδεια περιοχή.

(2.1) Ορισμός Αν $b \in R$ τότε μια ανάλυση του b θα είναι κάθε παράσταση της μορφής

$$b = a_1 \cdot a_2 \cdot \ldots \cdot a_s$$

όπου τα στοιχεία a_i είναι στοιχεία της R.

Βέβαια αν $u \in E(R)$ τότε υπάρχει $v \in R$ τέτοιο ώστε uv = 1 οπότε κάθε $b \in R$ έχει μια ανάλυση της μορφής $b = (bu) \cdot v = b' \cdot v$ $(b' = bu)$ όπου v μονάδα και b' συνεταιρικό του b.

Αυτή βέβαια είναι μια τετριμμένη ανάλυση.

(2.2) Ορισμός Η ανάλυση $b = a_1 \cdot a_2 \cdot \ldots \cdot a_s \mid a_i \in R\ \forall i$ θα λέγεται **τετριμμένη** όταν κάθε παράγοντας a_i του γινομένου είναι ή μονάδα ή συνεταιρικό στοιχείο του b.

Σημείωση Στην τετριμμένη ανάλυση του b μπορεί να υπάρχει το πολύ ένα συνεταιρικό στοιχείο του b. (γιατί;)

(2.3) Ορισμός Ένα στοιχείο $a \in R \setminus E(R)$ (όχι μονάδα) θα λέγεται **ανάγωγο** αν δεν έχει μη τετριμμένη ανάλυση. (Δηλαδή, κάθε ανάλυση του a είναι τετριμμένη).

Έστω $b \in R$. Ο $d \in R$ θα λέγεται **γνήσιος διαιρέτης** του b αν ο d δεν είναι συνεταιρικός του b και, φυσικά, $d \mid b$.

(2.4) Πρόταση Έστω R Ευκλείδεια περιοχή. Αν a ανάγωγο στοιχείο του R και d γνήσιος διαιρέτης αυτού τότε $d \in E(R)$.

Απόδειξη: Έχουμε ότι $d \mid a \Rightarrow a = d\lambda \mid \lambda \in R$. Η ανάλυση $a = d\lambda$ είναι τετριμμένη διότι a ανάγωγο. Επομένως, το d είναι ή συνεταιρικό του a ή μονάδα του R. Δεν είναι συνεταιρικό διότι είναι γνήσιος διαιρέτης άρα $d \in E(R)$.

(2.5) Παραδείγματα:

(i) Στο R=**Z** τα ανάγωγα στοιχεία είναι τα $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \pm 17, \ldots$

(ii) Στο R = K[X] τα ανάγωγα στοιχεία είναι τα ανάγωγα πολυώνυμα. Σ' αυτά θα αναφερθούμε αναλυτικά σε επόμενα κεφάλαια.

(iii) Στον **Z**[i] τα ανάγωγα στοιχεία είναι:
1) Οι πρώτοι αριθμοί p όπου $p \equiv 3 \pmod 4$. Π.χ. 3, 7, 11, 19, …
2) Τα στοιχεία $a + bi \in \mathbf{Z}[i] \mid a, b \in \mathbf{Z}$ τέτοια ώστε $a^2 + b^2 = 2$ ή $a^2 + b^2 = p$ όπου p πρώτος, $p \equiv 1 \pmod 4$. Π.χ. $1 + i$, $2 + i$, $3 + 2i$, …

(χωρίς απόδειξη)

(2.6) Ορισμός Έστω R ευκλείδεια περιοχή. Δυο στοιχεία $a, b \in R$ θα λέγονται πρώτα μεταξύ τους όταν ΜΚΔ(a, b) = 1 (ή οποιαδήποτε άλλη μονάδα του R).

(2.7) Λήμμα Αν R ευκλείδεια περιοχή και $a, b \in R$ πρώτοι μεταξύ τους (δηλαδή ΜΚΔ(a, b) = 1) $\Leftrightarrow$ $\exists s, t \in R$ τέτοια ώστε $sa + tb = 1$.

Απόδειξη:

($\Rightarrow$) Ο ΜΚΔ των a,b γράφεται σαν γραμμικός συνδυασμός των a και b. Αφού, ΜΚΔ(a,b) = 1 έπεται ότι το 1 γράφεται σαν γραμμικός συνδυασμός των a και b.

($\Leftarrow$) Αν το 1 γράφεται σαν γραμμικός συνδυασμός των a,b τότε ο ΜΚΔ(a, b) θα διαιρεί το 1, δηλαδή ΜΚΔ(a, b) = 1.

(2.8) Λήμμα Αν $p \in R$ ανάγωγο (δεν έχει γνήσια ανάλυση) και p δεν διαιρεί το $\alpha \in R$ τότε p και α είναι πρώτοι μεταξύ τους (ΜΚΔ(α,p)=1).

Απόδειξη: Αν d κοινός παράγοντας των p και α, δηλαδή $d \mid p \wedge d \mid a$, τότε επειδή $d \mid p$ έχουμε ότι υπάρχει $\beta \in R$ τέτοιο ώστε $p = d\beta$. Επειδή p ανάγωγο το d είναι συνεταιρικό του p ή μονάδα του R. Επειδή με τη σειρά του το p δεν διαιρεί το α κανένα συνεταιρικό του p δεν διαιρεί το α (διότι αλλιώς p|α). Τελικά, το d είναι κατ' ανάγκη μονάδα του R. Επομένως ΜΚΔ(α,p)=μονάδα του R δηλαδή ΜΚΔ(α,p)=1.

(2.9) Λήμμα Έστω $a \in R$, $p \in R$ όπου p ανάγωγο στοιχείο του R και $p \nmid a$. Τότε υπάρχουν $s, t \in R$ τέτοια ώστε $ps + at = 1$.

Απόδειξη: Από το λήμμα (2.8) έπεται ότι ΜΚΔ(p, a)=1 οπότε από το λήμμα (2.7) υπάρχουν $s, t \in R$ τέτοια ώστε $ps + at = 1$.

(2.10) Λήμμα Αν p ανάγωγο στοιχείο του R, $a, b \in R$ και $p \mid ab$ τότε $p \mid a$ ή $p \mid b$.

Απόδειξη:
Αν $p \mid a$ τελειώσαμε.
Αν $p \nmid a$ τότε από το λήμμα (2.9) έπεται ότι υπάρχουν $s, t \in R$ τέτοια ώστε ps + at = 1.
Τότε $p(bs) + (ab)t = 1 \cdot b = b$.
Οπότε $\left.\begin{matrix} p \mid p(bs) \\ p \mid ab \end{matrix}\right\} \Rightarrow p \mid p(bs) + ab \Rightarrow p \mid b.$

(2.11) Λήμμα Αν $a, b \in R$ και ο a είναι γνήσιος διαιρέτης του b τότε $g(a) < g(b)$.

Απόδειξη

Έστω b = ac
Επειδή a γνήσιος διαιρέτης του b έχουμε ότι $c \notin E(R)$.
Επειδή R Ευκλείδεια περιοχή έχουμε ότι υπάρχουν $q, r \in R$ τέτοια ώστε a = bq+r με r = 0 είτε $g(r) < g(b)$. Αν r = 0 θα είχαμε ότι $b \mid a$ άτοπο. Συνεπώς r = a – bq = a – qac = a(1–qc).
$c \notin E(R) \Rightarrow qc \neq 1$. Επομένως $g(r) = g(a)g(1 - qc) \geq g(a)$.
$\left.\begin{matrix} g(r) \geq g(a) \\ g(r) < g(b) \end{matrix}\right\} \Rightarrow g(a) < g(b)$.

(2.12) Ορισμός Μια ακέραια περιοχή R θα λέγεται **δακτύλιος μονοσήμαντης ανάλυσης** (ή **περιοχή μονοσήμαντης ανάλυσης**) αν

(i) Κάθε $b \in R$, $b \notin E(R)$ έχει μια ανάλυση σε γινόμενο ανάγωγων στοιχείων $b = p_1 p_2 \ldots p_s$, όπου p_i ανάγωγα

(ii) Αν $b = q_1 q_2 \ldots q_r$, όπου q_i ανάγωγα, τότε s = r και, με κατάλληλη αλλαγή των δεικτών, $q_i = p_i \varepsilon_i$ $(\varepsilon_i \in E(R))$ $\forall i, 1 \leq i \leq s$.

(2.13) Θεώρημα Κάθε Ευκλείδειος δακτύλιος είναι **δακτύλιος με μονοσήμαντη ανάλυση.**

Απόδειξη Επαγωγικά ως προς το g(b).

Αν b ανάγωγο τότε b = b
Αν b όχι ανάγωγο τότε b = ac όπου a και c γνήσιοι διαιρέτες του b.
Από το λήμμα (2.11) έχουμε ότι $g(a) < g(b)$
$g(c) < g(b)$

Λόγω της υπόθεσης της μαθηματικής επαγωγής τα a και c αναλύονται σε γινόμενο ανάγωγων στοιχείων. Έστω $\begin{cases} a = p_1 p_2 \dots p_j \text{ όπου } p_i = \text{ανάγωγα } (1 \le i \le j) \\ b = p_{j+1} p_{j+2} \dots p_r \text{ όπου } p_i = \text{ανάγωγα } (j+1 \le i \le r) \end{cases}$

Τότε $b = ac = p_1 p_2 \dots p_j p_{j+1} \dots p_r$ όπου $p_i = \text{ανάγωγα } (1 \le i \le r)$ (αποδείξαμε την (i)).

Έστω $b = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ δύο αναλύσεις του b σε γινόμενο ανάγωγων.
Έχουμε ότι $p_1 \mid b = q_1 q_2 \dots q_s$. Οπότε λόγω του λήμματος (2.10): Υπάρχει q_i τ.ω. $p_1 \mid q_i$.
Χωρίς περιορισμό της γενικότητας υποθέτουμε ότι $p_1 \mid q_1$. Επομένως υπάρχει $\varepsilon_1 \in R$ τέτοιο ώστε $q_1 = p_1 \varepsilon_1$. Επειδή q_1 ανάγωγο έπεται ότι $\varepsilon_1 \in E(R)$ (διότι p_1 ανάγωγο $\Rightarrow p_1 \notin E(R)$).

Οπότε q_1 και p_1 συνεταιρικά. Το b λοιπόν γράφεται $b = p_1 p_2 \dots p_r = \varepsilon_1 p_1 q_2 \dots q_s$. Δηλαδή
$$p_2 \dots p_r = q_2' q_3 \dots q_s \quad (1) \text{ όπου } q_2' = \varepsilon_1 q_2 .$$

Η έκφραση (1) είναι η ανάλυση του στοιχείου $b' = \dfrac{b}{p_1}$ του R σε γινόμενο ανάγωγων κατά δυο «διαφορετικούς» τρόπους. Το b' είναι γνήσιος διαιρέτης του b επομένως $g(b') < g(b)$. Από την υπόθεση της μαθηματικής επαγωγής έχουμε ότι r-1 = s-1 ή r = s και p_i συνεταιρικά των q_i για i = 2,3,…, r.

(2.14) Παρατήρηση Δεν είναι όλες οι ακέραιες περιοχές, περιοχές μονοσήμαντης ανάλυσης. Για παράδειγμα η ακέραια περιοχή $\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in Z\}$ δεν είναι περιοχή μονοσήμαντης ανάλυσης αφού $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ είναι δύο γνήσιες αναλύσεις του 6 σε γινόμενο αναγώγων.

Κεφάλαιο 3

Κατασκευή σωμάτων μέσω ευκλείδειων περιοχών

Ας πάρουμε R = **Z** και p ένα πρώτο αριθμό. Δείξαμε στο κεφάλαιο 0 ότι μέσω της ισοδυναμίας a, b $\in$ **Z,** $a \equiv b \pmod p :\Leftrightarrow p \mid a - b$ φτιάχνουμε το σώμα με p στοιχεία, το οποίο συμβολίσαμε με $\mathbf{Z}_p$ ή $\mathbf{F}_p$.

Εντελώς ανάλογα, αν R ευκλείδεια περιοχή και p ανάγωγο στοιχείο αυτής φτιάχνουμε ένα σώμα, το σώμα των κλάσεων υπολοίπων mod p του R.

(3.1) Ορισμός Έστω $m \in R$ όχι κατ' ανάγκη ανάγωγο. Δυο στοιχεία a, b $\in$ R θα λέγονται **ισοδύναμα** mod m (συμβολίζονται: $a \underset{m}{\sim} b$ ή $a \sim b$ ή $a \equiv b \bmod m$) όταν $m \mid a - b$.

Αποδεικνύεται, ακριβώς όπως και στο **Z**, ότι αυτή είναι μια σχέση ισοδυναμίας επομένως ο R διαμερίζεται σε κλάσεις ισοδυναμίας mod m. Αν a $\in$ R η κλάση ισοδυναμίας του a είναι το σύνολο $\{b \in R \mid b \sim a\} = \{b \in R \mid b \equiv a \bmod m\}$.
Άλλοι συμβολισμοί: $[a] = \bar{a} = K_a = a \bmod m$.

Στο σύνολο των κλάσεων mod m του R ορίζουμε τις πράξεις:

$$[a] \oplus [b] = [a + b] \text{ και } [a] \otimes [b] = [a \cdot b].$$

Θα πρέπει οι πράξεις να είναι καλά ορισμένες δηλαδή ανεξάρτητες των αντιπροσώπων των κλάσεων. Αυτό σημαίνει ότι, αν $a \sim a' \left([a] = [a']\right)$ και $b \sim b' \left([b] = [b']\right)$ τότε $[a + b] = [a' + b']$ και $[a \cdot b] = [a' \cdot b']$.
Για την πρόσθεση αυτό θα πει ότι $a + b \equiv a' + b' \pmod m$ το οποίο ισχύει διότι $m \mid (a + b) - (a' + b') = (a - a') + (b - b')$ αφού $m \mid (a - a') \wedge m \mid (b - b')$ (το τελευταίο διότι $a \sim a' \wedge b \sim b'$)

Ανάλογα αποδεικνύουμε ότι και ο πολλαπλασιασμός είναι καλά ορισμένος.

(3.2) Πρόταση: Το σύνολο των κλάσεων υπολοίπων mod m αποτελεί αντιμεταθετικό δακτύλιο με μοναδιαίο ως προς τις πράξεις $\oplus$ και $\otimes$. Ο δακτύλιος αυτός θα συμβολίζεται R_m ή R/m.

Απόδειξη:

(i) Η πρόσθεση $\oplus$ είναι καλά ορισμένη.
(ii) Ισχύει ο προσεταιρισμός ως προς την πρόσθεση αφού για κάθε a, b, c $\in$ R ισχύει ότι

$$([a] \oplus [b]) \oplus [c] = [a + b] \oplus [c] = [(a + b) + c] \overset{(1)}{=} [a + (b + c)] = [a] \oplus [b + c] = [a] \oplus ([b] \oplus [c])$$

Στη θέση (1) χρησιμοποιήσαμε τον προσεταιρισμό του δακτυλίου R.

(iii) Η κλάση [0] είναι ουδέτερο στοιχείο διότι για κάθε $[a] \in R_m$ ισχύει ότι

$$[0] \oplus [a]=[0+a]=[a]$$
$$[\alpha] \oplus [0]=[a+0]=[a]$$

(iv) Για κάθε $a \in R$ υπάρχει η αντίθετη κλάση του [a] η ποία είναι η [–a] διότι

$$[\alpha] \oplus [-a]=[a+(-a)]=[0]$$

(v) Ισχύει η αντιμεταθετικότητα της πρόσθεσης αφού για κάθε a, b $\in$ R ισχύει ότι

$$[a] \oplus [b] = [a + b] = [b + a] = [b] \oplus [a]$$

Ομοίως ως προς τον πολλαπλασιασμό:

(vi) Ο πολλαπλασιασμός $\otimes$ είναι καλά ορισμένος.
(vii) Ισχύει ο προσεταιρισμός του πολλαπλασιασμού αφού για κάθε a, b ,c $\in$ R ισχύει ότι

$$([a] \otimes [b]) \otimes [c] = [a \cdot b] \otimes [c] = [(a \cdot b) \cdot c] \overset{(2)}{=} [a \cdot (b \cdot c)] = [a] \otimes [b \cdot c] = [a] \otimes ([b] \otimes [c])$$

Η ισότητα (2) ισχύει, λόγω προσεταιρισμού του πολλαπλασιασμού στον δακτύλιο R.

(viii) Ισχύει ο επιμερισμός του πολλαπλασιασμού ως προς την πρόσθεση (τόσο από τα δεξιά όσο και από τα αριστερά)
(ix) Η κλάση [1] είναι μοναδιαίο στοιχείο διότι για κάθε a $\in$ R ισχύει ότι

$$[1] \otimes [a]=[1a]=[a]$$
$$[a] \otimes [1]=[a1]=[a]$$

(x) Ισχύει η αντιμεταθετικότητα του πολλαπλασιασμού αφού για κάθε a, b $\in$ R ισχύει ότι

$$[a] \otimes [b] = [a \cdot b] = [b \cdot a] = [b] \otimes [a]$$

Ενδιαφερόμαστε να γνωρίζουμε πότε ο $(R/m, \oplus, \otimes)$ είναι <u>σώμα</u>.

Θα πρέπει να ελέγξουμε για κάθε $[a] \neq [0]$ την ύπαρξη αντιστρόφου, δηλαδή την ύπαρξη κάποιας κλάσης [b] (b $\in$ R) τέτοιας ώστε [a] $\otimes$ [b] = [1].

Αυτή η κλάση <u>δεν</u> υπάρχει πάντα. Για παράδειγμα αν πάρουμε R = **Z** και m = 4 έχουμε ότι η κλάση [2] <u>δεν</u> έχει αντίστροφο γιατί:

$$[2][1]=[2]$$
$$[2][2]=[0]$$
$$[2][3]=[2]$$

(Θα μπορούσαμε να πούμε ότι αφού [2][2]=[0] έχουμε ότι [2] διαιρέτης του μηδενός, δηλαδή διαιρέτης της κλάσης του 0, άρα δεν έχει αντίστροφο).

Θα αποδείξουμε όμως ότι

(3.3) Θεώρημα Αν R ευκλείδεια περιοχή και p ανάγωγο (≡πρώτο) στοιχείο του R τότε το R/p είναι σώμα.

Απόδειξη:

Έστω $[a] \neq [0]$, $a \in R$. Θα αποδείξουμε ότι υπάρχει $b \in R$ τέτοιο ώστε $[a] \otimes [b] = [1]$.
Κατ' αρχήν $[a] \neq [0]$ θα πει ότι $p \nmid a$.
Από το λήμμα (2.9) έπεται ότι υπάρχουν $b, t \in R$ τέτοια ώστε $ab + pt = 1$.
Οπότε $ab \equiv 1 \pmod p$. Δηλαδή $[ab] = [1]$ ή $[a] \otimes [b] = [1]$

□

(3.4) Παραδείγματα

(1) Έστω R = **Z** και p = 13
Σύμφωνα με το Θεώρημα (3.3) ο δακτύλιος **Z**/13 είναι σώμα.
Θα βρούμε τον αντίστροφο του [6].
Εφαρμόζουμε τον αλγόριθμο του Ευκλείδη.

$13 = 2 \cdot 6 + 1$
$1 = 13 + 6 \cdot (-2)$

Επομένως $[1] = [13] + [6][-2]$ δηλαδή $b = -2$, $[b] = [11]$.

(2) Έστω R = **Z** και p = 29
Σύμφωνα με το Θεώρημα (3.3) ο δακτύλιος **Z**/29 είναι σώμα.
Θα βρούμε τα αντίστροφα των κλάσεων [5], [13], [18].
Για το [5]:
$29 = 5 \cdot 5 + 4$
$5 = 1 \cdot 4 + 1$
$1 = 5 - 4$
$1 = 5 - (29 - 5 \cdot 5) = -29 + 6 \cdot 5$

Επομένως $[5]^{-1} = [6]$

Ανάλογα, με τον αλγόριθμο του Ευκλείδη βρίσκουμε ότι

$[13]^{-1} = [9]$
$[18]^{-1} = [21]$

(3) Αν R = **Z** και p οποιοσδήποτε πρώτος αριθμός τότε το R/p είναι σώμα.

Επομένως υπάρχουν άπειρα στο πλήθος πεπερασμένα σώματα διότι έχουμε άπειρο πλήθος πρώτων. Εδώ το R/p θα το συμβολίζουμε $\mathbf{F}_p$ ή GF(p). Αργότερα θα αποδείξουμε την ύπαρξη κι άλλων πεπερασμένων σωμάτων πέραν των $\mathbf{F}_p$.

(4) Έστω R = R[X] ο δακτύλιος των πολυωνύμων μιας μεταβλητής με συντελεστές πραγματικούς αριθμούς.
Αφού R σώμα έπεται ότι R ευκλείδειος δακτύλιος.
Το $p(X) = X^2 + 1 \in R[X] = R$ είναι ανάγωγο στοιχείο του R.
Επομένως ο δακτύλιος R[X]/p(X) είναι σώμα. Μπορεί να αποδειχθεί ότι το σώμα αυτό είναι ισόμορφο προς το σώμα των μιγαδικών αριθμών.

(3.4) Δυο πολυώνυμα f(X), g(X) ∈ R[X] είναι ισοδύναμα modulo p(X) (δηλαδή $p(X)\big|\big(f(X)-g(X)\big)$) όταν και μόνο όταν τα υπόλοιπα των διαιρέσεων των f(X) και g(X) με το p(X) , έστω $r_1(X)$, $r_2(X)$, είναι ίσα.

Απόδειξη:

$(\Leftarrow)$ Έστω $f(X) = p(X)\pi_1(X) + r(X)$ και $g(X) = p(X)\pi_2(X) + r(X)$ με r(X) = 0 ή $\deg r(x) < \deg p(x)$. Τότε $f(X) - g(X) = p(X)(\pi_1(X) - \pi_2(X))$. Οπότε $p(X)\big|\big(f(X)-g(X)\big)$

$(\Rightarrow)$ Αν $p(X)\ \big|\big(f(X)-g(X)\big)$ και $f(X) = p(X)\pi_1(X) + r_1(X)$ και $g(X) = p(X)\pi_2(X) + r_2(X)$ τότε $p(X)\big|\ \big(p(X)\pi_1(X) + r_1(X) - p(X)\pi_2(X) - r_2(X)\big)$

Επομένως, $p(X)\big|\ \big(p(X)\big(\pi_1(X)-\pi_2(X)\big)+\big(r_1(X)-r_2(X)\big)\big)$ ή αλλιώς $p(X)\ \big|\big(r_1(X)-r_2(X)\big)$

Αν $r_1(x) - r_2(X) \neq 0$ θα είχαμε ότι $\deg(r_1 - r_2) < \deg p$ άτοπο,

(αφού το p διαιρεί το $r_1 - r_2$).

Συνεπώς, κατ' ανάγκη $r_1(X) = r_2(X)$.

□

Επομένως ένα σύνολο αντιπροσώπων των κλάσεων [f(X)] στον δακτύλιο R = R[X]/p(X) είναι τα πολυώνυμα της μορφής aX + b όπου a, b ∈ R.

Η απεικόνιση

$$\varphi : \big(R[X]/p(X),\oplus,\otimes\big) \to \big(C,+,\cdot\big)$$

$$ax + b \mapsto ai + b$$

αποδεικνύεται ότι είναι ισομορφισμός σωμάτων δηλαδή $R[X]/p(X) \cong C$.

Ένα πολυώνυμο $f(X) \in R[X]$, βαθμού degf = 2, έστω $f(X) = AX^2 + BX + C$, είναι ανάγωγο αν και μόνο αν $\Delta = B^2 - 4AC < 0$. Αν λοιπόν πάρουμε το πολυώνυμο f(X)

ξαναφτιάχνουμε το σώμα R[X]/f(X) αλλά όπως και για το $p(X) = X^2 + 1 \in R[X]$ αποδεικνύεται ότι αυτό είναι πάλι ισόμορφο με το C, δηλαδή τίποτα καινούριο δεν προέκυψε.

Αυτό είναι γνωστό σαν το Θεμελιώδες Θεώρημα της Άλγεβρας το οποίο διατυπώνεται ως εξής: Στο δακτύλιο C[X] κάθε πολυώνυμο αναλύεται σε γινόμενο γραμμικών παραγόντων δηλαδή στον C[X] τα μόνα ανάγωγα στοιχεία είναι τα πολυώνυμα πρώτου βαθμού.

$AX - B$ ή $X - \frac{A}{B}$, δηλαδή τα πολυώνυμα της μορφής $X - a$ όπου $a \in C$.

Άμεση συνέπεια του θεωρήματος αυτού είναι ότι τα ανάγωγα στοιχεία του δακτυλίου R[X] είναι τα πολυώνυμα πρώτου βαθμού και εκείνα από τα πολυώνυμα δεύτερου βαθμού που έχουν διακρίνουσα αρνητική.

Στη συνέχεια θα προσπαθήσουμε να κατασκευάσουμε σώματα παίρνοντας τον δακτύλιο $\mathbf{F}_p[X]$ όπου δηλαδή οι συντελεστές του πολυωνύμου θα είναι στοιχεία του πεπερασμένου σώματος $\mathbf{F}_p$ (όπου p οποιοσδήποτε πρώτος) και όχι πραγματικοί αριθμοί.

Ας δούμε τον αλγόριθμο της διαίρεσης δυο πολυωνύμων, μέσω ενός παραδείγματος.

Θεωρούμε στον δακτύλιο $\mathbf{F}_{13}[X]$ τα πολυώνυμα:

$\alpha(X) = X^8 + X^6 + 10X^4 + 10X^3 + 8X^2 + 2X + 8$ και $b(X) = 3X^6 + 5X^4 + 9X^2 + 4X + 8$.

Ζητούνται πολυώνυμα q(X) και r(X) (στον $\mathbf{F}_{13}[X]$) για τα οποία: $\alpha(X) = q(X)b(X) + r(X)$ με $r(X)=0$ ή $\deg r(X) < \deg b(X)$.

$X^8+X^6+10X^4+10X^3+8X^2+2X+8$	$3X^6+5X^4+9X^2+4X+8$
$-X^8-6X^6-3X^4-10X^3-7X^2$	$9X^2 + 7$
$8X^6+7X^4+X^2+2X+8$	
$-8X^6-9X^4-11X^2-2X-4$	
$11X^4+3X^2+4$	

Ας μελετήσουμε, κατ' αρχήν, ένα παράδειγμα κατασκευής του σώματος $\frac{F_p[X]}{q(X)}$ όπου q(X) ανάγωγο στοιχείο του $\mathbf{F}_p[X]$ ($p \in P$).

Έστω $p = 2$ και $q(X) = X^3 + X + 1$.

Το q(X) είναι ανάγωγο $\mathbf{F}_2[X]$ διότι αν δεν ήταν ανάγωγο θα είχε (επειδή $\deg q(X)=3$) στη παραγοντοποίησή του σε ανάγωγους παράγοντες τουλάχιστον ένα γραμμικό παράγοντα (παράγοντα πρώτου βαθμού) δηλαδή θα είχε τουλάχιστον μια ρίζα στο $\mathbf{F}_2=\{0,1\}$. Δεν έχει όμως καμία ρίζα στο $\mathbf{F}_2$ αφού ισχύει ότι $q(0) = 0 + 0 + 1 = 1 \neq 0$ και $q(1) = 1 + 1 + 1 = 1 \neq 0$.

Μπορούμε να φτιάξουμε το σώμα $\frac{F_2[X]}{q(X)}$. Ταυτίζουμε τα στοιχεία του με τα υπόλοιπα της διαίρεσης των πολυωνύμων του $\mathbf{F}_2[X]$ με q(X). Δηλαδή εδώ ένα πλήρες σύστημα αντιπροσώπων κλάσεων αποτελούν τα πολυώνυμα $aX^2 + bX + c \mid a, b, c \in \mathbf{F}_2$. Υπάρχουν ακριβώς 8 τέτοια πολυώνυμα πράγμα που σημαίνει ότι το $\frac{F_2[X]}{q(X)}$ είναι σώμα με 8 ($=2^3$) στοιχεία.

Οι πράξεις στο σώμα $\frac{F_2[X]}{q(X)}$:

Το πολυώνυμο $a_2X^2 + a_1X + a_0$ το γράφουμε και $[a_2, a_1, a_0]$.

- **Η πρόσθεση**.

$(a_2X^2 + a_1X + a_0) + (b_2X^2 + b_1X + b_0) = (a_2+b_2)X^2+(a_1+b_1)X+(a_0+b_0)$

Δηλαδή $[a_2, a_1, a_0]+[b_2, b_1, b_0]=[a_2 + b_2, a_1 + b_1, a_0 + b_0]$.

(Όπου + η πρόσθεση στο $\mathbf{F}_2$).

- **Ο πολλαπλασιασμός**.

Πολλαπλασιάζουμε κατ' αρχήν τα πολυώνυμα:

$(a_2X^2 + a_1X + a_0)(b_2X^2 + b_1X + b_0) = a_2b_2X^4 + (a_2b_1+a_1b_2)X^3 + (a_2b_0+a_1b_1+a_0b_2)X^2 + (a_1b_0+ a_0b_1)X + a_0b_0$

Στη συνέχεια εκφράζουμε τις δυνάμεις που είναι μεγαλύτερες του 2 σαν γραμμικό συνδυασμό μικρότερων δυνάμεων, modulo q(X).

Έχουμε ότι $X^3 \equiv X + 1 \bmod(X^3 +X +1)$ οπότε $X^4 \equiv X^2 + X \bmod(X^3 +X +1)$.

(Τα πρόσημα δεν παίζουν σημασία γιατί βρισκόμαστε στο σώμα $\mathbf{F}_2$).

Άρα $a_2b_2X^4 \equiv a_2b_2(X^2 + X) \equiv a_2b_2X^2 + a_2b_2X \mod q(X)$ και

$(a_2b_1 + a_1b_2)X^3 \equiv (a_2b_1 + a_1b_2)(X + 1) \equiv (a_2b_1 + a_1b_2)X + (a_2b_1 + a_1b_2) \mod q(X)$

Επομένως $[a_2, a_1, a_0][b_2, b_1, b_0] = [c_2, c_1, c_0]$ όπου

$c_2 = a_2b_0 + a_1b_1 + a_0b_2 + a_2b_2$

$c_1 = a_1b_0 + a_0b_1 + a_2b_2 + a_2b_1 + a_1b_2$

$c_0 = a_0b_0 + a_2b_1 + a_1b_2$

Για να κάνουμε πιο εύκολο τον πολλαπλασιασμό, σχηματίζουμε ένα πίνακα των δυνάμεων του $X \bmod q(X)$.

$$X^0 \equiv 1$$
$$X^1 \equiv X$$
$$X^2 \equiv X^2$$
$$X^3 \equiv X + 1$$
$$X^4 \equiv X^2 + X$$
$$X^5 \equiv X^3 + X^2 \equiv X^2 + X + 1$$

$$X^6 \equiv X^3 + X^2 + X \equiv (X+1) + X^2 + X \equiv X^2 + 1$$
$$X^7 \equiv X^3 + X \equiv X + 1 + X \equiv 1$$

Παρατηρούμε ότι η ακολουθία των πολυωνύμων (δυνάμεις του X) είναι περιοδική με περίοδο 7.

Ας συμβολίσουμε την κλάση του X mod q(X) με α, α=[0,1,0].

Έχουμε λοιπόν τον ακόλουθο πίνακα για τις δυνάμεις του α:

$$\alpha^0 \equiv 1$$
$$\alpha^1 \equiv \alpha$$
$$\alpha^2 \equiv \alpha^2$$
$$\alpha^3 \equiv \alpha + 1$$
$$\alpha^4 \equiv \alpha^2 + \alpha$$
$$\alpha^5 \equiv \alpha^2 + \alpha + 1$$
$$\alpha^6 \equiv \alpha^2 + 1$$
$$\alpha^7 \equiv 1$$

Με $GF(8) = \{1, \alpha, \alpha^2, \ldots, \alpha^6, 0\}$ θα συμβολίσουμε το σώμα με 8 στοιχεία. Επομένως η πολλαπλασιαστική ομάδα του σώματος GF(8) είναι κυκλική (τάξης 7).

Χρησιμοποιούμε το α σαν βάση των «λογαρίθμων». Συμφωνούμε να χρησιμοποιούμε το συμβολισμό: $\log_\alpha(\beta) = k \Leftrightarrow \alpha^k = \beta$ και φτιάχνουμε τους ακόλουθους πίνακες:

k	$\boldsymbol{\alpha^k}$
*	000
0	001
1	010
2	100
3	011
4	110
5	111
6	101

β	$\boldsymbol{\log_\alpha \beta}$
000	*
001	0
010	1
011	3
100	2
101	6
110	4
111	5

Στο δεύτερο πίνακα η διάταξη των στοιχείων β είναι σύμφωνα με το δυϊκό σύστημα.

(3.5) Παραδείγματα:

1) Υποθέτουμε ότι θέλουμε να πολλαπλασιάσουμε a = [110] και b = [111] (Δηλαδή θέλουμε να υπολογίσουμε το γινόμενο ab = [110][111]).

Βρίσκουμε τους αντίστοιχους «λογάριθμους»:

$\log_\alpha(a) = \log_\alpha([110]) = 4$ δηλαδή $a = \alpha^4$

$\log_\alpha(b) = \log_\alpha([111]) = 5$ δηλαδή $b = \alpha^5$

Επομένως $ab = \alpha^4\,\alpha^5 = \alpha^9 = \alpha^2 = [100]$

2) Το ίδιο για a = [111] και b = [011]

Έχουμε ότι:

$\log_\alpha(a) = \log_\alpha([111]) = 5$ δηλαδή $a = \alpha^5$

$\log_\alpha(b) = \log_\alpha([011]) = 3$ δηλαδή $b = \alpha^3$

Επομένως $ab = \alpha^5\,\alpha^3 = \alpha^8 = \alpha = [010]$

Ας πάρουμε πάλι το δακτύλιο $\mathbf{F}_2[X]$ και το πολυώνυμο $q(X) := X^4 + X + 1 \in \mathbf{F}_2[X]$

Κατ' αρχήν επειδή $q(0) = 0 + 0 + 1 = 1 \neq 0$ και $q(1) = 1 + 1 + 1 = 1 \neq 0$ το q(X) δεν έχει ρίζα στο $\mathbf{F}_2 = \{0, 1\}$. Δηλαδή, αν το q(X) αναλύεται (σε γινόμενο ανάγωγων πολυωνύμων), δεν εμφανίζεται παράγοντας πρώτου βαθμού στην ανάλυσή του.

Δυνατοί τύποι ανάλυσης ως προς τον βαθμό των παραγόντων είναι: (1, 1, 1, 1), (2, 1, 1), (3, 1), (2, 2). Επομένως μας μένει να ελέγξουμε αν το q(X) αναλύεται σε γινόμενο δυο παραγόντων βαθμού 2 ο καθένας.

Από τη σχέση $q(X) = (a_2X^2 + a_1X + a_0)(b_2X^2 + b_1X + b_0)$ με αντικατάσταση έχουμε ότι

$$X^4 + X + 1 = a_2b_2X^4 + (a_2b_1 + a_1b_2)X^3 + (a_2b_0 + a_1b_1 + a_0b_2)X^2 + (a_1b_0 + a_0b_1)X + a_0b_0$$

Δηλαδή πρέπει:

$$\begin{cases} a_2b_2 = 1 \\ a_2b_1 + a_1b_2 = 0 \\ a_2b_0 + a_1b_1 + a_0b_2 = 0 \\ a_1b_0 + a_0b_1 = 1 \\ a_0b_0 = 1 \end{cases}$$

Εύκολα διαπιστώνουμε ότι το παραπάνω σύστημα <u>δεν</u> έχει λύση στο σώμα $\mathbf{F}_2$. Επομένως το q(X) είναι ανάγωγο και το $\frac{F_2[X]}{q(X)}$ είναι σώμα με 16 ($= 2^4$) στοιχεία.

Κεφάλαιο 4

Τάξη πεπερασμένου σώματος

Κύριος σκοπός των επόμενων δύο κεφαλαίων είναι η απόδειξη της ύπαρξης ανάγωγου πολυωνύμου q(X) βαθμού n, για κάθε φυσικό αριθμό n στο δακτύλιο $\mathbf{F}_p[X]$, όπου $\mathbf{F}_p$ το πεπερασμένο σώμα με p στοιχεία και p οποιοσδήποτε πρώτος αριθμός. Δηλαδή η απόδειξη της ύπαρξης (και αργότερα και της μοναδικότητας) ενός σώματος με p^n στοιχεία για κάθε πρώτο p και για κάθε φυσικό n.

(4.1) Θεώρημα Αν F πεπερασμένο σώμα με q στοιχεία τότε $q = p^n$ για κάποιο πρώτο p και κάποιο φυσικό n.

(Δηλαδή δεν υπάρχουν σώματα πεπερασμένα τάξεως n όταν ο n διαιρείται με περισσότερους από έναν πρώτους αριθμούς).

Απόδειξη Με 1 θα συμβολίζουμε το μοναδιαίο στοιχείο του πεπερασμένου σώματος F. Ορίζουμε την ακολουθία $\{u_0,u_1,u_2,\ldots\}$ με $u_0 = 0$, $u_n = u_{n-1} + 1$ $\quad n = 1, 2, 3, \ldots$
Από τον ορισμό της ακολουθίας (κάνοντας επαγωγή ως προς m) προκύπτει ότι

$$\begin{cases} u_{m+n} = u_m + u_n & (1) \\ u_{m\cdot n} = u_m \cdot u_n & (2) \end{cases}$$

Επειδή το σώμα F είναι πεπερασμένο έπεται ότι δεν είναι δυνατόν όλα τα u_m να είναι διαφορετικά μεταξύ τους, και συνεπώς υπάρχουν στοιχεία που συμπίπτουν (επαναλαμβάνονται). Έστω $u_k = u_{k+c}$ η πρώτη επανάληψη.
Δηλαδή τα $u_0,u_1,u_2,\ldots,u_{k+c-1}$ είναι διακεκριμένα μεταξύ τους. Τότε:

$$\left.\begin{array}{l} u_k = u_{k+c} \\ (1) \Rightarrow u_{k+c} - u_k = u_c \end{array}\right\} \Rightarrow u_c = 0$$

Δηλαδή το πρώτο στοιχείο που θα επαναληφθεί θα είναι το μηδέν. Επομένως $\{u_0,u_1,u_2, \ldots,u_{c-1}\}$ είναι όλοι διακεκριμένοι μεταξύ τους.

(4.2) Ορισμός Ο ακέραιος c, ο οποίος θα είναι κατ' ανάγκην μεγαλύτερος ή ίσος του 2, θα λέγεται **χαρακτηριστική του σώματος** F.

Για παράδειγμα έστω το σώμα $\mathbf{F}_2$ τότε $u_0 = 0$. Τότε έχουμε ότι $u_1 = u_0 + 1 = 0 + 1 = 1$ και $u_2 = u_1 + 1 = 1 + 1 = 0$. Επομένως η χαρακτηριστική του σώματος $\mathbf{F}_2$ είναι 2.

(4.3) Παρατήρηση Η χαρακτηριστική πεπερασμένου σώματος είναι κατ' ανάγκη πρώτος αριθμός.

Πράγματι αν $c = ab$ με $1 < a < c$ και $1 < b < c$ τότε από την (2) θα είχαμε ότι $u_c = u_a u_b$
Αλλά όπως δείξαμε $u_c = 0$ ενώ $u_a \neq 0$ και $u_b \neq 0$ το οποίο είναι άτοπο.
Επομένως c = p για κάποιο πρώτο αριθμό p.

Το $\{u_0,u_1,u_2,\ldots,u_{p-1}\}$ είναι υποσύνολο του F και υπόσωμα του F, αφού είναι κλειστό ως προς τις πράξεις + και · λόγω των (1) και (2). Μάλιστα το σύνολο $\{u_0,u_1,u_2,\ldots, u_{p-1}\}$ είναι ισόμορφο με το σώμα $\mathbf{F}_p=\{0,1,2,\ldots,p-1\}$ μέσω της απεικόνισης $u_i \leftrightarrow i \quad (i = 0,1,2,\ldots,p-1)$ και συνεπώς $\mathbf{F}_p \subseteq F$.

Μπορούμε να δούμε το F σαν $\mathbf{F}_p$-δ.χ. δηλαδή σαν διανυσματικό χώρο πάνω από το σώμα $\mathbf{F}_p$.

Έστω m η διάσταση του F και $\{\omega_1,\omega_2,\ldots,\omega_m\}$ μια $\mathbf{F}_p$-βάση του F. Τότε κάθε $a \in F$ μπορεί να γραφεί σαν $a = a_1\omega_1 + a_2\omega_2 + \ldots a_m\omega_m$ όπου $a_i \in \mathbf{F}_p$.

Επομένως $\#F = p^m$.

Η πρόσθεση στο F είναι απλή και γίνεται κατά συνιστώσες.

Θα μελετήσουμε την πολλαπλασιαστική δομή του F.

Θα δούμε ιδιαίτερα ότι η πολλαπλασιαστική ομάδα $(F^*,\cdot)$, όπου $F^* = F \setminus (0)$, του F είναι κυκλική τάξης $q - 1$.

(4.4) Πρόταση Αν $\alpha \in F^*$ τάξης $\text{ord}(\alpha) = t$, τότε $t \mid (q-1)$.

Απόδειξη: Εφαρμόζουμε το θεώρημα του Lagrange στην ομάδα $(F^*,\cdot)$, όπου $F^* = F \setminus (0)$.

(4.5) Λήμμα Αν $p(X)$ πολυώνυμο βαθμού m με συντελεστές από ένα σώμα F, $p(X) \in F[X]$, τότε η εξίσωση $p(X) = 0$ έχει το πολύ m διακεκριμένες λύσεις στο F.

Απόδειξη Θα εφαρμόσουμε τη μέθοδο της μαθηματικής επαγωγής ως προς το βαθμό m του πολυωνύμου $p(X)$.

Αν m=1 τότε το $p(X)$ είναι της μορφής $p(X) = \alpha X+b$ οπότε η εξίσωση $p(X)=0$ έχει ακριβώς μια λύση στο F την $x = -\frac{b}{a}$.
Αν $m \geq 2$ και η $p(X) = 0$ δεν έχει λύση στο F τελειώσαμε.

Αν η εξίσωση $p(X) = 0$ έχει τουλάχιστο μια λύση στο F , έστω $\alpha \in F$, τότε $p(\alpha) = 0$ οπότε το πολυώνυμο $p(X)$ γράφεται στη μορφή $p(X) = (X-\alpha)q(X)$ όπου $q(X) \in F[x]$.

Αν τώρα $\beta \neq \alpha$ μια οποιαδήποτε λύση της $p(X) = 0$, τότε $p(\beta) = 0$. Τότε όμως έχουμε ότι $(\beta - \alpha)q(\beta) = 0$ και επειδή $\beta \neq \alpha$ έπεται ότι $q(\beta) = 0$. Είδαμε ότι κάθε άλλη ρίζα του $p(X)$ είναι και ρίζα του $q(X)$. Όμως $\deg q(X) = m - 1 < m$.
Η υπόθεση της μαθηματικής επαγωγής δίνει ότι το $q(X)$ έχει το πολύ $m - 1$ ρίζες στο F. Το $p(X)$ έχει τις ρίζες στο F τις ρίζες του $q(X)$ και την ρίζα $x = \alpha$. Δηλαδή έχει το πολύ $(m-1) + m = m$ ρίζες.

□

Προσοχή Η εξίσωση δεύτερου βαθμού $X^2 - 1 = 0$ στο $\mathbf{Z}_8$ έχει 4 λύσεις. Τις $x = 1, 3, 5, 7$ αφού:

$1^2 - 1 = 1 - 1 = 0,$
$3^2 - 1 = 9 - 1 = 8 = 0,$
$5^2 - 1 = 25 - 1 = 1 - 1 = 0,$
$7^2 - 1 = (-1)^2 - 1 = 1 - 1 = 0$

Αυτό δεν έρχεται σε αντίθεση με το λήμμα (4.5) διότι το $\mathbf{Z}_8$ δεν είναι σώμα.

Αν τώρα $\alpha \in F$, ord(α) = t τότε τα στοιχεία του συνόλου $\{1,\alpha,\ldots,\alpha^{t-1}\}$ είναι λύσεις της εξίσωσης $X^t - 1 = 0$. Σύμφωνα με το λήμμα (4.5) η εξίσωση $X^t - 1 = 0$ δεν έχει άλλες λύσεις. Αυτό σημαίνει ότι αν $b \in F$ και $b^t = 1$ τότε $b = \alpha^\lambda$ για κάποιο $\lambda = 0, 1, \ldots, t-1$

(4.6) Λήμμα Αν ord(α) = t τότε $\text{ord}(a^i) = \dfrac{t}{\text{ΜΚΔ}(i,t)}$

Απόδειξη: Έστω m η τάξη του α^i. Τότε επειδή $(\alpha^i)^t = (\alpha^t)^i = 1^i = 1$ θα πρέπει το m να διαιρεί το it. Ο ΜΚΔ(i, t) γράφεται σαν γραμμικός συνδυασμός των i και t. δηλαδή υπάρχουν u, v ακέραιοι τέτοιοι ώστε ΜΚΔ(i, t) = ut + vi. Αφού ο ΜΚΔ(i, t) διαιρεί τα i και t μπορούμε να γράψουμε $1 = u\dfrac{t}{\text{ΜΚΔ}(i,t)} + v\dfrac{i}{\text{ΜΚΔ}(i,t)}$. Οι $\dfrac{t}{\text{ΜΚΔ}(i,t)}$ και $\dfrac{i}{\text{ΜΚΔ}(i,t)}$ είναι ακέραιοι και όπως φαίνεται από την τελευταία ισότητα πρώτοι μεταξύ τους. Επομένως, ο $\dfrac{t}{\text{ΜΚΔ}(i,t)}$ διαιρεί το it δηλαδή τον m. Δηλαδή, $m = \dfrac{t}{\text{ΜΚΔ}(i,t)}$.

(4.7) Παράδειγμα Έστω $\alpha \in F$ ($\alpha \neq 0$) και ord(α) = 12.
Σχηματίζουμε τις δυνάμεις α^i (i=0,1,2,…,11). (t = 12)

i	**ΜΚΔ(i,12)**	**ord(α^i)**
0	12	1
1	1	12
2	2	6
3	3	4
4	4	3
5	1	12
6	6	2
7	1	12
8	4	3
9	3	4
10	2	6
11	1	12

Παρατηρούμε ότι απ' τις δυνάμεις του α τελικά υπάρχουν 4 που έχουν τάξη 12. Το αποτέλεσμα αυτό μπορούμε να το δούμε υπολογίζοντας τη συνάρτηση φ του Euler.

Γενικά αν $n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$ τότε $\varphi(n) = n \cdot (1-\frac{1}{p_1}) \cdot (1-\frac{1}{p_2}) \cdot \dots \cdot (1-\frac{1}{p_s})$.

π.χ. για $n = 12 = 2^3\, 3$ έχουμε ότι $\varphi(12) = 12 \cdot (1-\frac{1}{2}) \cdot (1-\frac{1}{3}) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = \frac{24}{6} = 4$.

Ειδικά αν $n = p \in \mathbf{P}$ τότε $\varphi(p) = p \cdot (1-\frac{1}{p}) = p - 1$.

(4.8) Πρόταση

Έστω t φυσικός και F πεπερασμένο σώμα.
Στο F είτε δεν υπάρχει στοιχείο τάξης t είτε υπάρχουν ακριβώς φ(t) στοιχεία τάξης t.

Απόδειξη:

Αν δεν υπάρχει στο σώμα F στοιχείο τάξης t δεν έχουμε να αποδείξουμε τίποτα.

Αν υπάρχει ένα στοιχείο $\alpha \in F$ με $\mathrm{ord}(\alpha) = t$ τότε κάθε άλλο στοιχείο που έχει τάξη t περιέχεται στο σύνολο $\{1, \alpha, \dots, \alpha^{t-1}\}$, λόγω του λήμματος (4.5).

Από το λήμμα (4.6) έχουμε ότι $t = \mathrm{ord}(\alpha^i) = \frac{t}{\mathrm{ΜΚΔ}(i,t)}$. Επομένως $\mathrm{ΜΚΔ}(i, t) = 1$.

Δηλαδή υπάρχουν ακριβώς φ(t) τέτοια i (από τον ορισμό της συνάρτησης φ).

Συνδυάζοντας τώρα τις προτάσεις (4.4) και (4.8) βλέπουμε ότι αν F είναι ένα πεπερασμένο σώμα με $\#F = q$ στοιχεία τότε για κάθε t

(I) Αν $t \nmid q - 1$ τότε δεν υπάρχει $\alpha \in F$ με $\mathrm{ord}(\alpha) = t$

(II) Αν $t \mid q - 1$ τότε είτε δεν υπάρχει στοιχείο $\alpha \in F$ τάξης t
είτε υπάρχουν ακριβώς φ(t) στοιχεία του F τάξης t

Εμείς θα αποδείξουμε ότι αν $t \mid q - 1$ τότε υπάρχουν πάντοτε ακριβώς φ(t) στοιχεία του F τάξης t.

(4.9) Παράδειγμα Έστω q = 16. Τότε $q - 1 = 16 - 1 = 15$. Τα t για τα οποία $t \mid (q - 1)$ ή αλλιώς $t \mid 15$ είναι τα t = 1, 3, 5, 15. Βρίσκουμε τα αντίστοιχα φ(t):

t	**φ(t)**
1	1
3	2
5	4
15	8

Το πλήθος αυτών τον στοιχείων είναι 1 + 2 + 4 + 8 = 15 δηλαδή ίσο με q – 1. Επομένως για t θα πρέπει να υπάρχουν ακριβώς φ(t) στοιχεία του σώματος F τάξης t. Το αποτέλεσμα αυτό είναι γενικό και είναι άμεση συνέπεια του παρακάτω θεωρήματος:

(4.10) Θεώρημα Έστω $n \in \mathbf{N}$ τότε $\sum_{d \mid n} \varphi(d) = n$.

Απόδειξη: Η απόδειξη έχει γίνει στο μάθημα Θεωρία Αριθμών Ι.

Συνδυάζοντας τώρα την πρόταση (4.4), την πρόταση (4.8) και το θεώρημα (4.1) έχουμε το:

(4.11) Θεώρημα Έστω F πεπερασμένο σώμα με q στοιχεία και $t \in \mathbb{N}$.

(i) Αν $t \nmid q-1$ τότε δεν υπάρχει $\alpha \in F$ με $\text{ord}(\alpha) = t$
(ii) Αν $t \mid q-1$ τότε υπάρχουν ακριβώς $\varphi(t)$ στοιχεία του F τάξης t

Απόδειξη:
Το (i) είναι άμεση συνέπεια της πρότασης (4.8).
Για το (ii): Έστω $t \mid q-1$ και έστω $\psi(t)$ το πλήθος των στοιχείων του F που έχουν τάξη t. Σύμφωνα με το θεώρημα του Lagrange κάθε μη-μηδενικό στοιχείο του F έχει σαν τάξη κάποιο t όπου $t \mid q-1$. $\sum_{t|q-1} \psi(t) = q-1$.

Αλλά από το θεώρημα (4.10) έχουμε ότι $\sum_{t|q-1} \varphi(t) = q-1$.

Επομένως $\sum_{t|q-1} \varphi(t) = \sum_{t|q-1} \psi(t)$

ή $\sum_{t|q-1} \varphi(t) - \sum_{t|q-1} \psi(t) = 0$

ή $\sum_{t|q-1} \left(\varphi(t) - \psi(t)\right) = 0$

Αλλά από την πρόταση (4.8) έχουμε ότι $\varphi(t) - \psi(\tau) \geq 0$ για κάθε t το οποίο διαιρεί το $q-1$ (αφού $\psi(t)$ είναι ίσο με $\varphi(t)$ ή με μηδέν).

Οπότε κατ' ανάγκην $\psi(t) = \varphi(t)$ για κάθε $t \mid q-1$, δηλαδή το θεώρημα.

□

(4.12) Πόρισμα Αν F πεπερασμένο σώμα με q στοιχεία τότε υπάρχει τουλάχιστον ένα στοιχείο τάξης $q-1$. (Υπάρχουν μάλιστα $\varphi(q-1)$ τέτοια στοιχεία).
Δηλαδή η ομάδα $\left(F^*,\cdot\right)$ είναι πάντα κυκλική.

(4.13) Ορισμός Κάθε γεννήτορας της ομάδας $\left(F^*,\cdot\right)$ θα λέγεται **πρωταρχική ρίζα** του σώματος F.

(4.14) Παράδειγμα Έστω $F = \mathbf{F}_7 = \{0,1,2,3,4,5,6\}$. Θα βρούμε μια πρωταρχική ρίζα του σώματος F.

Παίρνουμε τις δυνάμεις του 2:

$$2^0 = 1$$
$$2^1 = 2$$
$$2^2 = 4$$
$$2^3 = 1$$

Άρα $\text{ord}(2)=3$ και το 2 δεν είναι πρωταρχική ρίζα του F.

Παίρνουμε τις δυνάμεις του 3:

$$3^0 = 1$$
$$3^1 = 3$$
$$3^2 = 2$$
$$3^3 = 6$$

Άρα από Θ. Lagrange ord(3) = 6 και το 3 είναι πρωταρχική ρίζα του σώματος F = $\mathbf{F}_7$.

Είδαμε ένα παράδειγμα υπολογισμού των πρωταρχικών ριζών ενός σώματος με τη μέθοδο της δοκιμής και της επιτυχίας.

Αν το πεπερασμένο σώμα F είναι μεγάλο τότε τα πράγματα είναι δύσκολα. Υπάρχει ένας αλγόριθμος του Gauβ που μας δίνει στοιχεία του F, $\alpha_1,\alpha_2,\ldots,\alpha_\kappa$ τέτοια ώστε: $\text{ord}(\alpha_1) < \text{ord}(\alpha_2) < \ldots < \text{ord}(\alpha_\kappa) = q - 1$. Μάλιστα ισχύει, $\text{ord}(\alpha_i) | \text{ord}(\alpha_{i+1})$ για κάθε i = 1, 2, …, k – 1.

(4.15) Αλγόριθμος του Gauβ

G1. Έστω i = 1 και $\alpha_1 \in$ F με $\text{ord}(\alpha_1) = t_1$.
G2. Αν $t_i = q - 1$ τελειώσαμε. Το α_i είναι μια πρωταρχική ρίζα.
G3. Αν $\text{ord}(\alpha_i) < q - 1$ επιλέγω μη-μηδενικό στοιχείο του F, έστω β, τέτοιο ώστε $\beta \neq \alpha_i^{\lambda}$ για κάθε λ (το β να μην είναι δύναμη του α_i). Έστω ord(β) = s. Αν s = q – 1 θέτουμε $\alpha_{i+1} = \beta$ και τελειώσαμε.
G4. Αλλιώς βρίσκουμε d | t_i και e | s τέτοια ώστε ΜΚΔ(d, e) = 1 και $d \cdot e = \text{ΕΚΠ}(t_i, s)$. Οπότε θέτουμε:
$\alpha_{i+1} = \alpha_i^{t_i/d}\beta^{s/e}$, $t_{i+1} = \text{ΕΚΠ}(t_i,s)$, $i \mapsto i + 1$ και πηγαίνουμε στο G2.

Αποδεικνύεται ότι d και e υπάρχουν πάντα.

Παρατήρηση
Στο προηγούμενο παράδειγμα ουσιαστικά εφαρμόσαμε τον αλγόριθμο του Gauβ και είχαμε $\alpha_1 = 2$, $t_1 = 3$ και $\beta = 3$, s = 6.
Δεν φτάσαμε ποτέ στο βήμα G4.

(4.16) Παράδειγμα Έστω F = $\mathbf{F}_{25}$ το πεπερασμένο σώμα με 25 στοιχεία. Θεωρούμε το πολυώνυμο $X^2 - 2 \in \mathbf{F}_5[X]$. Αυτό το πολυώνυμο είναι ανάγωγο ως προς το σώμα $\mathbf{F}_5$. Πράγματι, το $X^2 - 2$ δεν έχει ρίζα στο $\mathbf{F}_5 = \{0, 1, 2, 3= -2, 4= -1\}$ αφού
για x = 0 έχουμε $x^2 - 2 = 0 - 2 = -2 \neq 0$
για $x = \pm 1$ έχουμε $x^2 - 2 = 1 - 2 = -1 \neq 0$
για $x = \pm 2$ έχουμε $x^2 - 2 = 4 - 2 = 2 \neq 0$

Επομένως το F είναι ισόμορφο με $\dfrac{F_5[X]}{< X^2 - 2 >}$.

Το F είναι $\mathbf{F}_5$-δ.χ. διάστασης 2. Δηλαδή το F γράφεται $F = \{(\alpha, \beta) \mid \alpha, \beta \in \mathbf{F}_5\}$. Η πρόσθεση γίνεται φυσιολογικά κατά συνιστώσες:
$(\alpha_1, \beta_1) + (\alpha_2, \beta_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2)$

Για τον πολλαπλασιασμό το F γράφεται $F = \dfrac{F_5[X]}{< X^2 - 2 >} = \{\alpha X + \beta \mid \alpha, \beta \in \mathbf{F}_5\}$.

Έχουμε πολλαπλασιασμό πολυωνύμων:
$(\alpha_1 X + \beta_1)(\alpha_2 X + \beta_2) = \alpha_1\alpha_2 X^2 + (\alpha_1\beta_2 + \alpha_2\beta_1)X + \beta_1\beta_2$
Ισχύει ότι $X^2 - 2 \equiv 0 \bmod(X^2 - 2)$. Δηλαδή $X^2 \equiv 2 \bmod(X^2 - 2)$.
Άρα $(\alpha_1 X + \beta_1)(\alpha_2 X + \beta_2) = (\alpha_1\beta_2 + \alpha_2\beta_1)X + \beta_1\beta_2 + 2\,\alpha_1\alpha_2$
Άρα ο πολλαπλασιασμός στο F είναι: $(\alpha_1, \beta_1) \cdot (\alpha_2, \beta_2) = (\alpha_1\beta_2 + \alpha_2\beta_1, \beta_1\beta_2 + 2\,\alpha_1\alpha_2)$

Ξεκινάμε τον αλγόριθμο του Gauβ:

Έστω $\alpha_1 = (1,0)$. Με τη βοήθεια των κανόνων πρόσθεσης και πολλαπλασιασμού υπολογίζουμε μερικές δυνάμεις του α_1:

$\alpha_1^0 = (0,1)$
$\alpha_1^1 = (1,0)$
$\alpha_1^2 = \alpha_1\,\alpha_1 = (1,0)\,(1,0) = (1\cdot 0 + 1\cdot 0,\ 0\cdot 0 + 2\cdot 1\cdot 1) = (0,2)$
$\alpha_1^3 = \alpha_1^2\,\alpha_1 = (0,2)\,(1,0) = (0\cdot 0 + 1\cdot 2,\ 2\cdot 0 + 2\cdot 0\cdot 1) = (2,0)$
$\alpha_1^4 = \alpha_1^3\,\alpha_1 = (2,0)\,(1,0) = (2\cdot 0 + 1\cdot 0, 0\cdot 0 + 2\cdot 2\cdot 1) = (0,4)$

Με αυτό τον τρόπο κατασκευάζουμε τον παρακάτω πίνακα δυνάμεων του α_1:

i	$\boldsymbol{\alpha_1^i}$
0	(0,1)
1	(1,0)
2	(0,2)
3	(2,0)
4	(0,4)
5	(4,0)
6	(0,3)
7	(3,0)
8	(0,1)

Για το α_1^8 έχουμε: $\alpha_1^8 = \alpha_1^7\,\alpha_1 = (3,0)\,(1,0) = (3\cdot 0 + 1\cdot 0,\ 0\cdot 0 + 2\cdot 3\cdot 1) = (0,1)$
Επομένως $\text{ord}(\alpha_1) = 8$. Άρα $t_1 = 8 \neq q - 1 = 24$.
Το α δεν είναι πρωταρχική ρίζα.

Εφαρμόζουμε το βήμα G3.
Διαλέγουμε $\beta \in F$, $\beta \neq \alpha_1^i$ $(i = 0, 1, 2, \ldots, 7)$.

Έστω $\beta = (1,1)$. Υπολογίζουμε τις δυνάμεις του β:

i	$\boldsymbol{\beta^i}$
0	(0,1)
1	(1,1)
2	(2,3)
3	(0,2)
4	(2,2)
5	(4,1)
6	(0,4)
7	(4,4)
8	(3,2)

9	(0,3)
10	(3,3)
11	(1,4)
12	(0,1)

Επομένως το β=(1,1) έχει τάξη 12 (ord(β) = 12). Άρα $s = 12 \neq q - 1 = 24$.
Άρα πάλι δεν έχουμε βρει πρωταρχική ρίζα.

Εφαρμόζουμε το βήμα G4.
Ψάχνουμε d, e με $d \mid t_1 = 8$ και $e \mid s = 12$ τέτοια ώστε ΜΚΔ(d, e) = 1 και $d \cdot e =$ ΕΚΠ(t_1, s) = ΕΚΠ(8, 12) = 24.
Παίρνουμε d = 8 και e = 3
Σύμφωνα με το βήμα G4 παίρνουμε $\alpha_2 = \alpha_1^{t_1/d} \cdot \beta^{s/e}$. Δηλαδή $\alpha_2 = \alpha_1^{8/8} \cdot \beta^{12/3}$
ή $\alpha_2 = \alpha_1\beta^4$.
Από τον πίνακα των δυνάμεων του β έχουμε ότι $\beta^4 = (2,2) = 2\alpha_1 + 2$
Από τον πίνακα των δυνάμεων του α_1 έχουμε $\alpha_1^2 = (0,2) = 2$
Οπότε $\alpha_2 = \alpha_1 (2\alpha_1 + 2) = 2\alpha_1^2 + 2\alpha_1 = 2\alpha_1 + 4$

Τώρα χρησιμοποιούμε το γνωστό από τη Θεωρία Ομάδων

(4.17) Λήμμα: Αν ord(α) = m, ord(β) = n, (m, n) = 1 και α, β αντιμετατίθενται τότε $\text{ord}(\alpha\beta) = m \cdot n$

Στο παράδειγμά μας $\text{ord}(\alpha_1) = 8$, $\text{ord}(\beta^4) = \frac{12}{(4,12)} = \frac{12}{4} = 3$, οπότε $\text{ord}(\alpha_2) = \text{ord}(\alpha_1 \cdot \beta^4) = 8 \cdot 3 = 24$.

Επομένως το $\alpha_2 = 2\alpha_1 + 4$ είναι μια πρωταρχική ρίζα του $\mathbf{F}_{25}$.

Ας αφήσουμε για λίγο τις πρωταρχικές ρίζες και ας έρθουμε στην έννοια του ελάχιστου (ανάγωγου) πολυωνύμου.

Αν F πεπερασμένο σώμα τότε $\#F = p^m$ για κάποιο πρώτο p και κάποιο φυσικό m. Το F μπορεί να θεωρηθεί σαν $\mathbf{F}_p$-δ.χ. με διάσταση $\dim_{F_p} F = m$.

Έστω τώρα $\alpha \in F$.

Παίρνουμε τις δυνάμεις του α: $1, \alpha, \alpha^2, \ldots, \alpha^m$
Τα στοιχεία αυτά του F έχουν πλήθος m + 1.
Επειδή $\dim_{F_p} F = m < m + 1$ έχουμε ότι τα $1, \alpha, \alpha^2, \ldots, \alpha^m$ είναι $\mathbf{F}_p$-γραμμικά εξαρτημένα. Δηλαδή υπάρχουν στοιχεία $A_0, A_1, A_2, \ldots, A_m$ του $\mathbf{F}_p$ όχι όλα μηδέν τέτοια ώστε $A_0 + A_1\alpha + A_2\alpha^2 + \ldots + A_m\alpha^m = 0$.
Επομένως το α είναι ρίζα του πολυωνύμου $A(X) = A_0 + A_1X + A_2X^2 + \ldots + A_mX^m$
Το α μπορεί να είναι ρίζα κι άλλων πολυωνύμων. Έστω, $S(\alpha) = \{f(X) \in \mathbf{F}_p[X] \mid f(\alpha) = 0\}$ το σύνολο όλων των πολυωνύμων του $\mathbf{F}_p[X]$ που έχουν ρίζα το α. Επειδή $A(X) \in S(\alpha)$, το $S(\alpha)$ είναι μη κενό και αναγκαστικά περιέχει ένα πολυώνυμο βαθμού μικρότερου ή ίσου του m.

Έστω P(X) ένα μη-μηδενικό πολυώνυμο του $S(\alpha)$ ελάχιστου βαθμού.
Αν $f(X) \in S(\alpha)$ τότε υπάρχουν κάποια πολυώνυμα $q(X), r(X) \in \mathbf{F}_p[X]$ τέτοια ώστε $f(X) = P(X)q(X) + r(X)$ όπου $r(X) = 0$ ή $\deg r(X) < \deg P(X)$.

Αν $r(X) \neq 0$ θα είχαμε ότι deg r(X) < deg P(X) και ακόμα $f(\alpha) = P(\alpha)q(\alpha) + r(\alpha)$ και επειδή $f(\alpha) = P(\alpha) = 0$ (τα υποθέσαμε στοιχεία του συνόλου S(α)) τότε θα είχαμε $r(\alpha) = 0$, άτοπο αφού εμείς υποθέσαμε ότι P(X) είναι το πολυώνυμο ελάχιστου βαθμού με αυτή την ιδιότητα.
Συνεπώς r(X) = 0 και επομένως f(X) = P(X)q(X). Δηλαδή P(X)|f(X) (στο $\mathbf{F}_p[x]$).
Αποδείξαμε ότι P(X) | f(X) για κάθε $f(X) \in S(\alpha)$.

(4.18) Ορισμός Το P(X) θα λέγεται **ελάχιστο πολυώνυμο του α** ως προς το σώμα $\mathbf{F}_p$.

Συνήθως θα παίρνουμε το P(X) σαν μονικό (monic) δηλαδή με συντελεστή της μεγαλύτερης δύναμης του x το 1. Οπότε το P(X) θα είναι μονοσήμαντα ορισμένο. Δηλαδή $F \ni a \mapsto P(X) \in \mathbf{F}_p[X]$

Παρατήρηση: Το P(X) είναι ανάγωγο στο $\mathbf{F}_p[X]$.

Απόδειξη: Αν P(X) = A(X)B(X) με degA(X) < degP(X) και degB(X) < degP(X) τότε P(α) = A(α)B(α). Δηλαδή A(α)B(α) = 0. Οπότε A(α) = 0 ή B(α) = 0.

Δηλαδή το α θα ήταν ρίζα μη μηδενικού πολυωνύμου (του A ή του B) βαθμού μικρότερου του degP(X). Άτοπο. Επομένως P(X) ανάγωγο στο $\mathbf{F}_p[x]$.

□

Έχουμε ήδη αποδείξει το

(4.19) Θεώρημα: Αν F ένα σώμα με $q = p^m$ στοιχεία τότε σε κάθε στοιχείο α του F αντιστοιχεί μονοσήμαντα ένα πολυώνυμο (τα ελάχιστο πολυώνυμο του α) με τις εξής ιδιότητες:

(a) $P(\alpha) = 0$
(b) $\deg P(X) \leq m$
(c) Αν $f(X) \in \mathbf{F}_p[X]$ με $f(\alpha) = 0$ τότε P(X) | f(X).

(4.20) Ορισμός Το πολυώνυμο αυτό P(X) λέγεται **ελάχιστο πολυώνυμο του α** ως προς το υπόσωμα $\mathbf{F}_p$ του F.

Ας γυρίσουμε τώρα πάλι πίσω στο παράδειγμα για το $\mathbf{F}_{25}$.
Θα υπολογίσουμε το ελάχιστο πολυώνυμο για μερικά στοιχεία του $\mathbf{F}_{25}$.

Ας πάρουμε το στοιχείο (1,0) = α και ας πάρουμε τις δυνάμεις του α.
- $\alpha^0 = 1$ Το ελάχιστο πολυώνυμο είναι το X – 1.
- Ας πάρουμε τώρα το α. (Φυσικά αν το α άνηκε στο $\mathbf{F}_5$, το ελάχιστο πολυώνυμο του α θα ήταν το X – α). Το $\alpha \notin \mathbf{F}_5$ οπότε το X – α δεν μας κάνει διότι ένας συντελεστής, ο –α, δεν ανήκει στο $\mathbf{F}_5$.

Παίρνουμε τα στοιχεία $\alpha^0 = 1$, α, α^2 τα οποία τα θεωρούμε σαν 3 διανύσματα του 2-διάστατου διανυσματικού χώρου $\mathbf{F}_{25}$ ως προς το $\mathbf{F}_5$. Επομένως θα είναι γραμμικά εξαρτημένα κάτι το οποίο μας δίνει ένα πολυώνυμο $2^{ου}$ βαθμού που έχει σαν ρίζα το α. Ας βρούμε αυτό το πολυώνυμο. 1 = (0,1), α = (1,0), α^2 = (0,2) (το υπολογίσαμε προηγουμένως). Προφανώς $\alpha^2 - 2 \cdot 1 = 0$. Επομένως το ελάχιστο πολυώνυμο του α είναι το $X^2 - 2$. Είναι, δηλαδή, αυτό μέσω του οποίου ορίστηκε το σώμα $\mathbf{F}_{25}$ σαν $\frac{F_5[X]}{< X^2 - 2 >}$. Αυτό δεν είναι τυχαίο.

Ας ξαναθυμηθούμε των πίνακα τον δυνάμεων του α.

i	**α^i**	**ελάχιστο πολυώνυμο**
0	(0,1)	$X-1$
1	(1,0)	X^2-2
2	(0,2)	$X-2$
3	(2,0)	X^2-3
4	(0,4)	$X-4$
5	(4,0)	X^2-2
6	(0,3)	$X-3$
7	(3,0)	X^2-3

Ας προσπαθήσουμε τώρα να βρούμε το ελάχιστο πολυώνυμο της πρωταρχικής ρίζας $\beta = 2\alpha + 4$ του $\mathbf{F}_{25}$.
Έχουμε ότι:
$\beta^0 = 1 = (0,1)$
$\beta = 2\alpha + 4 = 2(1,0) + 4(0,1) = (2,4)$
$\beta^2 = \beta \cdot \beta = (2,4) \cdot (2,4) = (2\cdot 4 + 2\cdot 4, 4\cdot 4 + 2\cdot 2\cdot 2) = (16,14) = (1,4)$
Πρέπει να εκφράσουμε το β^2 σαν γραμμικό συνδυασμό των β και $\beta^0 = 1$ με συντελεστές από το σώμα $\mathbf{F}_5$.
Παρατηρούμε ότι $2\beta^2 - \beta = (2,3) - (2,4) = (0,4)$
ή $2\beta^2 - \beta = 4 \cdot 1$ ή $\beta^2 - 3\beta = 2 \cdot 1$ ή $\beta^2 + 2\beta + 3 = 0$

Συνεπώς το β έχει ελάχιστο πολυώνυμο το $X^2 + 2X + 3$. Το πολυώνυμο αυτό είναι <u>ανάγωγο</u> (δες παρατήρηση σελίδας 32). Θα μπορούσαμε να είχαμε χρησιμοποιήσει αυτό για την κατασκευή του $\mathbf{F}_{25}$ αντί του $X^2 - 2$. Τότε το $\alpha = (1,0)$ θα ήταν <u>πρωταρχική ρίζα</u>. Αυτό θα ήταν πολύ πιο βολικό για την παράσταση του σώματος F.

Στη συνέχεια θα μελετήσουμε συστηματικά το ελάχιστο πολυώνυμο κάτι το οποίο θα μας επιτρέψει να κατανοήσουμε μερικά από τα «μυστήρια» του προηγούμενου παραδείγματος.

Έστω F πεπερασμένο σώμα και K υπόσωμα του F. (Το K μπορεί να είναι το F_p ή κάποιο μεγαλύτερό του). Το K θα είναι κι αυτό πεπερασμένο. Έστω ότι $\#K = q = p^m$. Όπως και προηγουμένως το F μπορεί να θεωρηθεί σαν K-δ.χ. Προφανώς η $\dim_K F$ (διάσταση του F ως προς τον διανυσματικό χώρο K) είναι πεπερασμένη. Έστω n η διάσταση. Τότε $\#F = q^n = p^{nm}$.

Έστω $\alpha \in F$.

(4.21) <u>Ορισμός</u> Το <u>ελάχιστο πολυώνυμο</u> P(X) του α ως προς το σώμα K είναι το μοναδικό μονικό πολυώνυμο με τις εξής ιδιότητες:
(a) $P(\alpha) = 0$
(b) $\deg P(X) \le n$
(c) Αν $f(X) \in K[X]$ με $f(\alpha) = 0$ τότε $P(X) \mid f(X)$ στο $K[X]$.

Θα προσπαθήσουμε να έχουμε μια πιο σαφή εικόνα για το P(X).
Θα χρειαστούμε μερικά λήμματα.

(4.20) Λήμμα Το στοιχείο β του σώματος F ανήκει στο K τότε και μόνο τότε όταν $\beta^q = \beta$.

Ιδιαίτερα, όλα τα στοιχεία του K επαληθεύουν την εξίσωση $X^q - X = 0$.

Απόδειξη Έστω $\beta \in K$.

Αν $\beta = 0$ έχουμε ότι $\beta^q = \beta$

Αν $\beta \neq 0$ τότε έστω $t := \text{ord}(\beta)$ οπότε $t \mid (q-1)$. Θα υπάρχει επομένως ένας ακέραιος λ τέτοιος ώστε $q - 1 = t\lambda$. Επομένως $\beta^{q-1} = (\beta^t)^\lambda = 1^\lambda = 1$ και συνεπώς $\beta^q = \beta$.
Τα q στοιχεία του K είναι οι q διακεκριμένες ρίζες του πολυωνύμου $X^q - X$.
Είχαμε δει όμως ότι το $X^q - X$ έχει το πολύ q διακεκριμένες ρίζες. Οπότε δεν υπάρχουν άλλες λύσεις πέραν των στοιχείων του K.

□

(4.23) Λήμμα Αν p πρώτος τότε ο $\binom{p}{k}$ όπου $1 \le k \le p-1$ διαιρείται από το p.

Απόδειξη

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{(p-k)!(p-k+1)(p-k+2)\ldots p}{(p-k)!k!} = \frac{(p-k+1)(p-k+2)\ldots p}{1\cdot 2\cdot \ldots \cdot k}$$

Έστω $\binom{p}{k} = \lambda$ τότε $(p-k+1)(p-k+2)\ldots p = \lambda \cdot 1\cdot 2\cdot \ldots \cdot (k-1)\cdot k$

Έχουμε ότι $p \mid (p-k+1)(p-k+2)\ldots p$ οπότε το p διαιρεί το $\lambda \cdot 1\cdot 2\cdot \ldots \cdot (k-1)\cdot k$ και επειδή $1 \le k \le p-1$ θα πρέπει το p να διαιρεί το λ. Δηλαδή $p \mid \binom{p}{k}$.

□

(4.24) Λήμμα Αν F πεπερασμένο (ή άπειρο) σώμα χαρακτηριστικής p (chF = p) και $\alpha_1, \alpha_2, \ldots, \alpha_t$ στοιχεία του F τότε $(\alpha_1 + \alpha_2 + \ldots + \alpha_t)^{p^\lambda} = \alpha_1^{p^\lambda} + \alpha_2^{p^\lambda} + \ldots + \alpha_t^{p^\lambda}$ για κάθε $\lambda = 1, 2, 3, \ldots$

Απόδειξη Το αποδεικνύουμε για t = 2 και συνεχίζουμε επαγωγικά. Για την απόδειξη με t = 2, χρησιμοποιούμε το διωνυμικό τύπο, και εφαρμόζουμε το λήμμα (4.23).

□

Αν λοιπόν τώρα $\alpha \in F$ και p(X) το ελάχιστο πολυώνυμο του α ως προς το K και $f(X) = f_0 + f_1X + \ldots + f_dX^d \in K[X]$ τέτοιο ώστε $f(\alpha) = 0$ τότε

$$f_0 + f_1\alpha + \ldots + f_d\alpha^d = 0 \quad (1)$$

(με $f_i \in K$ για κάθε i) άρα και $f(\alpha^q) = 0$, διότι αν υψώσουμε την (1) στην q-δύναμη θα έχουμε $\left(\sum_{k=0}^{d} f_k\alpha^k\right)^q = 0$. Οπότε σύμφωνα με το λήμμα (4.24) παίρνουμε $\sum_{k=0}^{d} f_k^d\alpha^{kd} = 0$ ή $f(\alpha^q) = 0$. Επομένως α^q επίσης ρίζα του f(X).

Δηλαδή αν α ρίζα του f(X) τότε και $\alpha^q, \alpha^{q^2}, \alpha^{q^3}, \ldots$ επίσης ρίζες του f(X). Αυτές λέγονται συζυγή του α ως προς το σώμα K. Η ακολουθία $\alpha^q, \alpha^{q^2}, \alpha^{q^3}, \ldots$ έχει πεπερασμένο πλήθος διακεκριμένων μεταξύ τους στοιχείων. Υποθέτουμε $\alpha \neq 0$. Έστω

d ο ελάχιστος θετικός ακέραιος για τον οποίο υπάρχει j με $0 \le j < d$.και $\alpha^{q^d} = \alpha^{q^j}$
Τότε $1 = \alpha^{q^d - q^j} = \alpha^{q^j}(\alpha^{q^{d-j}-1})$.
Επομένως, $\text{ord}(\alpha) \mid q^j (q^{d-j} - 1)$. (2)
Απ' την άλλη μεριά $\alpha \in F^*$ και $\#F^* = q^n - 1$ οπότε $\text{ord}(\alpha) \mid q^n - 1$ και συνεπώς $\text{ΜΚΔ}(\text{ord}(\alpha), q^j) = 1$, οπότε λόγω της (2), έχουμε $\text{ord}(\alpha) \mid (q^{d-j} - 1)$ ή $\alpha^{q^{d-j}} = \alpha$. Το d όμως είναι ο εκθέτης της πρώτης επανάληψης. Συνεπώς θα πρέπει $j = 0$ οπότε $\alpha^{q^d} = \alpha$. Όμως $\alpha \in F$ και $\#F = q^n$ το οποίο σύμφωνα με το λήμμα (4.22) μας δίνει $\alpha^{q^n} = \alpha$. Στη συνέχεια εφαρμόζουμε το <u>πόρισμα</u> (1.12), δηλαδή ότι

$$\text{ΜΚΔ}(X^{q^n} - X, X^{q^d} - X) = X^{q^{\text{ΜΚΔ}(n,d)}} - X$$

Επομένως $\alpha^{q^{\text{ΜΚΔ}(n,d)}} = \alpha$. Αυτό όμως είναι σε κάθε περίπτωση <u>άτοπο</u>, διότι υποθέσαμε ότι α^{q^d} είναι η <u>πρώτη</u> επανάληψη της ακολουθίας $\alpha, \alpha^q, \alpha^{q^2}, \alpha^{q^3}, \ldots$, εκτός αν $\text{ΜΚΔ}(n, d) = d$. Δηλαδή πρέπει το d να διαιρεί το n.

<u>Συμπέρασμα</u> Το πλήθος των διακεκριμένων συζυγών του α είναι ένας διαιρέτης d του n.

(4.25) <u>Ορισμός</u> Το d αυτό θα λέγεται **βαθμός** του α.

Έχουμε δει ότι είναι ο ελάχιστος θετικός ακέραιος τέτοιος ώστε $q^d \equiv 1 \pmod t$ όπου $t = \text{ord}(\alpha)$.

Δηλαδή αποδείξαμε το
(4.26) <u>Θεώρημα</u> Το πλήθος των (διακεκριμένων) συζυγών του α, έστω d, είναι ένας διαιρέτης του n. Ο d είναι ο ελάχιστος θετικός ακέραιος που ικανοποιεί την

$$t = \text{ord}(\alpha) \mid q^d - 1 .$$

Ακόμα, αν $\lambda = \mu d + r$ όπου $0 \le r \le d - 1$ τότε $\alpha^{q^\lambda} = \alpha^{q^r}$.

<u>Απόδειξη</u> $\alpha^{q^\lambda} = \alpha^{q^{\mu d + r}} = \left(\alpha^{q^d}\right)^\mu \alpha^{q^r} = \alpha^{q^r}$

Το ελάχιστο πολυώνυμο του α θα πρέπει να έχει τουλάχιστον d ρίζες. Συγκεκριμένα αποδείξαμε ότι μαζί με το α και οι δυνάμεις $\alpha^q, \alpha^{q^2}, \alpha^{q^3}, \ldots$ είναι επίσης ρίζες.

Έστω $f_a(X) := (X - \alpha)(X - \alpha^q) \ldots (X - \alpha^{q^{d-1}})$ και P(X) το ελάχιστο πολυώνυμο του α ως προς το σώμα K.

Τότε το $f_\alpha(X)$ διαιρεί το P(X).

<u>Θα αποδείξουμε ότι</u> $f_\alpha(X) = P(X)$.

Γράφουμε $(X - \alpha)(X - \alpha^q) \ldots (X - \alpha^{q^{d-1}}) = A^d X^d + A_{d-1} X^{d-1} + \ldots + A_1 X + A_0$ όπου $A_i \in F$.
Υψώνουμε στην q-στη δύναμη εφαρμόζοντας ταυτόχρονα το λήμμα (4.24):

$$(X-\alpha)^q(X-\alpha^q)^q \ldots (X-\alpha^{q^{d-1}})^q = A_d^q X^{qd} + A_{d-1}^q X^{q(d-1)} + \ldots + A_1^q X^q + A_0^q \quad (3)$$

Από το λήμμα (4.24) (αν υποθέσουμε ότι $2 \nmid q$) προκύπτει ακόμα ότι

$$(X-\beta)^q = X^q + (-1)^q\beta^q = X^q - \beta^q .$$

Εύκολα διαπιστώνουμε ότι αυτό ισχύει και στην περίπτωση όπου το 2 διαιρεί το q.
Επομένως το αριστερό μέλος της (3) είναι ίσο με $= (X^q-\alpha^q)\ (X^q-\alpha^{q^2})\ldots(X^q-\alpha^{q^d})$
αλλά $\alpha^{q^d} = \alpha$ οπότε «αριστερό μέλος της (3)» = $f_\alpha(X^q)$.
Επειδή $f_\alpha(X) = \sum_{i=0}^{d} A_i X^i$ έχουμε ότι $f_a(X^q) = A_d X^{qd} + A_{d-1}X^{q(d-1)} + \ldots + A_1 X^q + A_0$.
Επομένως $A_d X^{qd} + A_{d-1}X^{q(d-1)} + \ldots + A_1 X^q + A_0 = f_a(X^q)$ = «αριστερό μέλος της (3)» = «δεξιό μέλος της (3)» = $A_d^q X^{qd} + A_{d-1}^q X^{q(d-1)} + \ldots + A_1^q X^q + A_0^q$.
Συνεπώς $A_i^q = A_i$ για κάθε i = 0, 1, 2, …, d – 1. Η τελευταία σχέση όμως για τα A_i είναι αυτή που χαρακτηρίζει τα στοιχεία του σώματος K, άρα $A_i \in K$ για κάθε i = 0, 1, 2, …, d – 1. Καταλήξαμε στο συμπέρασμα ότι $f_\alpha(X) \in K[X]$, και αποδείξαμε το ακόλουθο

(4.27) Θεώρημα Αν F πεπερασμένο σώμα με q^n στοιχεία και $K \subseteq F$ με q στοιχεία και $\alpha \in F$ τότε το **ελάχιστο πολυώνυμο του α ως προς το σώμα K** είναι το

$$f_\alpha(X) = (X-\alpha)(X-\alpha^q)\ldots(X-\alpha^{q^{d-1}}),$$

όπου d είναι ο ελάχιστος φυσικός τέτοιος ώστε $q^d \equiv 1 \pmod t$ και $t := \mathrm{ord}(\alpha)$.

(4.28) Παράδειγμα Για q = 2 και n = 4

$F = \mathbf{F}_{16}$
$\quad\quad |$
$K = \mathbf{F}_2 = \{0,1\}$

Το $X^4 + X + 1 \in \mathbf{F}_2[X]$ είναι ανάγωγο. Θα κατασκευάσουμε το σώμα με 16 ($= 2^4$) στοιχεία μέσω αυτού του πολυωνύμου δηλαδή θα κατασκευάσουμε το $\mathbf{F}_{16} = \dfrac{F_2[X]}{<X^4+X+1>}$. Ο $\mathbf{F}_{16}$ είναι $\mathbf{F}_2$-δ.χ. διάστασης 4.

Αν με α συμβολίσουμε το X (modulo $X^4 + X + 1$) τότε, σαν διάνυσμα, το α είναι το [0,0,1,0].

Τα στοιχεία του $\mathbf{F}_{16}$ θα αντιστοιχούν σε διατεταγμένες τετράδες [a,b,c,d] όπου τα a, b, c, d είναι οι συντελεστές του υπολοίπου της διαίρεσης με $X^4 + X + 1$, το υπόλοιπο δηλαδή θα είναι $aX^3 + bX^2 + cX + d$.

Υπολογίζουμε τις δυνάμεις του α:
$\alpha^2 \to X^2$ επομένως $\alpha^2 = [0, 1, 0, 0]$
$\alpha^3 \to X^3$ επομένως $\alpha^3 = [1, 0, 0, 0]$

$\alpha^4 \rightarrow X^4$ (modulo $X^4 + X + 1$) = $\alpha + 1$ επομένως $\alpha^4 = [0, 0, 1, 1]$
$\alpha^5 = \alpha^2 + \alpha$ επομένως $\alpha^5 = [0, 1, 1, 0]$
$\alpha^6 = \alpha^3 + \alpha^2$ επομένως $\alpha^6 = [1, 1, 0, 0]$
$\alpha^7 = \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1$ επομένως $\alpha^7 = [1, 0, 1, 1]$
$\alpha^8 = \alpha^4 + \alpha^2 + \alpha = \alpha^2 + 2\alpha + 1 = \alpha^2 + 1$ επομένως $\alpha^8 = [0, 1, 0, 1]$
$\alpha^9 = \alpha^3 + \alpha$ επομένως $\alpha^9 = [1, 0, 1, 0]$
$\alpha^{10} = \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1$ επομένως $\alpha^{10} = [0, 1, 1, 1]$
$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$ επομένως $\alpha^{11} = [1, 1, 1, 0]$
$\alpha^{12} = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1$ επομένως $\alpha^{12} = [1, 1, 1, 1]$
$\alpha^{13} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + 2\alpha + 1 = \alpha^3 + \alpha^2 + 1$ επομένως $\alpha^{13} = [1, 1, 0, 1]$
$\alpha^{14} = \alpha^4 + \alpha^3 + \alpha = \alpha^3 + 2\alpha + 1 = \alpha^3 + 1$ επομένως $\alpha^{14} = [1, 0, 0, 1]$
$\alpha^{15} = \alpha^4 + \alpha = 2\alpha + 1 = 1$ επομένως $\alpha^{15} = [0, 1, 0, 1]$

Κατασκευάζουμε τον παρακάτω πίνακα:

i	**α^i**	**ord(α^i)**	**deg(α)**	**ελάχιστο πολυώνυμο**
0	[0001]	1	1	$X + 1$
1	[0010]	15	4	$(X - \alpha)(X - \alpha^2)(X - \alpha^4)(X - \alpha^8)$
2	[0100]	15	4	$(X - \alpha)(X - \alpha^2)(X - \alpha^4)(X - \alpha^8)$
3	[1000]	5	4	$(X - \alpha^3)(X - \alpha^6)(X - \alpha^9)(X - \alpha^{12})$
4	[0011]	15	4	$(X - \alpha)(X - \alpha^2)(X - \alpha^4)(X - \alpha^8)$
5	[0110]	3	2	$(X - \alpha^5)(X - \alpha^{10})$
6	[1100]	5	4	$(X - \alpha^3)(X - \alpha^6)(X - \alpha^9)(X - \alpha^{12})$
7	[1011]	15	4	
8	[0101]	15	4	$(X - \alpha)(X - \alpha^2)(X - \alpha^4)(X - \alpha^8)$
9	[1010]	5	4	$(X - \alpha^3)(X - \alpha^6)(X - \alpha^9)(X - \alpha^{12})$
10	[0111]	3	2	$(X - \alpha^5)(X - \alpha^{10})$
11	[1110]	15	4	
12	[1111]	5	4	$(X - \alpha^3)(X - \alpha^6)(X - \alpha^9)(X - \alpha^{12})$
13	[1101]	15	4	
14	[1001]	15	4	
15	[0001]			

Θυμόμαστε ότι ο βαθμός του α^i είναι ο ελάχιστος φυσικός $d > 0$ τέτοιος ώστε $q^d \equiv 1 \pmod t$ όπου $t = \text{ord}(\alpha^i)$.
Εδώ για το α έχουμε $t = 15$ και $q = 2$ οπότε θέλουμε $2^d \equiv 1 \pmod{15}$. Δηλαδή $d = 4$.

Έχουμε ότι:
$(X - \alpha)(X - \alpha^2)(X - \alpha^4)(X - \alpha^8) = (X^2 - \alpha X - \alpha^2 X + \alpha^3)(X - \alpha^4)(X - \alpha^8) =$
$= (X^3 - \alpha X^2 - \alpha^2 X^2 + \alpha^3 X - \alpha^4 X^2 + \alpha^5 X + \alpha^6 X - \alpha^7)(X - \alpha^8) =$
$= (X^3 - (\alpha + \alpha^2 + \alpha^4)X^2 + (\alpha^3 + \alpha^5 + \alpha^6)X - \alpha^7)(X - \alpha^8) =$
$= X^4 - (\alpha + \alpha^2 + \alpha^4)X^3 + (\alpha^3 + \alpha^5 + \alpha^6)X^2 - \alpha^7 X - \alpha^8 X^3 + \alpha^8(\alpha + \alpha^2 + \alpha^4)X^2 - \alpha^8(\alpha^3 + \alpha^5 X^2 + \alpha^6)X + \alpha^{15} =$
$= X^4 + (\alpha^8 + \alpha^4 + \alpha^2 + \alpha)X^3 + (\alpha^{12} + \alpha^{10} + \alpha^9 + \alpha^6 + \alpha^5 + \alpha^3)X^2 + (\alpha^{14} + \alpha^{13} + \alpha^{11} + \alpha^7)X + \alpha^{15} =$
$= X^4 + 0X^3 + 0X^2 + 1X + 1 =$
$= X^4 + X + 1$

Αυτό δεν είναι τυχαίο. Είναι το πολυώνυμο απ' το οποίο ξεκινήσαμε.

Τα α^2, α^4, α^8 είναι τα συζυγή του α, άρα το ελάχιστο πολυώνυμο και για αυτά είναι το ίδιο με του α.

Αν πάρουμε το $(X-\alpha^3)(X-\alpha^6)(X-\alpha^9)(X-\alpha^{12})$ θα βρούμε το $X^4+X^3+X^2+X+1$
Αντί να κάνουμε τον πολλαπλασιασμό (βαρετό!!!) κάνουμε το εξής:

Ονομάζουμε $\beta=\alpha^3$ τότε έχουμε:

$$1 = [0001]$$
$$\beta = [1000]$$
$$\beta^2 = [1100]$$
$$\beta^3 = [1010]$$
$$\beta^4 = [1111]$$

Σχηματίζουμε τον παρακάτω πίνακα:

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \xrightarrow{\Sigma_1 \to \Sigma_1+\Sigma_2} \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \xrightarrow{\Sigma_1 \to \Sigma_1+\Sigma_3} \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Το άθροισμα όλων των γραμμών είναι 0.
Άρα $\beta^4 + \beta^3 + \beta^2 + \beta + 1 = 0$
Αλλά $\beta = \alpha^3 \neq 1$ οπότε $\beta^5 = (\alpha^3)^5 = \alpha^{15} = 1$
Το β είναι μια 5–ρίζα της μονάδας δηλαδή ρίζα του πολυωνύμου

$$X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1).$$

Κεφάλαιο 5

Πεπερασμένα σώματα αριθμών υπάρχουν και είναι μοναδικά

Είδαμε μέχρι τώρα ότι για κάθε πρώτο αριθμό p υπάρχει ένα σώμα με p στοιχεία, το $\mathbf{F}_p$. Επίσης, είδαμε ότι αν υπάρχει κάποιο ανάγωγο πολυώνυμο $q(X) \in \mathbf{F}_p[X]$ βαθμού m τότε υπάρχει ένα σώμα με p^m στοιχεία. Το $\frac{F_p[X]}{q(X)}$.
Ακόμα, είδαμε ότι δεν υπάρχουν πεπερασμένα σώματα τάξης όχι δύναμης πρώτου.

Εντελώς φυσιολογικά ερωτήματα:

Α Δίνεται πρώτος p και φυσικός m. Υπάρχει σώμα με p^m στοιχεία;
Β Αν υπάρχει ένα σώμα με p^m στοιχεία όπως το κατασκευάσαμε, μήπως υπάρχουν κι άλλα σώματα με p^m στοιχεία μη-ισόμορφα με αυτό;

Η απάντηση στο Α είναι ΝΑΙ. Το πρόβλημα είναι ισοδύναμο με την εύρεση ενός ανάγωγου πολυώνυμο στο $\mathbf{F}_p[X]$ βαθμού m. Θα αποδείξουμε ότι για οποιοδήποτε πρώτο p και οποιοδήποτε φυσικό m υπάρχει ανάγωγο πολυώνυμο βαθμού m στο $\mathbf{F}_p[X]$.

Η απάντηση στο Β είναι ΟΧΙ.

Τις απαντήσεις στα ερωτήματά μας θα τις αποδείξουμε μέσω της παραγοντοποίησης συγκεκριμένων πολυωνύμων ως προς τον $\mathbf{F}_p[X]$, όπου p πρώτος.

Έστω K ένα πεπερασμένο σώμα με q στοιχεία όπου q δύναμη ενός πρώτου p.
Θεωρούμε το πολυώνυμο $X^{q^n} - X$ στο K[X] για κάποιο φυσικό n.
Το πολυώνυμο αναλύεται μονοσήμαντα σε γινόμενο μονικών αναγώγων πολυωνύμων.

Αναφέρουμε χωρίς απόδειξη το ακόλουθο

(5.1) Θεώρημα

$$X^{q^n} - X = \prod_{d|n} V_d(X)$$

όπου $V_d(X)$ το γινόμενο όλων των μονικών ανάγωγων πολυωνύμων του K[X] βαθμού d.

(5.2) Παράδειγμα Για q = 2 και n = 4

Το σώμα είναι το $K = \mathbf{F}_2$ και το πολυώνυμο το $X^{2^4} - X = X^{16} - X = X^{16} + X$.
Θα δούμε στο επόμενο κεφάλαιο ότι:

$$X^{16} + X = (X^4+X+1)\,(X^4+X^3+1)\,(X^4+X^3+X^2+X+1)(X^2+X+1)(X+1)X$$

Επομένως,

$$V_1(X) = X^2 + X$$
$$V_2(X) = X^2 + X+1$$
$$V_4(X) = X^{12} + X^9 + X^6 + X^3 + 1$$

Συγκρίνοντας τους βαθμούς των πολυωνύμων των δυο πλευρών του Θεωρήματος (5.1) καταλήγουμε στο ακόλουθο πάρα πολύ χρήσιμο

(5.3) Πόρισμα

$$q^n = \sum_{d|n} d \cdot I_d$$

όπου I_d το πλήθος των διακεκριμένων μονικών ανάγωγων πολυωνύμων βαθμού d.

Στο παράδειγμά μας: $q^n = 2^4 = 16$ ενώ $\sum_{d|4} d \cdot I_d = I_1 + 2I_2 + 4I_4 = 2 + 2\cdot 1 + 4\cdot 3 = 16$.

Ο επόμενος στόχος μας θα είναι να "λύσουμε" τις εξισώσεις:

1. $n = \sum_{d|n} \varphi(d)$ ως προς $\varphi(d)$,
2. $X^{q^n} - X = \prod_{d|n} V_d(X)$ ως προς $V_d(X)$ και
3. $q^n = \sum_{d|n} d \cdot I_d$ ως προς I_d.

Θα χρειαστούμε τον νόμο αντιστροφής του Möbius:

Γενικά αν G προσθετική αβελιανή ομάδα και

α(1), α(2), α(3), …
b(1), b(2), b(3), …

δυο ακολουθίες στοιχείων της ομάδας οι οποίες συνδέονται από τη σχέση:

$$\alpha(n) = \sum_{d|n} b(d) \text{ για κάθε } n \geq 1$$

Ζητείται αντίστροφος τύπος ο οποίος να μας δίνει τα b(n) συναρτήσει τον α(d).

(5.4) Παράδειγμα 1

Αν πάρουμε G = **Z**, (G,+) = (**Z**,+) και α(n) = n, b(d) = φ(d) τότε έχουμε: $\alpha(n) = \sum_{d|n} b(d)$ αφού $n = \sum_{d|n} \varphi(d)$

(5.5) Παράδειγμα 2

Έστω G το σύνολο των ρητών συναρτήσεων ως προς κάποιο πεπερασμένο σώμα K, δηλαδή $g := \frac{p(X)}{q(X)}$, p(X), q(X) ∈ K[X] και q(X) όχι το μηδενικό πολυώνυμο.

Το G με πράξη $g_1 \cdot g_2 = \frac{p_1(X)\cdot p_2(X)}{q_1(X)\cdot q_2(X)}$ όπου $g_i = \frac{p_i(X)}{q_i(X)}$ i = 1, 2 γίνεται αντιμεταθετική (αβελιανή) ομάδα. Αν πάρουμε $\alpha(n) = X^{q^n} - X$ και $b(d) = V_d(X)$ τότε λόγω της ισότητας (2) ισχύει ότι $\alpha(n) = \sum_{d|n} b(d)$.

(5.6) Παράδειγμα 3

Αν πάρουμε G = **Z** και πράξη την πρόσθεση (+) και έχουμε $\alpha(n) = q^n$ και $b(d) = d \cdot I_d$ τότε λόγω της ισότητας (3) ισχύει ότι $\alpha(n) = \sum_{d|n} b(d)$.

Η σχέση $\alpha(n) = \sum_{d|n} b(d)$ μας δίνει ότι τα b(n) εκφράζονται μονοσήμαντα μέσω της α(n) διότι: $b(1) = \alpha(1) \left(\alpha(1) = \sum_{d|1} b(d) = b(1) \right)$ και $b(n) = \alpha(n) - \sum_{\substack{d|n \\ d\neq n}} b(d)$.

Έχουμε ότι:

$b(1) = \alpha(1)$
$b(2) = \alpha(2) - \sum_{\substack{d|2 \\ d\neq 2}} b(d) = \alpha(2) - b(1) = \alpha(2) - \alpha(1)$
$b(3) = \alpha(3) - b(1) = \alpha(3) - \alpha(1)$
$b(4) = \alpha(4) - b(2) - b(1) = \alpha(4) - (\alpha(2) - \alpha(1)) - \alpha(1) = \alpha(4) - \alpha(2)$
$b(5) = \alpha(5) - \alpha(1)$
$b(6) = \alpha(6) - \alpha(3) - \alpha(2) + \alpha(1)$
…….

(5.6) Ο Möbius όρισε τη ομώνυμη συνάρτησή του:
Αν n φυσικός αριθμός και $n = p_1^{\alpha_1} \cdot p_2^{\alpha_{21}} \cdot \ldots \cdot p_s^{\alpha_s}$ τότε:

$$\mu(n) = \begin{cases} 1 & \text{αν } n = 1 \\ 0 & \text{αν για κάποια } \alpha_i \text{ ισχύει } \alpha_i \geq 2 \\ (-1)^s & \text{αλλιώς} \end{cases}$$

Ισχύει (για n > 1): $\sum_{d|n} \mu(d) = 0$ (Απόδειξη, Θεωρία Αριθμών Ι)

Ο τύπος αντιστροφής:

$b(n) = \sum_{d|n} \alpha(d)\cdot\mu(\frac{n}{d})$ ή ισοδύναμα $b(n) = \sum_{d|n} \mu(d)\cdot\alpha(\frac{n}{d})$

Βρίσκουμε, όπως και προηγουμένως, τα b(n):

$b(1) = \sum_{d|1} \mu(d)\cdot\alpha(\frac{1}{d}) = \alpha(1)\,\mu(1) = \alpha(1)\cdot 1 = \alpha(1)$

$b(2) = \sum_{d|2} \mu(d)\cdot\alpha(\frac{2}{d}) = \alpha(1)\,\mu(2) + \alpha(2)\,\mu(1) = \alpha(1)\cdot(-1) + \alpha(2)\cdot 1 = \alpha(2) - \alpha(1)$

$b(3) = \sum_{d|3} \mu(d)\cdot\alpha(\frac{3}{d}) = \alpha(1)\,\mu(3) + \alpha(3)\,\mu(1) = \alpha(1)\cdot(-1) + \alpha(3)\cdot 1 = \alpha(3) - \alpha(1)$

$b(4) = \sum_{d|4} \mu(d) \cdot \alpha(\frac{4}{d}) = \alpha(1)\,\mu(4) + \alpha(2)\,\mu(2) + \alpha(4)\,\mu(1)$

$= \alpha(1) \cdot 0 + \alpha(2) \cdot (-1) + \alpha(4) \cdot 1 = \alpha(4) - \alpha(2)$

$b(5) = \sum_{d|5} \mu(d) \cdot \alpha(\frac{5}{d}) = \alpha(1)\,\mu(5) + \alpha(5)\,\mu(1) = \alpha(1) \cdot (-1) + \alpha(5) \cdot 1 = \alpha(5) - \alpha(1)$

$b(6) = \sum_{d|6} \mu(d) \cdot \alpha(\frac{6}{d}) = \alpha(1)\,\mu(6) + \alpha(2)\,\mu(3) + \alpha(3)\,\mu(2) + \alpha(6)\,\mu(1)$

$= \alpha(1) \cdot (-1)^2 + \alpha(2) \cdot (-1) + \alpha(3) \cdot (-1) + \alpha(6) \cdot 1 = \alpha(6) - \alpha(3) - \alpha(2) + \alpha(1)$

κ.ο.κ.

(5.7) Εφαρμογές

1. $n = \sum_{d|n} \varphi(d)$

Έχουμε $\alpha(n) = n$ και $b(d) = \varphi(d)$

Επομένως, $\varphi(n) = \sum_{d|n} \alpha(d) \cdot \mu(\frac{n}{d}) = \sum_{d|n} \mu(d) \cdot \alpha(\frac{n}{d}) = \sum_{d|n} \mu(d) \cdot \frac{n}{d}$

Δηλαδή $\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$

Από εδώ συνεπάγεται ο τύπος της φ – συνάρτησης του Euler, ότι αν n φυσικός τέτοιος ώστε $n = p_1^{\alpha_1} \cdot p_2^{\alpha_{21}} \cdot \ldots \cdot p_s^{\alpha_s}$ τότε $\varphi(n) =$

$$n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdot \ldots \cdot (1 - \frac{1}{p_s}) = p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_{21} - 1} \cdot \ldots \cdot p_s^{\alpha_s - 1} \cdot (p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_s - 1).$$

Για παράδειγμα: $\varphi(180) = \varphi(2^2\, 3^2\, 5) = 180 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 48$

2. $q^n = \sum_{d|n} d \cdot I_d$

Εδώ έχουμε ότι $\alpha(n) = q^n$ και $b(d) = d \cdot I_d$

Επομένως, ο νόμος της αντιστροφής του Möbius μας δίνει:

$b(n) = \sum_{d|n} \mu(d) \cdot \alpha(\frac{n}{d})$ ή

$n \cdot I_n = \sum_{d|n} \mu(d) \cdot q^{\frac{n}{d}}$ ή

$I_n = \frac{1}{n} \sum_{d|n} \mu(d) \cdot q^{\frac{n}{d}}$

Ο τύπος αυτός μας δίνει το πλήθος των ανάγωγων (μονικών) πολυωνύμων βαθμού n ως προς το σώμα K με q στοιχεία.

Επειδή ο πιο μεγάλος όρος είναι για d = 1 έχουμε ότι $I_n \approx \frac{q^n}{n}$.

Όλα τα μονικά πολυώνυμα βαθμού n είναι q^n. Η πιθανότητα να εκλέξουμε ένα μονικό πολυώνυμο βαθμού n και να είναι ανάγωγο είναι $\frac{1}{n}$.

Θα υπολογίσουμε μερικά I_n.

$I_1 = q$ (κάθε πολυώνυμο βαθμού 1 στο σώμα K είναι ανάγωγο)

$I_2 = \frac{1}{2}\left(\mu(1)q^2 + \mu(2)q\right) = \frac{1}{2}\left(1 \cdot q^2 + (-1) \cdot q\right) = \frac{q^2 - q}{2}$

Ομοίως, $I_3 = \frac{q^3 - q}{3}, I_4 = \frac{q^4 - q^2}{4}, I_5 = \frac{q^5 - q}{5}, I_6 = \frac{1}{6} \cdot (q^6 - q^3 - q^2 + q).$

Θα αποδείξουμε ότι $I_n > 0$ για κάθε $n \in \mathbb{N}$.

Ας πάρουμε το I_6.

$I_6 = \frac{1}{6}\ (q^6 - q^3 - q^2 + q)$ ή $\frac{6I_6}{q} = q^5 - q^2 - q + 1 \equiv 1 \pmod q$. Οπότε $\frac{6I_6}{q} > 0$ ή $I_6 > 0$

Γενικά: $nI_n = \sum_{d|n} \mu(d) \cdot q^{\frac{n}{d}}$ το οποίο είναι ένα αλγεβρικό άθροισμα, με συντελεστές ± 1, φθίνουσων δυνάμεων του q και συνεπώς δεν μπορεί να είναι ποτέ μηδέν.

Επομένως ισχύει το

(5.8) Θεώρημα

Αν υπάρχει σώμα K με q στοιχεία τότε για κάθε $n \geq 1$ υπάρχει τουλάχιστον ένα ανάγωγο πολυώνυμο βαθμού n.
Δηλαδή, για κάθε φυσικό $n \geq 1$ υπάρχει τουλάχιστον ένα σώμα με q^n στοιχεία.

Έχουμε ήδη αποδείξει ότι υπάρχει σώμα με q στοιχεία όταν και μόνο όταν το q είναι δύναμη πρώτου αριθμού. Το μόνο πράγμα που μας μένει είναι πόσα σώματα τάξης q^n υπάρχουν. Θα δεχθούμε χωρίς απόδειξη ότι στην ουσία υπάρχει μόνο ένα σώμα τάξης q^n δηλαδή ότι: δυο οποιαδήποτε σώματα με q^n στοιχεία είναι μεταξύ τους ισόμορφα.

Συμβολισμός Το πεπερασμένο σώμα με p^m στοιχεία θα το συμβολίζουμε $GF(p^m)$
[GF = Galois Field].

(5.9) Παράδειγμα Έστω $F = \mathbf{F}_2[X]$ και $q(X) = X^4 + X^3 + X^2 + X + 1$ (q ανάγωγο στο $\mathbf{F}_2[X]$) τότε $E = \mathbf{F}_2[X]/q(X)$ δηλαδή $E = GF(2^4)$ και $\#E = 2^4 = 16$

Θα κλείσουμε το κεφάλαιο με το θέμα της περιγραφής των υποσωμάτων ενός πεπερασμένου σώματος.

(5.10) Ορισμός Ένα **υπόσωμα** K του σώματος F είναι ένα υποσύνολο K του F το οποίο, ως προς τις πράξεις του F, είναι επίσης σώμα.

π.χ. Q υπόσωμα του R
Q υπόσωμα του C
R υπόσωμα του C

Εμείς εδώ ενδιαφερόμαστε για πεπερασμένα σώματα.
Έχουμε ήδη αποδείξει ότι υπάρχει μοναδικό σώμα με p^n στοιχεία, $p \in \mathbf{P}$, $n \in \mathbf{N}$.
Εδώ, θα ασχοληθούμε με το εξής ερώτημα;

Ποια υποσώματα περιέχονται στο $GF(p^n)$;

Ισχύει το ακόλουθο

(5.11) Θεώρημα

Για κάθε διαιρέτη d | n το σώμα $GF(p^n)$ περιέχει ακριβώς ένα υπόσωμα ισόμορφο με το $GF(p^d)$ και το $GF(p^n)$ δεν περιέχει άλλα υποσώματα τάξης p^d.

Απόδειξη:
Έστω $F = GF(p^n)$ και $K \leq F$ (K υπόσωμα του F).
Αφού F πεπερασμένο, έπεται ότι K πεπερασμένο με πλήθος στοιχείων δύναμη του p.
Δηλαδή $K \cong GF(p^d)$ για $d < n$ και $K \neq F$.

Αποδείξαμε ότι κάθε στοιχείο $\alpha \in K$ επαληθεύει την εξίσωση $X^{p^d} - X = 0$.

$\alpha \in K \leq F \Rightarrow \alpha \in F \Rightarrow$ το α επαληθεύει την εξίσωση $X^{p^n} - X = 0$.

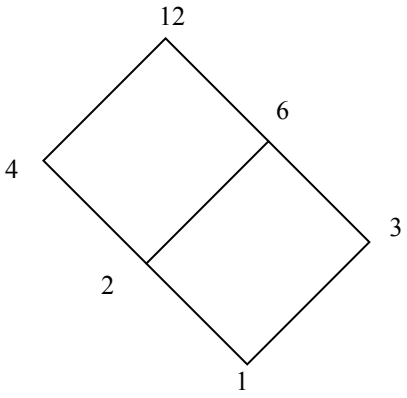
Επομένως αποδείξαμε ότι κάθε ρίζα του $X^{p^d} - X$ είναι και ρίζα του $X^{p^n} - X$ και επειδή τα πολυώνυμα έχουν απλές ρίζες έπεται ότι το $X^{p^d} - X$ διαιρεί το $X^{p^n} - X$.
Στο κεφάλαιο 4 έχουμε δει ότι αυτό συνεπάγεται ότι d | n. Δηλαδή, αν το $GF(p^n)$ έχει υπόσωμα το $GF(p^d)$ τότε d | n.

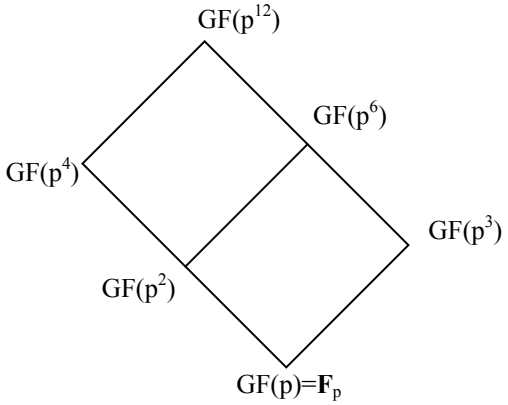
Τώρα υποθέτουμε ότι d | n.
Αν το F έχει υπόσωμα ισόμορφο στο $GF(p^d)$ τότε αυτό θα είναι $K = \left\{ \alpha \in F \;\middle|\; \alpha^{p^d} = \alpha \right\}$.

Τα στοιχεία του K ορίζονται ακριβώς σας οι ρίζες του $X^{p^d} - X$. Θα αποδείξουμε ότι το K περιέχει ακριβώς p^d στοιχεία και είναι σώμα.

Έχουμε δει ότι $X^{p^d} - X \mid X^{p^n} - X$ και $X^{p^n} - X = \prod (X - \alpha \mid \alpha \in F)$. Οι ρίζες του $X^{p^d} - X$ είναι και ρίζες του $X^{p^n} - X$ το οποίο όμως έχει όλες τις ρίζες του στο F δηλαδή έχει p^n ρίζες στο F. Επομένως το $X^{p^d} - X$ έχει p^d ρίζες στο F και το K έχει ακριβώς p^d στοιχεία.
Το K είναι σώμα αφού για κάθε $\alpha \in K$ και $b \in K$ ισχύει ότι $\alpha - b \in K$ διότι $(\alpha - b)^{p^d} = \alpha^{p^d} - b^{p^d} = \alpha - b$ και ανάλογα $ab \in K$ και $\alpha^{-1} \in K$.

(5.12) Παράδειγμα Έστω n = 12





Κεφάλαιο 6

Παραγοντοποίηση πολυωνύμων σε πεπερασμένα σώματα

Ξαναθυμίζουμε ότι $X^{q^n} - X = \prod_{d|n} V_d(X)$

όπου $V_d(X)$ το γινόμενο όλων των μονικών ανάγωγων πολυωνύμων βαθμού d ως προς το σώμα GF(q).

Εφαρμόζουμε το νόμο αντιστροφής του Möbius για την πολλαπλασιαστική ομάδα $\left\{ \frac{p(X)}{q(X)} \middle| p(X), q(X) \in K[X], p(X) \neq 0, q(X) \neq 0 \right\}$ όπου K = GF(q)

Ο τύπος του Möbius γράφεται πολλαπλασιαστικά: $b_n = \prod_{d|n} \alpha_d^{\mu(\frac{n}{d})}$

δηλαδή $V_n(X) = \prod_{d|n} (X^{q^d} - X)^{\mu(\frac{n}{d})}$

(6.1) Παράδειγμα: Για q = 2 και n = 6

$V_6(X) = \prod_{d|6} (X^{2^d} - X)^{\mu(\frac{6}{d})} = \frac{(X^2 - X)(X^{64} - X)}{(X^4 - X)(X^8 - X)} = \frac{(X-1)(X^{63}-1)}{(X^3-1)(X^7-1)}$ το οποίο είναι πολυώνυμο βαθμού 54. (Είναι γινόμενο 9 ανάγωγων πολυωνύμων βαθμού 6 το καθένα)

Ερώτημα: Πως θα τα βρούμε;

Το πρόβλημα είναι αρκετά δύσκολο. Θα κάνουμε κάποια πρόοδο αν μελετήσουμε τα λεγόμενα κυκλοτομικά πολυώνυμα.

Κατ' αρχήν θα μελετήσουμε τα κυκλοτομικά πολυώνυμα στο σώμα C των μιγαδικών αριθμών.

Έστω $n \in \mathbb{N}$ και $\zeta := e^{\frac{2\pi i}{n}}$. Ως γνωστόν ισχύει ότι $X^n - 1 = \prod_{j=0}^{n-1} (X - \zeta^j)$ (1)

Παρατήρηση: Η $\text{ord}(\zeta^j)$ εξαρτάται από τον ΜΚΔ(j, n) και για κάθε διαιρέτη d του n υπάρχουν ακριβώς φ(d) από τις ρίζες ζ^j, $0 \le j \le n-1$, που έχουν τάξη d.

$\left(n = \sum_{d|n} \phi(d) \right)$

(6.2) Ορισμός: Το d-στό **κυκλοτομικό πολυώνυμο** ορίζεται ως εξής:

$\Phi_d(X) = \prod \left\{ (X - \zeta^j) \middle| 0 \le j \le n-1 \wedge \text{ΜΚΔ}(j, n) = \frac{n}{d} \right\}$ (2)

Δηλαδή: $\text{ord}(\zeta^j) = \frac{n}{\text{ΜΚΔ}(j, n)} = \frac{n}{\frac{n}{d}} = d$.

Δηλαδή το $\Phi_d(X)$ είναι το μονικό πολυώνυμο βαθμού φ(d) με ρίζες εκείνες τις δυνάμεις του ζ^j που έχουν τάξη d.

Από τις (1) και (2) έχουμε ότι: $X^n - 1 = \prod_{d|n} \Phi_d(X)$

Με τη μέθοδο αντιστροφής του Möbius (Möbius inversion formula) έχουμε ότι:

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})}$$

Παρατήρηση $\Phi_n(X) \in \mathbf{Z}[X]$

Ο λόγος είναι ότι το $\Phi_n(X)$ είναι πηλίκο δυο μονικών πολυωνύμων με ακέραιους συντελεστές.

Στον αριθμητή είναι οι παράγοντες με $\mu\left(\frac{n}{d}\right) = +1$

Στον παρονομαστή είναι οι παράγοντες με $\mu\left(\frac{n}{d}\right) = -1$

(6.3) Παράδειγμα Το $\Phi_{18}(X) = \prod_{d|18} (X^d - 1)^{\mu(\frac{18}{d})} = \frac{(X^3 - 1)(X^{18} - 1)}{(X^6 - 1)(X^9 - 1)}$ είναι πηλίκο δυο μονικών πολυωνύμων με ακέραιους συντελεστές βαθμών 21 (ο αριθμητής) και 15 (ο παρονομαστής). Για να διαπιστώσουμε ότι $\Phi_{18}(X) \in \mathbf{Z}[X]$

1ος τρόπος Κάνουμε την διαίρεση
2ος τρόπος (του Berlekamp)
Το $\Phi_{18}(X)$ είναι πολυώνυμο βαθμού $\varphi(18) = \varphi(2 \cdot 3^2) = 6$.
Αν πάρουμε το πολυώνυμο $\Phi_{18}(X)$ modulo X^7 επειδή deg $\Phi_{18}(X) = 6 < 7 = \deg X^7$ δεν χάνουμε τίποτα.

$$\Phi_{18}(X) \equiv \frac{(X^3 - 1)(-1)}{(X^6 - 1)(-1)} \equiv \frac{1 - X^3}{1 - X^6} \text{ modulo } X^7$$

$$\frac{1 - X^3}{1 - X^6} = \frac{(1 - X^3)(1 + X^6)}{(1 - X^6)(1 + X^6)} = \frac{(1 - X^3)(1 + X^6)}{1 - X^{12}} \text{ αλλά } 1 - X^{12} \equiv 1 \pmod{X^7}$$

Επομένως: $\Phi_{18}(X) \equiv (1 - X^3)(1 + X^6) \equiv 1 - X^3 + X^6 \pmod{X^7}$
Δηλαδή: $\Phi_{18}(X) = X^6 - X^3 + 1$.

(6.4) Μικρός πίνακας κάποιων κυκλοτομικών πολυωνύμων

n	$\Phi_n(X)$
1	$X - 1$
2	$X + 1$
3	$X^2 + X + 1$
4	$X^2 + 1$
5	$X^4 + X^3 + X^2 + X + 1$
6	$X^2 - X + 1$
7	$X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$
8	$X^4 + 1$
9	$X^6 + X^3 + 1$

Μπορούμε να εργαστούμε σε πεπερασμένα σώματα διότι $\Phi_n(X) \in \mathbf{Z}[X]$

Ξαναγυρίζουμε πίσω στο $V_6(X) = \dfrac{(X-1)(X^{63}-1)}{(X^3-1)(X^7-1)}$

Από την (1) έχουμε: $X^n - 1 = \prod_{d|n} \Phi_d(X)$ επομένως

$X - 1 = \Phi_1(X)$
$X^{63} - 1 = \Phi_1(X)\,\Phi_3(X)\,\Phi_7(X)\,\Phi_9(X)\,\Phi_{21}(X)\,\Phi_{63}(X)$
$X^7 - 1 = \Phi_1(X)\,\Phi_7(X)$
$X^3 - 1 = \Phi_1(X)\,\Phi_3(X)$

Οπότε γράφουμε:

$$V_6(X) = \frac{\Phi_1(X)\Phi_1(X)\Phi_3(X)\Phi_7(X)\Phi_9(X)\Phi_{21}(X)\Phi_{63}(X)}{\Phi_1(X)\Phi_7(X)\Phi_1(X)\Phi_3(X)}$$

Δηλαδή:

$$V_6(X) = \Phi_9(X)\,\Phi_{21}(X)\,\Phi_{63}(X)$$

όπου

$\Phi_9(X)$ βαθμού $\varphi(9) = 6$
$\Phi_{21}(X)$ βαθμού $\varphi(21) = 12$
$\Phi_{63}(X)$ βαθμού $\varphi(63) = 36$

Το $\Phi_9(X) = X^6 + X^3 + 1$ είναι ανάγωγο στο GF(2) αφού είναι βαθμού 6 και $V_6(X)$ γινόμενο 9 ανάγωγων πολυωνύμων βαθμού 6 το καθένα.

Για να έχουμε την ανάλυση του $V_6(X)$ σε γινόμενο ανάγωγων χρειάζεται να γνωρίζουμε τον τρόπο παραγοντοποίησης των κυκλοτομικών πολυωνύμων.

Είναι γνωστό ότι το $\Phi_n(X) \in \mathbb{Q}[X]$ για κάθε $n \geq 1$ είναι ανάγωγο στο $\mathbb{Q}[X]$.
Αυτό δεν ισχύει στα πεπερασμένα σώματα.
Για παράδειγμα:

$$\Phi_4(X) = X^2 + 1 = \begin{cases} (X+1)^2 & \text{στο } F_2 \\ \text{ανάγωγο} & \text{στο } F_3 \\ (X+1)^2 & \text{στο } F_4 \\ (X-2)(X-3) & \text{στο } F_5 \end{cases}$$

Ισχύει το

(6.5) Θεώρημα Αν p πρώτος, $p \nmid n$ τότε για $k \geq 1$ ισχύουν:

(a) $\Phi_{n\cdot p^k}(X) = \Phi_{n\cdot p}(X^{p^{k-1}})$ (για σώματα κάθε χαρακτηριστικής)

(b) $\Phi_{n\cdot p^k}(X) = \dfrac{\Phi_n(X^{p^k})}{\Phi_n(X^{p^{k-1}})}$ (για σώματα κάθε χαρακτηριστικής)

(c) $\Phi_{n\cdot p^k}(X) = \Phi_n(X)^{p^k - p^{k-1}}$ (μόνο σε σώματα χαρακτηριστικής p)

(6.6) Παράδειγμα

$\Phi_{72}(X) = \Phi_{8\cdot 3^2}(X) \overset{(a)}{=} \Phi_{8\cdot 3}(X^{3^{2-1}}) = \Phi_{8\cdot 3}(X^3) = \Phi_{3\cdot 2^3}(X^3) \overset{(a)}{=} \Phi_{3\cdot 2}\left((X^3)^{2^{3-1}}\right) = \Phi_6(X^{12}) =$

$\overset{\text{ΠΙΝΑΚΑΣ (6.4)}}{=} (X^{12})^2 - X^{12} + 1 = X^{24} - X^{12} + 1.$

Ξανά: $\Phi_{72}(X) \overset{(b)}{=} \dfrac{\Phi_8(X^9)}{\Phi_8(X^3)} = \dfrac{X^{36}+1}{X^{12}+1} \overset{\text{ΔΙΑΙΡΕΣΗ}}{=} X^{24} - X^{12} + 1.$

Ξανά (αλλά τώρα σε σώμα χαρακτηριστικής 3): $\Phi_{72}(X) \overset{(c)}{=} \left[\Phi_8(X)\right]^{3^2-3} = \left[\Phi_8(X)\right]^6 =$
$= (X^4+1)^6 = [(X^4+1)^3]^2 = (X^{12}+1)^2 = X^{24} - X^{12} + 1.$

(6.7) Άσκηση Σε κάθε σώμα χαρακτηριστικής 2 ισχύουν:

(a) $\Phi_4(X) = (X+1)^2$

(b) $\Phi_3(X) = \Phi_6(X) = X^2 + X + 1$

(c) $\Phi_8(X) = (X+1)^4 = X^4 + 1$

Για να εφαρμόζουμε το (c) του θεωρήματος (6.5) σε σώματα χαρακτηριστικής p θα πρέπει το p να μην διαιρεί το n.

Έστω λοιπόν K πεπερασμένο σώμα τάξης $q = p^l$. Επειδή $p \nmid n$ έχουμε ότι υπάρχει φυσικός αριθμός λ τέτοιος ώστε $q^\lambda \equiv 1 \pmod n$. Έστω m ο ελάχιστος φυσικός μ' αυτή την ιδιότητα. $q^m \equiv 1 \pmod n$ Έστω F το σώμα με q^m στοιχεία $\left(F \cong GF(q^m)\right)$.
Επειδή $n \mid q^m - 1$ από προηγούμενο θεώρημα έχουμε ότι υπάρχει $\alpha \in F$ τέτοιο ώστε $\text{ord}(\alpha)=n$. Όπως κάναμε και πιο πριν: $\Phi_d(X) = \prod_{\substack{0\leq j\leq n-1 \\ \text{ord}(\alpha^j)=d \leftrightarrow \text{ΜΚΔ}(j,n)=\frac{n}{d}}} (X - \alpha^j) = \prod (X-\beta) \mid \text{ord}(\beta) = d.$

και $\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})}$.

Αυτό σημαίνει ότι το $\Phi_d(X)$ αναλύεται στο «μεγάλο» σώμα F σε γινόμενο γραμμικών παραγόντων.

<u>Πρόβλημα</u>: Τι γίνεται στο «μικρό» σώμα K;

Το ελάχιστο πολυώνυμο του α έχει ρίζες $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$
Δηλαδή υπάρχουν ακριβώς d-συζυγή του α στο σώμα F όπου d ο ελάχιστος φυσικός τέτοιος ώστε $q^d \equiv 1 \pmod n$.
Αλλά αυτό εμείς το ορίσαμε και το είπαμε m.
Επομένως το $\Phi_n(X)$ έχει έναν ανάγωγο παράγοντα βαθμού m.

<u>Πρόβλημα</u>: Ποια είναι τα ανάγωγα πολυώνυμα των άλλων ριζών του $\Phi_n(X)$;

Εξ ορισμού όλα έχουν βαθμό d = m. Με το ίδιο επιχείρημα όπως και προηγουμένως έπεται ότι υπάρχουν ακριβώς d = m συζυγή.

(6.8) <u>Θεώρημα</u> Αν p πρώτος, $p \nmid n$ και $q = p^l$ τότε το $\Phi_n(X)$ στο GF(q) = K αναλύεται σε γινόμενο $\frac{\varphi(n)}{m}$ ανάγωγων πολυωνύμων, βαθμού m, όπου m ο ελάχιστος φυσικός την ιδιότητα $q^m \equiv 1 \pmod n$.

(6.9) <u>Παράδειγμα 1</u> Το $\Phi_7(X)$ υπέρ του GF(2) = K.

Έχουμε ότι φ(7) = 6. Θα πρέπει να βρούμε το m για q = 2 και n = 7.
Δηλαδή τον ελάχιστο φυσικό τέτοιο ώστε $2^m \equiv 1 \pmod 7$. Οπότε m = 3.
Επομένως το $\Phi_7(X)$ αναλύεται στο GF(2) σε γινόμενο $\frac{6}{3} = 2$ ανάγωγων (κυκλικών) πολυωνύμων βαθμού 3 το καθένα.

Επομένως, αν α οποιοδήποτε στοιχείο τάξης 7 στο F = GF(2^3) τα ανάγωγα πολυώνυμα του $\Phi_7(X)$ στο K = GF(2) θα είναι

$$f_1(X)=(X-\alpha)(X-\alpha^2)(X-\alpha^4)$$
$$f_3(X)=(X-\alpha^3)(X-\alpha^6)(X-\alpha^5)$$

Αν π.χ. α ρίζα της εξίσωσης $X^3=X+1$ τότε μπορούμε να υπολογίσουμε ότι

$$f_1(X)=X^3+X+1 \text{ και}$$
$$f_3(X)=X^3+X^2+1.$$

Πράγματι, το GF(2^3) $\cong \mathbf{F}_2[X]/f(X)$ όπου f(X) ανάγωγο μονικό πολυώνυμο του $F_2[X]$.
Ένα τέτοιο πολυώνυμο είναι το X^3+X+1, επομένως αν για α πάρουμε μια ρίζα του X^3+X+1 θα έχουμε $\alpha^3+\alpha+1 = 0$. Οπότε $\alpha^3 = -(\alpha+1)$ ή $\alpha^3 = \alpha+1$.

Βρίσκουμε τους συντελεστές του $f_1(X)$:
- Συντελεστής του X^2 =

$\alpha + \alpha^2 + \alpha^4 = \alpha + \alpha^2 + \alpha\cdot\alpha^3 = \alpha + \alpha^2 + \alpha(\alpha + 1) = \alpha + \alpha^2 + \alpha + \alpha^2 = 2\alpha + 2\alpha^2 = 0$

- Συντελεστής του X =
$\alpha\cdot\alpha^2 + \alpha\cdot\alpha^4 + \alpha^2\cdot\alpha^4 = \alpha^3 + \alpha^5 + \alpha^6 = \alpha^3\,(1 + \alpha^2 + \alpha^3) = (\alpha + 1)(\,1 + \alpha^2 + \alpha + 1) = (\alpha + 1)(\,\alpha^2 + \alpha) = \alpha(\alpha + 1)^2 = \alpha(\alpha^2 + 1) = \alpha^3 + \alpha = \alpha + 1 + \alpha = 1$
- Σταθερός όρος =
$\alpha\cdot\alpha^2\cdot\alpha^4 = \alpha^7 = 1$

Επομένως $f_1(X) = X^3 + 0X + 1X + 1 = X^3 + X + 1$
Ομοίως βρίσκουμε: $f_3(X)=X^3 + X^2 + 1$

(6.10) Παράδειγμα 2 Ζητάμε να παραγοντοποιήσουμε το $\Phi_{180}(X)$ στο GF(3).
Έχουμε ότι $180=2^2\,3^2\,5$.
Επομένως λόγω του (c) του θεωρήματος $\Phi_{180}(X) = [\Phi_{20}(X)]^{9-3}=[\Phi_{20}(X)]^6$.
Συνεπώς θα πρέπει να παραγοντοποιήσουμε το κυκλοτομικό πολυώνυμο $\Phi_{20}(X)$ στο GF(3). Επειδή $3^4 \equiv 1 \pmod{20}$ έχουμε ότι m=4 και n=20 με φ(n)=φ(20)=8.
Άρα το $\Phi_{20}(X)$ είναι ίσο με το γινόμενο 8/4=2 αναγώγων πολυωνύμων βαθμού 4 το καθένα.
Οπότε, αν α στοιχείο τάξης 20 στο $GF(3^4)$ τότε οι δυο παράγοντες του $\Phi_{20}(X)$ είναι:
$f_1(X)=(X-\alpha)\,(X-\alpha^3)\,(X-\alpha^9)\,(X-\alpha^7)$
$f_{11}(X)=(X-\alpha^{11})\,(X-\alpha^{13})\,(X-\alpha^{19})\,(X-\alpha^{17})$
Αν πάλι έχουμε στο GF(81) ότι $\dfrac{F_2[X]}{q(X)}$ και α ρίζα του q(X) μπορούμε να υπολογίσουμε επακριβώς τα $f_1(X)$ και $f_{11}(X)$.
Πάντως καταλήξαμε ότι $\Phi_{180}(X)$ είναι ίσο με το γινόμενο 12 ($12 = 2\cdot 6$) αναγώγων πολυωνύμων βαθμού 4 το καθένα.

Θα προσπαθήσουμε να ανακαλύψουμε τεχνικές που μας επιτρέπουν να βρούμε τους ανάγωγους παράγοντες του κυκλοτομικού πολυωνύμου $\Phi_n(X)$ στο GF(q) επακριβώς.
Σαν πρώτο βήμα θα προσπαθήσουμε να βρούμε κριτήρια για το πότε το $\Phi_n(X)$ είναι ανάγωγο.

Σύμφωνα με το Θεώρημα (6.8):

$$\Phi_n(X) \text{ ανάγωγο στο } GF(q) \Leftrightarrow \left\{ \begin{array}{c} q^{\varphi(n)} \equiv 1 \pmod{n} \\ q^{\kappa} \not\equiv 1 \pmod{n}\ \forall \kappa < \varphi(n) \end{array} \right\} \quad (1)$$

Η (1) μας λέει ότι η ομάδα των πρώτων κλάσεων υπολοίπων mod n, η οποία έχει τάξη φ(n), είναι κυκλική και έχει το q σαν γεννήτορα. (Δηλαδή το q είναι πρωταρχική ρίζα modulo n).

Από τη Θεωρία Αριθμών όμως γνωρίζουμε ότι οι μοναδικές τιμές του n για τις οποίες υπάρχει πρωταρχική ρίζα mod n είναι $n = 1, 2, 4, p^s, 2p^s$, $s \in \mathbb{N}$ και $p \in \mathbb{P}$, $p \neq 2$.

Επομένως αν το n δεν είναι της παραπάνω μορφής τότε $\Phi_n(X)$ όχι ανάγωγο στο GF(q).
Απ' την άλλη μεριά αν το n είναι τέτοιας μορφής τότε
[$\Phi_n(X)$ ανάγωγο στο K = GF(q)] $\Leftrightarrow$ [το q είναι πρωταρχική ρίζα mod n].

(6.11) Παράδειγμα
Έστω n = 7 τότε φ(n) = φ(7) = 6.

Παίρνουμε τους πρώτους ως προς 7 (mod 7): 1, 2, 3, 4, 5, 6 (mod 7)
$2^3 \equiv 1 \pmod 7 \Rightarrow \text{ord}_7 2 = 3$. Επομένως, το 2 δεν είναι πρωταρχική ρίζα mod 7.
$3^1 \equiv 3 \pmod 7$, $3^2 \equiv 2 \pmod 7$, $3^3 \equiv 6 \pmod 7 \Rightarrow \text{ord}_7 3 = 6$. Επομένως, το 3 είναι πρωταρχική ρίζα mod 7.
$4^3 \equiv 1 \pmod 7 \Rightarrow \text{ord}_7 4 = 3$. Επομένως, το 4 δεν είναι πρωταρχική ρίζα mod 7.
$5^1 \equiv 5 \pmod 7$, $5^2 \equiv -3 \pmod 7$, $5^3 \equiv -1 \pmod 7 \Rightarrow \text{ord}_7 5 = 6$. Επομένως, το 5 είναι πρωταρχική ρίζα mod 7.
$6^2 \equiv 1 \pmod 7 \Rightarrow \text{ord}_7 6 = 2$. Επομένως, το 6 δεν είναι πρωταρχική ρίζα mod 7.

Άρα, $\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ είναι ανάγωγο στο σώμα GF(q)

$$\Leftrightarrow \begin{cases} q \equiv 3 \pmod 7 \\ \quad \text{ή} \\ q \equiv 5 \pmod 7 \end{cases}$$

π.χ. για q = 3, 5, 17, 19, … το $\Phi_7(X)$ είναι ανάγωγο στο GF(q).

Ας πάρουμε n = 8 (αναμένουμε να μην έχει πρωταρχικές ρίζες).
Έχουμε ότι $\varphi(n) = \varphi(8) = 4$.
Οι πρώτες κλάσεις mod 8 είναι: 1, 3, 5, 7.
$3^2 \equiv 1 \pmod 8 \Rightarrow \text{ord}_8 3 = 2 \Rightarrow$ το 3 δεν είναι πρωταρχική ρίζα mod 8.
$(-3)^2 \equiv 1 \pmod 8 \Rightarrow \text{ord}_8 5 = 2 \Rightarrow$ το 5 δεν είναι πρωταρχική ρίζα mod 8.
$7^2 \equiv (-1)^2 \equiv 1 \pmod 8 \Rightarrow \text{ord}_8 7 = 2 \Rightarrow$ το 7 δεν είναι πρωταρχική ρίζα mod 8.
Άρα δεν υπάρχουν πρωταρχικές ρίζες mod 8.

Αυτό σημαίνει ότι το πολυώνυμο $\Phi_8(X) = X^4 + 1$ δεν είναι ποτέ ανάγωγο στο GF(p) για κάθε πρώτο p.

Παρατήρηση: Το $\Phi_8(X)$ είναι ανάγωγο στο Q.

Στη συνέχεια θα προσπαθήσουμε να βρούμε ανάγωγους παράγοντες του $\Phi_n(X)$.

Πιο γενικά: Αν f(X) οποιοδήποτε πολυώνυμο του K[X], K=GF(q) θα περιγράψουμε αλγόριθμο (του Berlekamp) παραγοντοποίησης του f(X) σε γινόμενο ανάγωγων παραγόντων.

(6.12) Θεώρημα Αν f(X) μονικό πολυώνυμο με degf(x)=n όπου $f(X) \in K[X]$, K=GF(q) και αν $h(X) \in K[X]$, τέτοιο ώστε $h(X)^q \equiv h(X) \bmod f(X)$ τότε $f(X) = \prod_{s \in K} \text{ΜΚΔ}(f(X), h(X) - s)$.
(χωρίς απόδειξη)

Παρατήρηση Αν υπάρχει $s_0 \in K$ τέτοιο ώστε $h(X) \equiv s_0 \bmod f(X)$ τότε η παραγοντοποίηση του προηγούμενου θεωρήματος είναι τετριμμένη. Δηλαδή ένας παράγοντας είναι το f(X) και οι άλλοι είναι 1.

Το επόμενο θεώρημα θα μας δώσει ότι αν f(X) διαιρείται από δυο ή περισσότερα διακεκριμένα ανάγωγα πολυώνυμα τότε υπάρχει πολυώνυμο h(X) τέτοιο ώστε η παραγοντοποίηση του προηγούμενου θεωρήματος να μην είναι τετριμμένη.

Θεωρούμε τον δακτύλιο K[X]/<f(X)> σαν n-διάστατο K-διανυσματικό χώρο, V(f), όπου n=degf, με βάση $\{1,x,x^2,\ldots,x^{n-1}\}$.
Έστω $R(f)=\{h(X)\in K[X]$ τ.ω. $h(X)^q\equiv h(X) \bmod f(X)\}$.
Το R(f) είναι διανυσματικός υπόχωρος του V(f) διότι $[s_1h_1(X)+s_2h_2(X)]^q =$
$=s_1^qh_1(X)^q+s_2^qh_2(X)^q=s_1h_1(X)^q+s_2h_2(X)^q=s_1h_1(X)+s_2h_2(X) \mod f(X)$
Δηλαδή αν $h_1(X),h_2(X)\in R(f)\equiv s_1h_1(X)+s_2h_2(X) \mod f(X)$ και $s_1,s_2\in K$ τότε $s_1h_1(X)+s_2h_2(X)\in K$

(6.13) <u>Θεώρημα</u> Αν $f(X)=\prod_{i=1}^{m}P_i(X)^{l_i}$ όπου $P_i(X)$ διακεκριμένα ανά δύο, ανάγωγα μονικά πολυώνυμα τότε $\dim_K R(f)=m$

(χωρίς απόδειξη)

<u>Παρατήρηση</u>: Αν καταφέρουμε να υπολογίσουμε τη διάσταση του χώρου m, τότε γνωρίζουμε το πλήθος των ανάγωγων παραγόντων του f(X). (Θα είναι m)

(6.14) <u>Παράδειγμα</u>

Έστω $f(X)=X^4+X+1$ και q = 2 τότε $K=\mathbf{F}_2=GF(2)$
Αν $h(X)=h_0+h_1X+h_2X^2+h_3X^3$ τότε η συνθήκη $h(X)^q\equiv h(X) \bmod f(X)$ γράφεται
$h_0+h_1X^2+h_2X^4+h_3X^6\equiv h_0+h_1X+h_2X^2+h_3X^3 \bmod(X^4+X+1)$
Ισχύει ότι $X^4\equiv X+1 \bmod(X^4+X+1)$ οπότε και $X^6\equiv X^3+X^2 \bmod(X^4+X+1)$ και έχουμε ότι
$h(X)^2=h_0+h_1X^2+h_2(X+1)+h_3(X^3+X^2) \bmod(X^4+X+1)$.
Οπότε αν παραστήσουμε το πολυώνυμο $h(X)=h_0+h_1X+h_2X^2+h_3X^3$ με το διάνυσμα στήλη $[h_0,\ h_1,\ h_2,\ h_3]^\tau$ τότε $h(X)\in R(f) \Leftrightarrow h(X)^2\equiv h(X) \bmod f(X)$

$$\Leftrightarrow h_0\begin{bmatrix}1\\0\\0\\0\end{bmatrix}+h_1\begin{bmatrix}0\\0\\1\\0\end{bmatrix}+h_2\begin{bmatrix}1\\1\\0\\0\end{bmatrix}+h_3\begin{bmatrix}0\\0\\1\\1\end{bmatrix}\equiv h_0\begin{bmatrix}1\\0\\0\\0\end{bmatrix}+h_1\begin{bmatrix}0\\1\\0\\0\end{bmatrix}+h_2\begin{bmatrix}0\\0\\1\\0\end{bmatrix}+h_3\begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

Δηλαδή το $h(X)\in R(f)$ ισοδυναμεί με το ότι το διάνυσμα $(h_0,\ h_1,\ h_2,\ h_3)$ ανήκει στο χώρο μηδενισμού του πίνακα B, όπου

$$B=\begin{bmatrix}1&0&1&0\\0&0&1&0\\0&1&0&1\\0&0&0&1\end{bmatrix}-\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}=\begin{bmatrix}0&0&1&0\\0&-1&1&0\\0&1&-1&1\\0&0&0&0\end{bmatrix}=\begin{bmatrix}0&0&1&0\\0&1&1&0\\0&1&1&1\\0&0&0&0\end{bmatrix}$$

Κάνοντας στοιχειώδεις μετασχηματισμούς στον πίνακα B, συγκεκριμένα προσθέτοντας στη γραμμή 2 τη γραμμή 1 και στην γραμμή 3 τη γραμμή 2 φέρνουμε τον B στη μορφή:

$$B = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Επομένως $(h_0, h_1, h_2, h_3) \in R(f) \Leftrightarrow B \cdot \begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \end{bmatrix} = O \Leftrightarrow h_1 = h_2 = h_3 = 0$

Οι μοναδικές λύσεις που παίρνουμε είναι $[h_0\ 0\ 0\ 0]$. Όμως το h_0 είναι στοιχείο του $\mathbf{F}_2$ άρα οι λύσεις είναι [0 0 0 0] και [1 0 0 0].

Οπότε $\dim_K R(f) = 1$. Και από θεώρημα έπεται ότι το f(X) είναι δύναμη αναγώγου. Αλλά $f'(X) = 4X^3 + 1 = 1$. Δηλαδή f(X) ανάγωγο στο GF(2) σύμφωνα με το

(6.15) Θεώρημα

Έστω ένα πολυώνυμο $f(X) = P^{\lambda}(X)$, $\lambda \geq 2$ τότε $f'(X) = \lambda P^{\lambda-1}(X) P'(X)$ επομένως το P(X) διαιρεί τον ΜΚΔ($f'(X)$, f(X)).

Το θεώρημα είναι άμεση συνέπεια της γνωστής πρότασης, ότι αν ένα πολυώνυμο f(X) έχει ρίζα βαθμού πολλαπλότητας >1 τότε η ρίζα αυτή είναι και ρίζα της παραγώγου του.

(6.16) Παράδειγμα

Έστω ότι θέλουμε να παραγοντοποιήσουμε το $f(X)=X^5+X+1$ στο GF(2)
Αν $h(X) = h_0 + h_1X + h_2X^2 + h_3X^3 + h_4X^4$ τότε θέλουμε να έχουμε $h^2(X) \equiv h(X) \bmod (X^5+X+1)$.
Θα χρησιμοποιήσουμε τις ισοτιμίες:
$X^5 \equiv X+1 \bmod(X^5+X+1)$
$X^6 \equiv X^2+ X \bmod(X^5+X+1)$
$X^8 \equiv X^4+ X^3 \bmod(X^5+X+1)$
Η ισοδυναμία $h^q(X) \equiv h(X) \bmod f(X)$ (εδώ q=2) γράφεται

$$h_0\begin{bmatrix}1\\0\\0\\0\\0\end{bmatrix} + h_1\begin{bmatrix}0\\0\\1\\0\\0\end{bmatrix} + h_2\begin{bmatrix}0\\0\\0\\0\\1\end{bmatrix} + h_3\begin{bmatrix}0\\1\\1\\0\\0\end{bmatrix} + h_3\begin{bmatrix}0\\0\\0\\1\\1\end{bmatrix} \equiv h_0\begin{bmatrix}1\\0\\0\\0\\0\end{bmatrix} + h_1\begin{bmatrix}0\\1\\0\\0\\0\end{bmatrix} + h_2\begin{bmatrix}0\\0\\1\\0\\0\end{bmatrix} + h_3\begin{bmatrix}0\\0\\0\\1\\0\end{bmatrix} + h_3\begin{bmatrix}0\\0\\0\\0\\1\end{bmatrix}$$

(Οι συντελεστές h_i δεν αλλάζουν αφού κάθε $h_i \in GF(2)$ επαληθεύει την εξίσωση $X^q \equiv X \pmod q$ q=2).

Επομένως το διάνυσμα $h=[h_0, h_1, h_2, h_3, h_4]$ ανήκει στο χώρο μηδενισμού του πίνακα Β όπου

$$B=\begin{bmatrix}1&0&0&0&0\\0&0&0&1&0\\0&1&0&1&0\\0&0&0&0&1\\0&0&1&0&1\end{bmatrix}-\begin{bmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&1&0&1\end{bmatrix}=\begin{bmatrix}0&0&0&0&0\\0&1&0&1&0\\0&1&1&1&0\\0&0&0&1&1\\0&0&1&0&0\end{bmatrix}$$

Επομένως θα πρέπει $B\cdot h = \mathbf{0}$ δηλαδή

$$\begin{Bmatrix} h_1+h_3=0\\ h_1+h_2+h_3=0\\ h_3+h_4=0\\ h_2=0\end{Bmatrix} \text{ ή } \begin{Bmatrix} h_1+h_3=0\\ h_3+h_4=0\\ h_2=0\end{Bmatrix}$$

Η διάσταση του χώρου λύσεων είναι 2. Οπότε σύμφωνα με το γνωστό από τη Γραμμική Άλγεβρα Ι θεώρημα $\dim_K R(f)=2 \mid K=GF(2)$ και παράγεται από τα πολυώνυμα:

$[1\ 0\ 0\ 0\ 0]=1$ και $[0\ 1\ 0\ 1\ 1]=X+X^3+X^4$.

Επομένως, σύμφωνα με το Θεώρημα (6.13), το f(X) είναι γινόμενο δυο ανάγωγων πολυωνύμων πιθανόν σε κάποια δύναμη το καθένα.

Εύκολα επαληθεύεται ότι:
$ΜΚΔ(X^5+X+1, X^4+X^3+X) = X^3+X^2+1$
$ΜΚΔ(X^5+X+1, X^4+X^3+X+1) = X^2+X+1$
Επομένως, $X^5+X+1 = (X^3+X^2+1)(X^2+X+1)$.
Γνωρίζουμε ότι X^3+X^2+X και X^2+X+1 <u>ανάγωγα</u> στο GF(2).
Άρα η ανάλυση του f(X) σε γινόμενο ανάγωγων πολυωνύμων είναι $f(X) = X^5+X+1 = (X^3+X^2+1)(X^2+X+1)$.

Ο αλγόριθμος του Berlekamp μπορεί να απλοποιηθεί σημαντικά αν το πολυώνυμο που θέλουμε να παραγοντοποιήσουμε είναι της μορφής X^n-1 όπου $ΜΚΔ(n,q) = 1$.

Κατ' αρχήν το Θεώρημα (6.12) τροποποιείται ως εξής:

(6.17) <u>Θεώρημα</u>

Το πολυώνυμο $h(X) = \sum_{i=0}^{n-1} h_i X^i$ επαληθεύει την ισοδυναμία $h^q(X) \equiv h(X) \bmod(X^n-1)$ $\Leftrightarrow$ $h_{iq}=h_i$ για κάθε $i = 0,1,2,\ldots,n-1$ (όπου οι δείκτες θεωρούνται modulo n).

(χωρίς απόδειξη)

<u>Παρατήρηση</u>: Επειδή $ΜΚΔ(n, q) = 1$ η απεικόνιση $i \mapsto qi \pmod n$ είναι μια μετάθεση του συνόλου $\{0,1,2,\ldots,n-1\}$.

(6.18) <u>Παράδειγμα</u>

Για $q = 2$ και $n = 5$ έχουμε ότι $\{0,1,2,3,4\} \mapsto \{0,2,4,6,8\} \pmod 5 = \{0,2,4,1,3\}$.
Δηλαδή έχουμε τη μετάθεση:

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 2 & 4 & 1 & 3 \end{pmatrix}$$

(6.17) Παράδειγμα: Για q = 3 και n = 20 η μετάθεση που θα προκύψει σε γινόμενο κύκλων γράφεται: (0)(1 3 9 7)(2 6 18 14)(4 12 16 8)(5 15)(10)(11 13 19 17).

Σύμφωνα με το Θεώρημα (6.17) κάθε πολυώνυμο h(X) που επαληθεύει την ισοδυναμία $h^3(X) \equiv h(X) \bmod(X^{20} - 1)$ θα πρέπει να είναι GF(3)-γραμμικός συνδυασμός των ακόλουθων 7 πολυωνύμων:

$h_0 = 1$
$h_1(X) = X + X^3 + X^9 + X^7$
$h_2(X) = X^2 + X^6 + X^{18} + X^{14}$
$h_4(X) = X^4 + X^{12} + X^{16} + X^8$
$h_5(X) = X^5 + X^{15}$
$h_{10}(X) = X^{10}$
$h_{11}(X) = X^{11} + X^{13} + X^{19} + X^{17}$

Οι κύκλοι των μεταθέσεων $i \mapsto qi \bmod n$ λέγονται **κυκλοτομικά cosets**.

Μελετάμε το πολυώνυμο $f(X)=X^{20}-1$στο σώμα GF(3). Η τάξη του 3 modulo 20 είναι 4 αφού $3^4 \equiv 1 \pmod{20}$. Επομένως αν περάσουμε στο σώμα $GF(3^4) = GF(81)$ τότε αυτό θα έχει ένα στοιχείο τάξης 20, δηλαδή $X^{20} - 1 = \prod_{j=0}^{19}(X - \alpha^j)$, όπου α ένα στοιχείο τάξης 20 του GF(81).
Έχουμε ήδη δει ότι η παραγοντοποίηση του $X^{20}-1$ στο GF(3) καθορίζεται από την παραγοντοποίηση του $X^{20}-1$ στο GF(81).
Έστω για παράδειγμα ότι το ελάχιστο πολυώνυμο του α στο σώμα GF(3) είναι το $f_1(X) = (X - \alpha)(X - \alpha^3)(X - \alpha^9)(X - \alpha^7)$

Επειδή για κάθε i = 1, 3, 7, 9 έχουμε ότι (i, 20) = 1 έπεται ότι τα στοιχεία α^i για κάθε i = 1, 3, 7, 9 είναι επίσης τάξης 20. Επομένως το $f_1(X)$ είναι ανάγωγος παράγοντας όχι μόνο του $X^{20}-1$ αλλά και του $\Phi_{20}(X)$.

Ομοίως αν $f_i(X)$ είναι το ελάχιστο πολυώνυμο του α^i τότε το $f_i(X)$ είναι και ανάγωγο πολυώνυμο του $\Phi_{n/MK\Delta(n,i)}(X)$.

Αν τώρα συμβολίσουμε το κυκλοτομικό coset που περιέχει το i με C_i φτιάχνουμε τον ακόλουθο πίνακα:

i	C_i	$\lvert C_i\rvert = \deg f_i(X)$	$\frac{20}{MK\Delta(20,i)}$
0	0	1	1
1	(1, 3, 9, 7)	4	20
2	(2, 6, 18, 14)	4	10
4	(4, 12, 16, 8)	4	5
5	(5, 15)	2	4
10	(10)	1	2
11	(11, 13, 19, 17)	4	20

Με τη βοήθεια του παραπάνω πίνακα μπορούμε να φτιάξουμε τον πίνακα των παραγόντων του $X^{20}-1$ οι οποίοι δίνονται μέσω τον κυκλοτομικών πολυωνύμων $\Phi_d(X)$ όπου d | 20.

d	$\Phi_d(X)$	παράγοντες
1	$X-1$	$f_1(X)$ ανάγωγο
2	$X+1$	$f_{10}(X) = X - \alpha^{10}$ ανάγωγο
4	X^2+1	$f_5(X)$ ανάγωγο
5	$X^4+X^3+X^2+X+1$	$f_4(X)$ ανάγωγο
10	$X^4-X^3+X^2-X+1$	$f_2(X)$ ανάγωγο
20	$X^8-X^6+X^4-X^2+1$	$f_1(X)f_{11}(X)$

Μόνο το $\Phi_{20}(X)$ δεν παραγοντοποιείται πλήρως σε γινόμενο αναγώγων για αυτό εφαρμόζουμε και πάλι τον αλγόριθμο του Berlekamp. Για κάθε $h_i(X)$ ισχύει:

$$X^{20}-1 = \text{ΜΚΔ}(X^{20}-1, h_i(X))\ \text{ΜΚΔ}(X^{20}-1, h_i(X)+1)\ \text{ΜΚΔ}(X^{20}-1, h_i(X)+2)$$

Επειδή $\Phi_{20}(X) | X^{20}-1$ έπεται ότι $h^3(X) \equiv h(X) \bmod \Phi_{20}(X)$. Οπότε,
$\Phi_{20}(X) = \text{ΜΚΔ}(\Phi_{20}(X), h_i(X))\ \text{ΜΚΔ}(\Phi_{20}(X), h_i(X)+1)\ \text{ΜΚΔ}(\Phi_{20}(X), h_i(X)+2) = 1\cdot(X^4+X^3+2X+1)(X^4+2X^3+X+1)$.

Έτσι παραγοντοποιήσαμε πλήρως το $X^{20}-1$ σε γινόμενο ανάγωγων πολυωνύμων.

Προτού κλείσουμε το κεφάλαιο και ασχοληθούμε με την κωδικοποίηση, θα αναφερθούμε σε μια μέθοδο κατασκευής των στοιχείων πεπερασμένου σώματος $\mathbf{F}_q$ όπου $q = p^n$ για κάποιο πρώτο p και κάποιο ακέραιο n, όταν γνωρίζουμε ένα ανάγωγο πολυώνυμο $f(X) \in \mathbf{F}_q[X]$ βαθμού n χωρίς να κάνουμε τον πολλαπλασιασμό mod f(X).

Έστω $f(X) = f_0 + f_1X + \ldots + f_nX^n$.

Θεωρώ τον **«κανόνα»** (slider): $[-f_0, -f_1, \ldots, -f_{n-1}, \uparrow]$.

Αν α ρίζα του f(X), τότε το α είναι γεννήτορας της κυκλικής ομάδας $\mathbf{F}_q^*$ ενώ το σύνολο $\{1, \alpha, \ldots, \alpha^{n-1}\}$ αποτελεί μια βάση του $\mathbf{F}_p$-διανυσματικού χώρου $\mathbf{F}_q$ διάστασης n.

Το πως λειτουργεί ο αλγόριθμος, θα το δείξουμε σε παραδείγματα.

(6.18) Παράδειγμα 1 Αν $K = \mathbf{F}_2$ και $F = \mathbf{F}_8$, όπου $8 = 2^3$. Ένα ανάγωγο πολυώνυμο βαθμού 3 στο K[X] είναι το $f(X) = 1 + X + X^3$. Ο κανόνας είναι $[1, 1, 0, \uparrow]$.

Φτιάχνουμε τον πίνακα:

	$\alpha^0 = 1$	α^1	α^2	α^3	α^4	α^5	α^6
1	1	0	0	1	0	1	1
α	0	1	0	1	1	1	0
α^2	0	0	1	0	1	1	1
	1	1	0	↑			
		1	1	0	↑		
			1	1	0	↑	
				1	1	0	↑

Πολλαπλασιάζω τον κανόνα με κάθε γραμμή κατά συντεταγμένες και υπολογίζω τη στήλη που μου δείχνει το βέλος ↑ .

(6.19) Παράδειγμα 2 Αν $K = \mathbf{F}_3$ και $F = \mathbf{F}_9$, όπου $9 = 3^2$. Ένα ανάγωγο πολυώνυμο βαθμού 2 στο K[X] είναι το $f(X) = 2 + X + X^2$. Ο κανόνας είναι [1, 2, ↑].

Φτιάχνουμε τον πίνακα:

	$\alpha^0 = 1$	α^1	α^2	α^3	α^4	α^5	α^6	α^7
1	1	0	1	2	2	0	2	1
α	0	1	2	2	0	2	1	1
	1	2	↑					
		1	2	↑				
			1	2	↑			
				1	2	↑		
					1	2	↑	
						1	2	↑

(Βλέπε Holder – Schellwat, A simple slide rule for finite fields, American Math monthly, τόμος 108, April 2001).

Κεφάλαιο 7

Στοιχεία θεωρίας κωδικοποίησης

(7.1) Ορισμός

(i) **Αλφάβητο** ονομάζεται το πεπερασμένο σύνολο των συμβόλων (πολλές φορές θα τα ονομάζουμε **γράμματα**) που χρησιμοποιούμε για να καταγράψουμε-διατυπώσουμε ένα μήνυμα. Το αλφάβητό μας, σε αυτό το κεφάλαιο, θα είναι το πεπερασμένο σώμα $\mathbf{F}_q$.
(ii) Ένα **k-μήνυμα** αποτελείται από μια ακολουθία γραμμάτων των αλφαβήτου μας μήκους k. Είναι δηλαδή της μορφής: $a_1, a_2 \ldots, a_k$ με $a_i \in \mathbf{F}_q$.
(iii) Η αντίστοιχη **κωδική λέξη** x ενός k-μηνύματος είναι μια ακολουθία μήκους n. Είναι δηλαδή της μορφής $x = x_1, x_2 \ldots, x_n$ με $x_i \in \mathbf{F}_q$ και $n \geq k$. Όπου (σχεδόν) πάντα θα ισχύει ότι $x_1 = a_1$, $x_2 = a_2$, …, $x_k = a_k$ ενώ τα υπόλοιπα n – k σύμβολα $(x_{k+1}, x_{k+2}, \ldots, x_n)$ θα τα λέμε **σύμβολα ελέγχου** (**check symbols** ή **control symbols**).

(7.2) Συμβολισμός Οι κωδικές λέξεις θα γράφονται x ή $x_1, x_2, \ldots, x_n$ ή $(x_1, x_2, \ldots, x_n)$ ή $x_1x_2\ldots x_n$.

(7.3) Ορισμός Θα ονομάζουμε **διάνυσμα λήψης** (ή **μήνυμα λήψης**) το διάνυσμα $y = y_1, y_2, \ldots, y_n$ που λαμβάνουμε. Το y εν γένει είναι διαφορετικό από το μήνυμα x που μας στέλνουνε. Το $e := y - x = e_1e_2\ldots e_n$ θα λέγεται **διάνυσμα λάθους** (ή απλά **λάθος**).

(7.4) Ορισμός Ένας **n-κώδικας** C είναι ένα υποσύνολο του $\mathbf{F}_q^n$. Ακριβέστερα ο κώδικας θα λέγεται **(n, k)-κώδικας**, όπου k το μήκος του μηνύματος που κωδικοποιούμε. Αν ο κώδικας C είναι $\mathbf{F}_q$-διανυσματικός υπόχωρος του $\mathbf{F}_q^n$ τότε θα λέγεται **(n, k)-γραμμικός κώδικας**. Τα στοιχεία του C θα είναι οι κωδικές λέξεις.

(7.5) Παραδείγματα

(i) Έστω C = {000, 001, 010, 011} υποσύνολο του $\mathbf{F}_2^3$. Ο C αποτελείται από ακριβώς αυτές τις κωδικές λέξεις που έχουν σαν πρώτο στοιχείο το 0 και εύκολα φαίνεται ότι ο C είναι ένας γραμμικός 3-κώδικας.
(ii) Επίσης, το C = {00, 11, 22} αποτελεί ένα γραμμικό 2-κώδικα του $\mathbf{F}_3^2$.

Όταν πάρουμε το y θα πρέπει να αποφασίσουμε ποια κωδική λέξη μας έχουν στείλει. Θα διαλέγουμε από το σύνολο C την κωδική λέξη που διαφέρει λιγότερο από το y. Αυτό ονομάζεται **αποκωδικοποίηση μέγιστης πιθανότητας**.

(7.6) Ορισμός **Απόσταση Hamming** d(x, y) δύο διανυσμάτων x, y στο $\mathbf{F}_q^n$, με

$$x = x_1, x_2 \ldots, x_n \text{ και } y = y_1, y_2 \ldots, y_n,$$

είναι το πλήθος των συντεταγμένων στις οποίες τα x και y διαφέρουν. Δηλαδή

$$d(x, y) = \#\{i \in \mathbf{N},\ 1 \le i \le n \mid x_i \neq y_i\}$$

(7.7) Ορισμός **Βάρος (weight) Hamming** w(x) ενός διανύσματος $x = x_1, x_2 \ldots, x_n$ στο $\mathbf{F}_q^n$ είναι το πλήθος των μη-μηδενικών συντεταγμένων του x. Δηλαδή,

$$w(x) = \#\{i \in \mathbf{N},\ 1 \le i \le n \mid x_i \neq 0\}$$

Προφανώς, w(x) = d(x, 0).

(7.8) Παράδειγμα Έστω $C \subseteq \mathbf{F}_3^4$.

Το βάρος Hamming του 1201 είναι w(1201) = 3.
Η απόσταση Hamming των 1201 και 2211 είναι d(1201, 2211) = 2.

(7.9) Παρατήρηση Η απόσταση Hamming d(C) είναι μια μετρική στον $\mathbf{F}_q^n$ και το βάρος Hamming w είναι μια νόρμα στον $\mathbf{F}_2^n$.

(7.10) Ορισμός Αν $C \subseteq \mathbf{F}_q^n$ ένας (n, k)-κώδικας, **η ελάχιστη απόσταση $d_{min}(C)$ του κώδικα** είναι

$$d_{min}(C) = \min_{\substack{u,v \in C \\ u \neq v}} d(u, v)$$

Άρα, όταν παίρνουμε το y πρέπει να ελέγχουμε τις q^k κωδικές λέξεις για να βρούμε ποια έχει την μικρότερη απόσταση Hamming από το y. Προφανώς, αυτή η διαδικασία είναι αδύνατη για μεγάλα k και ένα από τους στόχους της θεωρίας κωδίκων είναι να βρει κώδικες με γρηγορότερους αλγόριθμους αποκωδικοποίησης.

Το επόμενο αποτέλεσμα μας δείχνει ότι για κάθε γραμμικό κώδικα, η ελάχιστη απόσταση μπορεί να υπολογισθεί από το βάρος Hamming των κωδικών λέξεων.

Μια από τις πιο σημαντικές ιδιότητες των γραμμικών κωδίκων είναι η παρακάτω

(7.11) Πρόταση Έστω C ένας γραμμικός (n, k)-κώδικας. Η ελάχιστη απόσταση του C είναι ίση με το ελάχιστο δυνατό βάρος που έχει κωδική λέξη διάφορη του μηδενικού στοιχείου.

Απόδειξη Έστω w το ελάχιστο δυνατό βάρος Hamming κωδικής λέξης διάφορης του μηδενικού στοιχείου 0. Έστω $x \in C$ μια κωδική λέξη βάρους Hamming w. Τότε ισχύει ότι d(x, 0) = w(x) = w. Επομένως, ισχύει ότι $w \ge d_{min}(C)$. Τώρα έστω u και v ένα ζευγάρι κωδικών λέξεων του C με απόσταση τέτοια ώστε $d(u, v) = d_{min}(C)$. Αφού C γραμμικός κώδικας έπεται ότι και η u – v είναι επίσης κωδική λέξη. Η u – v έχει βάρος $d_{min}(C)$. Επομένως, $d_{min}(C) \ge w$. Δηλαδή, $d_{min}(C) = w$.

(7.12) Ορισμός Το σύνολο $S_r(x) := \{y \in \mathbf{F}_q^n \mid d(x, y) \leq r\}$ θα λέγεται η **σφαίρα ακτίνας r ως προς το x** $\in \mathbf{F}_q^n$.

(7.13) Παράδειγμα Έστω $C = \mathbf{F}_2^3$ τότε ο κύκλος με ακτίνα 1 ως προς το 100 είναι

$$S_1(100) = \{100,000,110,101\}.$$

Στόχος Παίρνοντας σφαίρες κατάλληλης ακτίνας r κέντρου κωδικής λέξης θα πρέπει κατά το δυνατό να καλύπτει η ένωσή τους όλο το χώρο $\mathbf{F}_q^n$ ώστε να μπορούμε να αποκωδικοποιούμε όλα τα κωδικοποιημένα μηνύματα που λαμβάνουμε ενώ συγχρόνως η ακτίνα r θα πρέπει να είναι αρκετά μικρή ώστε οι σφαίρες να μην τέμνονται (ή εφάπτονται) και να μπορούμε να αποκωδικοποιούμε μονοσήμαντα.

Πρέπει πάντως να ισχύει ότι $r < \frac{1}{2} d_{min}(C)$.

Η σημασία της ιδέας της ελάχιστης απόστασης δίνεται από την

(7.14) Πρόταση Υποθέτουμε ότι ο C είναι γραμμικός κώδικας με ελάχιστη απόσταση $d_{min}(C) = d$. Ο C **ανιχνεύει** την ύπαρξη d – 1 ή λιγότερων λαθών και **διορθώνει** e λάθη για κάθε e τέτοιο ώστε $2e + 1 \leq d$.

Απόδειξη Έστω ότι λάβαμε το μήνυμα y με απόσταση f από την κωδική λέξη x, όπου $f \leq d–1$. Φανταζόμαστε ότι η x είναι η μεταδιδόμενη (αρχική) λέξη και y η λέξη που πήραμε τελικά. Δηλαδή έχουμε f λάθη κατά την μεταφορά. Επειδή d είναι η ελάχιστη απόσταση του C η λέξη y καταλαβαίνουμε αμέσως ότι δεν μπορεί να είναι κωδική λέξη. Δηλαδή, ο κώδικας C ανακαλύπτει d – 1 ή λιγότερα λάθη.

Αν τώρα το μήνυμα y έχει απόσταση e από την κωδική λέξη x και $2e + 1 \leq d$ τότε δεν υπάρχει άλλη κωδική λέξη πιο κοντά στη y, διότι αν $d(y, x_1) \leq e$ για κάποια x_1 τότε θα ίσχυε

$$d(x, x_1) \leq d(x, y) + d(y, x_1) \leq e + e < d$$

άτοπο, διότι η ελάχιστη απόσταση του κώδικα C είναι d. Επομένως, υπάρχει μοναδική κοντινότερη λέξη του y και συνεπώς ο C διορθώνει e λάθη σ’ αυτήν την περίπτωση.

Ένα από τα βασικά προβλήματα στη θεωρία κωδίκων είναι να ελαχιστοποιηθούν τα λάθη αλλά χωρίς να μειωθεί υποχρεωτικά **η αναλογία της πληροφορίας** $\frac{k}{n}$.

Κεντρικό πρόβλημα της Θεωρίας Κωδίκων είναι το εξής:

Δίνονται d, n *φυσικοί αριθμοί. Να υπολογιστεί ο μέγιστος αριθμός διανυσμάτων, έστω* A(n, d*), του διανυσματικού χώρου* $\mathbf{F}_2^n$ *τα οποία ανά δυο να έχουν απόσταση μεγαλύτερη ή ίση με* d*. Φυσικά, αν είναι δυνατόν να βρεθούν τα διανύσματα.*

Ο επόμενος πίνακας μας δίνει κάποιες τιμές του A(n, d) για d = 3

n	3	4	5	6	7	8	9	10
A(n, 3)	2	2	4	8	16	20	40	άγνωστος, μεταξύ 72 και 79

(7.15) Ορισμός Ένας κώδικας C ο οποίος **διορθώνει** την ύπαρξη t λαθών θα λέγεται **t-κώδικας διόρθωσης λαθών** (**t-error-correcting code**), ενώ ένας κώδικας C που **ανιχνεύει** e λάθη θα λέγεται **e-κώδικας ανίχνευσης λαθών** (**e-error-detecting code**).

Έστω τώρα C κώδικας ως προς το $\mathbf{F}_q$ μήκους n με πλήθος κωδικών λέξεων M. Υποθέτουμε ότι ο κώδικας είναι ένας t-κώδικας διόρθωσης λαθών. Υπάρχουν $\binom{n}{m}$ διανύσματα του $\mathbf{F}_q^n$ τα οποία να έχουν βάρος m στο $\mathbf{F}_q$. Αν $c \in C$ τότε μέσα στην σφαίρα $S_t(c)$ υπάρχουν $1 + (q-1)\binom{n}{1} + \ldots + (q-1)^t\binom{n}{t}$ διανύσματα του $\mathbf{F}_q^n$.

(7.16) Θεώρημα (Φράγμα του Hamming) Οι παράμετροι q, n, t, M ενός t-κώδικα διόρθωσης λαθών C ορισμένου στο σώμα $\mathbf{F}_q$ μήκους n με M κωδικές λέξεις ικανοποιούν την ανισότητα

$$M\left(1 + (q-1)\binom{n}{1} + \ldots + (q-1)^t\binom{n}{t}\right) \le q^n.$$

Αν όλα τα διανύσματα του $\mathbf{F}_q^n$ είναι μέσα σε σφαίρες ακτίνας t κέντρου κωδικών λέξεων ενός (n, k)-γραμμικού κώδικα τότε παίρνουμε μια ειδική κατηγορία κωδίκων:

(7.17) Ορισμός Ένας t-κώδικας διόρθωσης λαθών ορισμένος στο σώμα $\mathbf{F}_q$ θα ονομάζεται **τέλειος** αν στο θεώρημα 7.16 ισχύει η ισότητα.

Αν ο C είναι κώδικας όπως αυτός του θεωρήματος 7.16 με $d_{min}(C) = d = 2t + 1$, τότε αν διαγράψουμε τα τελευταία d – 1 σύμβολα πάλι έχουμε έναν κώδικα με όλες τις κωδικές λέξεις διαφορετικές. Ο κώδικας που προκύπτει έχει μήκος n – d + 1, και παίρνουμε το

(7.18) Θεώρημα (Φράγμα του Singleton) Αν ένας κώδικας $C \subseteq \mathbf{F}_q^n$ έχει ελάχιστη απόσταση d, τότε $|C| \le q^{n-d+1}$ ή αλλιώς $k \le n - d + 1$.

(7.19) Ορισμός Ένας κώδικας C θα λέγεται **διαχωρίσιμος μέγιστης απόστασης** (**maximum distance separable**) ή πιο απλά **κώδικας MDS** αν στο θεώρημα 7.18 ισχύει η ισότητα.

(7.20) Παράδειγμα Έστω ο κώδικας

$$C = \{000000, 001011, 010101, 011110, 100110, 101101, 110011, 111000\} \subseteq \mathbf{F}_2^6$$

όπου $d_{min}(C) = 3$. Έχουμε επομένως, $M = 8$, $q = 2$, $n = 6$, $d = 3$, $t = 1$. Το φράγμα του Hamming δίνει την ανισότητα $8\left(1+\binom{6}{1}\right) \leq 2^6$, δηλαδή $56 < 64$. Αυτό σημαίνει ότι μόνο $64 - 56 = 8$ λέξεις μήκους 6 στο $\mathbf{F}_2^6$ βρίσκονται έξω από κάποια σφαίρα και δεν μπορούν να διορθωθούν σωστά (αυτό είναι προφανές και από το γεγονός ότι έχουμε 8 μη τεμνόμενες σφαίρες με 7 στοιχεία η κάθε μια). Ένα παράδειγμα μιας από τις 8 λέξεις που δεν μπορούν να διορθωθούν σωστά είναι η 111111 η οποία έχει απόσταση μεγαλύτερη ή ίση του 2 από όλες τις κωδικές λέξεις. Το φράγμα του Singleton μας δίνει $8 \leq 2^4 = 16$, άρα ο C δεν είναι MDS.

Ας υποθέσουμε τώρα ότι τα σύμβολα ελέγχου μπορούν να προκύψουν από το k-μήνυμα με τέτοιο τρόπο ώστε οι κωδικές λέξεις x να ικανοποιούν το σύστημα με γραμμικές εξισώσεις

$$Hx^T = 0,$$

όπου H είναι ένας δοσμένος $(n - k) \times n$ πίνακας με στοιχεία από το σώμα $\mathbf{F}_q$. Η **κανονική μορφή** για τον H είναι $[A \mid I_{n-k}]$ όπου A ένας $(n - k) \times k$ πίνακας και I_{n-k} ο $(n - k) \times (n - k)$ μοναδιαίος πίνακας.

Προκύπτει ο παρακάτω

(7.21) Ορισμός Έστω H ένας $(n - k) \times n$ πίνακας με βαθμό $n - k$ και στοιχεία από το σώμα $\mathbf{F}_q$. Το σύνολο όλων των n-διάστατων διανυσμάτων x που ικανοποιούν την εξίσωση $Hx^T = 0$ ονομάζονται **γραμμικός κώδικας** C πάνω από το $\mathbf{F}_q$ με **μήκος** n. Ο πίνακας H είναι ο **πίνακας ελέγχου ισοτιμίας (parity-check matrix)** του κώδικα.C ο οποίος ονομάζεται και γραμμικός (n, k)-κώδικας. Αν ο H είναι στην μορφή $[A \mid I_{n-k}]$ τότε τα πρώτα k σύμβολα από την κωδική λέξη x είναι το αρχικό k-μήνυμα, ενώ τα υπόλοιπα $n - k$ σύμβολα του x είναι τα σύμβολα ελέγχου. Ο C ονομάζεται επίσης **συστηματικός γραμμικός (n, k)-κώδικας** και τότε θεωρούμε ότι ο H είναι στην **κανονική μορφή**. Αν $q = 2$ τότε ο C ονομάζεται **δυαδικός κώδικας** (**binary code**).

(7.22) Παρατήρηση Το σύνολο C των λύσεων x της $Hx^T = 0$ (ή αλλιώς ο **μηδενόχωρος** του H) είναι ένας υπόχωρος του διανυσματικού χώρου $\mathbf{F}_q^n$ με διάσταση k. Επειδή οι κωδικές λέξεις είναι προσθετική ομάδα, ο C ονομάζεται επίσης **κώδικας-ομάδα**.

(7.23) Παράδειγμα (**Κώδικας Επανάληψης**) Αν κάθε κωδική λέξη ενός κώδικα C αποτελείται από ένα μόνο σύμβολο $a_1 \in \mathbf{F}_q$ και τα υπόλοιπα n–1 σύμβολα ελέγχου $x_2 = \ldots = x_n$ είναι όλα ίσα με a_1 (Το a_1 επαναλαμβάνεται άλλες n–1 φορές) τότε λαμβάνουμε έναν δυαδικό (n, 1)-κώδικα με πίνακα ελέγχου ισοτιμίας

$$H = \begin{bmatrix} 1 & 1 & 0 & \dots & 0 \\ 1 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \dots & 1 \end{bmatrix}$$

Υπάρχουν μόνο δύο κωδικές λέξεις σε αυτόν τον κώδικα. Οι λέξεις 00…0 και 11…1.

Στους κώδικες επανάληψης μπορούμε, φυσικά, να χρησιμοποιήσουμε κωδικές λέξεις με περισσότερα από ένα σύμβολα για το αρχικό μήνυμα. Αν για παράδειγμα μεταδώσουμε ένα μήνυμα μήκους k τρεις φορές και συγκρίνουμε τις αντίστοιχες «συντεταγμένες» x_i, x_{k+i}, x_{2k+i} της κωδικής λέξης

$$x_1 \dots x_i \dots x_k x_{k+1} \dots x_{k+i} \dots x_{2k} x_{2k+1} \dots x_{2k+i} \dots x_{3k},$$

τότε ποιο ήταν το k-μήνυμα που στάλθηκε το αποφασίζουμε με το «πλειοψηφικό σύστημα», δηλαδή αν $x_i = x_{k+i} \neq x_{2k+i}$, τότε μάλλον έχει σταλεί το x_i και όχι το x_{2k+i}. Είναι συχνά πάντως μη πρακτικό, δύσκολο ή πολύ δαπανηρό να στέλνουμε το αρχικό μήνυμα πάνω από μία φορά.

Είδαμε, ότι σε ένα συστηματικό κώδικα, ένα μήνυμα $a = a_1, \dots, a_k$ κωδικοποιείται σε ένα κωδικό μήνυμα $x = x_1, \dots, x_n$ με $x_1 = a_1, x_2 = a_2, \dots, x_k = a_k$. Οι εξισώσεις ελέγχου $[A \mid I_{n-k}]x^T = 0$ δίνονται από το σύστημα

$$\begin{pmatrix} x_{k+1} \\ \vdots \\ x_n \end{pmatrix} = -A \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = -A \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}$$

από όπου παίρνουμε

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{bmatrix} I_k \\ -A \end{bmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}$$

το οποίο γράφεται και στη μορφή

$$(x_1, \dots, x_n) = (a_1, \dots, a_k)\,[I_k \mid -A^T].$$

(7.24) Ορισμός Ο πίνακας $G = [I_k \mid -A^T]$ ονομάζεται (**κανονικός**) **γεννήτορας πίνακας** (ή **κανονικός βασικός πίνακας** ή **πίνακας κωδικοποίησης**) του γραμμικού (n, k)-κώδικα με πίνακα ελέγχου ισοτιμίας $H = [A \mid I_{n-k}]$ στην κανονική μορφή.

Ισχύει: $GH^T = 0$.

(7.25) Παραδείγματα

(1) Έστω $G = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$.

Ο γραμμικός (2,3)-κώδικας $C \subseteq \mathbf{F}_2^3$ αποτελείται από όλους τους συνδυασμούς των δυο γραμμών:

$$000,\ 101,\ 011,\ 110$$

Οι κωδικές λέξεις μπορούν να περιγραφούν σαν διανύσματα της μορφής uG, όπου u = 00, 01, 10, 11. Κάθε κωδική λέξη, διάφορη της μηδενικής, έχει βάρος ίσο με 2. Αυτό σημαίνει ότι ο κώδικας ανιχνεύει μέχρι 1 λάθος, αλλά δεν διορθώνει λάθη.

(2) Αν $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$.

Από τις τρεις γραμμές του πίνακα παίρνουμε τον (3, 6)-κώδικα $C \subseteq \mathbf{F}_2^6$ ο οποίος αποτελείται από 8 κωδικές λέξεις:

$$000000,\ 100110,\ 010101,\ 001011,\ 110011,\ 011110,\ 101101,\ 111000$$

Όπως και πριν κάθε κωδική λέξη x μπορεί να περιγραφεί σαν διανύσματα της μορφής $x = uG$, όπου $u = u_1u_2u_3$ με $u_i \in \mathbf{F}_2$.

Υπάρχουν τέσσερις κωδικές λέξεις βάρους 3, τρεις κωδικές λέξεις βάρους 4 και μια κωδική λέξη βάρους 0. Η ελάχιστη απόσταση του κώδικα είναι 3, επομένως ανακαλύπτει δύο λάθη και διορθώνει ένα λάθος.

(3) Αν $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$.

τότε ο κώδικας $C \subseteq \mathbf{F}_3^{12}$ αποτελείται από κωδικές λέξεις x όπου η κάθε μια μπορεί να περιγραφεί σαν διάνυσμα της μορφής $x = uG$, όπου $u = u_1u_2u_3u_4u_5u_6$ με $u_i \in \mathbf{F}_3$.
Η ελάχιστη απόσταση του κώδικα είναι το πολύ 5, αφού υπάρχει ήδη γραμμή του πίνακα G βάρους 5. Μπορεί να αποδειχθεί ότι ο κώδικας έχει ελάχιστη απόσταση ακριβώς 5. Ο κώδικας αυτός ονομάζεται **κώδικας Golay**.

Για περισσότερες πληροφορίες για τους κώδικες Golay παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στο F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Code, North-Holland Mathematical Library, Sixth printing: 1988, κεφάλαιο 20.

(7.26) Θεώρημα Έστω G ο γεννήτορας πίνακας ενός γραμμικού κώδικα C. Τότε οι γραμμές του G σχηματίζουν μια βάση του C.

Απόδειξη Οι k γραμμές του πίνακα G είναι γραμμικώς ανεξάρτητες από τον ορισμό του γεννήτορα πίνακα ενός γραμμικού κώδικα. Αν r είναι ένα διάνυσμα-γραμμή του G τότε $rH^T = 0$ άρα και $Hr^T = 0$ για κάθε $r \in C$. τώρα, dimC είναι η διάσταση του μηδενόχωρου του H, η οποία είναι n – rank(H) = k. Επομένως, οι k γραμμές του G σχηματίζουν μια βάση του C.

Ένας κώδικας μπορεί να έχει πολλούς πίνακες ελέγχου ισοδυναμίας και γεννήτορες πίνακες. Κάθε $k \times n$ πίνακας του οποίου ο χώρος γραμμών είναι ίσος με τον C μπορεί να είναι ο γεννήτορας πίνακας του C.

Αν ο «γεννήτορας πίνακας» H δεν είναι στην κανονική μορφή μπορούμε να τον μετατρέψουμε σε ένα πίνακα της μορφής $[I_k \mid -A^T]$ χωρίς να αλλάξουμε τον μηδενόχωρο του H, δηλαδή τον κώδικα C. Μετά μετατρέπουμε τις συντεταγμένες για να σχηματίσουμε τον πίνακα H' ο οποίος να είναι σε κανονική μορφή. Οι συντεταγμένες του κώδικα C' που αντιστοιχεί στον H' είναι «ισοδύναμος» με τον C με την ακόλουθη έννοια:

(7.27) Ορισμός Δύο κώδικες C και C' ίδιου μήκους n θα λέγονται **ισοδύναμοι** αν υπάρχει μια μετάθεση π του συνόλου {1, 2, …, n} τέτοια ώστε

$$(x_1, \ldots, x_n) \in C \Leftrightarrow \left(x_{\pi(1)}, \ldots, x_{\pi(n)}\right) \in C'$$

Έτσι, σχηματίζουμε τον γεννήτορα πίνακα G' του πίνακα C' και ύστερα εφαρμόζουμε την αντίστροφη μετάθεση π^{-1} στις συντεταγμένες.

Ας αναφέρουμε έναν ορισμό που θα μας χρειαστεί σε επόμενη παράγραφο:

(7.28) Ορισμός Ένα γραμμικός κώδικας C μήκους n, διάστασης k και ελάχιστης απόστασης d θα ονομάζεται **(n, k, d)-κώδικας**.

Έστω τώρα, $u = u_1, \ldots, u_n$ και $v = v_1, \ldots, v_n$ δύο διανύσματα του διανυσματικού χώρου $\mathbf{F}_q^n$ και έστω $u \cdot v = u_1v_1 + \ldots + u_nv_n$ να συμβολίζει το γινόμενο των u και v πάνω από τον $\mathbf{F}_q^n$. Αν $u \cdot v = 0$ τότε τα u και v θα λέγονται **ορθογώνια**.

(7.29) Ορισμός Έστω C ένας γραμμικός (n, k)-κώδικας ορισμένος στο σώμα $\mathbf{F}_q$. Ο **ορθογώνιος κώδικας** $C^\perp$ του κώδικα C ορίζεται να είναι ο

$$C^\perp = \{u \mid uv = 0 \text{ για κάθε } v \in C\}$$

Επειδή ο C είναι ένας k-διάστατος υπόχωρος του n-διάστατου διανυσματικού χώρου $\mathbf{F}_q^n$ το ορθογώνιο συμπλήρωμα του C είναι διάστασης n – k και είναι ένας (n, n – k) κώδικας. Μπορεί να αποδειχτεί ότι αν ο κώδικας C έχει γεννήτορα τον πίνακα G και πίνακα ελέγχου ισοτιμίας H τότε ο $C^\perp$ έχει γεννήτορα πίνακα τον H και πίνακα ελέγχου ισοτιμίας του G. Η ορθογωνιότητα των δύο κωδίκων μπορεί να εκφραστεί

από τη σχέση $GH^T = HG^T = 0$. Τώρα θα συνοψίσουμε κάποιες απλές ιδιότητες των γραμμικών κωδίκων.

(7.30) Παρατήρηση Έστω mld(H) ο ελάχιστος αριθμός γραμμικά εξαρτημένων στηλών του H. Επειδή οποιεσδήποτε rank(H) + 1 το πλήθος στήλες του H είναι γραμμικά εξαρτημένες προφανώς ισχύει, $mld(H) \leq rank(H) + 1$ για κάθε πίνακα H.

(7.31) Θεώρημα Έστω H ένας πίνακας ελέγχου ισοδυναμίας ενός (n, k, d)-κώδικα C με $n > k$. Τότε ισχύουν:

(i) $dimC = k = n - rank(H)$
(ii) $d = mld(H)$
(iii) $d \leq n - k + 1$.

Απόδειξη Το (i) είναι προφανές ενώ το (iii) προκύπτει από το (ii) και την προηγούμενη παρατήρηση. Για να αποδείξουμε το (ii) ας υποθέσουμε ότι ο H έχει στήλες $s_1, \ldots, s_n$. Παίρνουμε μια κωδική λέξη $c = (c_1, \ldots, c_n) \in C$ με βάρος w. Τότε επειδή

$$Hc^T = c_1s_1 + \ldots c_ns_n$$

ισχύει ότι $c_1s_1 + \ldots c_ns_n = 0$. Έχουμε επίσης ότι η c έχει μη-μηδενική συντεταγμένη σε w θέσεις επομένως κάποιες w, και μάλιστα όχι λιγότερες, στο πλήθος στήλες του H είναι γραμμικά εξαρτημένες. Δηλαδή, $mld(H) = w$. Εφαρμόζοντας την πρόταση 7.11 έχουμε ότι ελάχιστη απόσταση d του κώδικα είναι ίση με το βάρος της c και το ζητούμενο.

Προκειμένου να επιβεβαιώσουμε την ύπαρξη γραμμικών (n, k)-κωδίκων με ελάχιστη απόσταση d πάνω από το $\mathbf{F}_q$ αρκεί να δείξουμε ότι υπάρχει $(n - k) \times n$ πίνακας H με $mld(H) = d$.

Αναφέρουμε δύο θεωρήματα χωρίς απόδειξη

(7.32) Θεώρημα (Φράγμα των Gilbert – Varshamov)

Αν

$$q^{n-k} > \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i$$

τότε μπορούμε να κατασκευάσουμε έναν γραμμικό (n, k)-κώδικα ορισμένο στο σώμα $\mathbf{F}_q$ με ελάχιστη απόσταση μεγαλύτερη ή ίση από d. (Δες Rudolf Lidl - Gunter Pilz, Applied Abstract Algebra, Springer-Verlag 1998, κεφάλαιο 4, θεώρημα 17.14, σελίδα 196).

(7.33) Θεώρημα (Φράγμα του Plotkin) Αν υπάρχει ένας γραμμικός κώδικας μήκους n με M κωδικές λέξεις και ελάχιστη απόσταση d πάνω από το $\mathbf{F}_q$ τότε

$$d \le n \frac{M(q-1)}{(M-1)q}$$

(Δες Rudolf Lidl - Gunter Pilz, Applied Abstract Algebra, Springer-Verlag 1998, κεφάλαιο 4, θεώρημα 17.15, σελίδα 197).

Για να πετύχουμε καλύτερα αποτελέσματα μπορούμε να δημιουργήσουμε κώδικες (concatenated codes) συνδέοντας αλυσιδωτά δύο κώδικες με τον παρακάτω τρόπο:

Έστω C_1 ένας (n_1, k_1, d_1)-κώδικας και C_2 ένας (n_2, k_2, d_2)-κώδικας. Έστω ότι το μήνυμα που θέλουμε να στείλουμε είναι το $\alpha = \alpha_1, \ldots, \alpha_{k_1}$ όπου $\alpha_i = \beta_{i_1}, \beta_{i_2}, \ldots, \beta_{i_{k_2}}$ με $\alpha_i \in GF(2^{k_2})$. Μέσω του C_1 κωδικοποιώ το α στο $c = c_1, \ldots, c_{n_1}$ όπου $c_i \in GF(2^{k_2})$ και είναι της μορφής $c_i = \gamma_{i_1}, \gamma_{i_2}, \ldots, \gamma_{i_{\kappa_2}}$. Στη συνέχεια παίρνω κάθε c_i και το κωδικοποιώ με την βοήθεια του κώδικα C_2 στο $y_i = y_{i_1}, y_{i_2}, \ldots, y_{i_{n_2}}$. Επομένως, συνολικά το μήνυμα α που θέλουμε να στείλουμε κωδικοποιείται μέσω του κώδικα C, ο οποίος προκύπτει από την αλυσιδωτή σύνδεση των κωδίκων C_1 και C_2, στην κωδική λέξη $c = (y_{1_1}, y_{1_2}, \ldots, y_{1_{n_2}})(y_{2_1}, y_{2_2}, \ldots, y_{2_{n_2}}) \ldots (y_{n_{1_1}}, y_{n_{1_2}}, \ldots, y_{n_{1_{n_2}}})$.

Ισχύει η ακόλουθη

(7.34) Πρόταση Η ελάχιστη απόσταση του κώδικα C, που περιγράψαμε παραπάνω, είναι τουλάχιστον $d_1 \cdot d_2$.

Στη συνέχεια θα ανεφερθούμε στους λεγόμενους κυκλικούς κώδικες.

(7.35) Ορισμός Έστω C ένας γραμμικός (n, k)-κώδικας θα λέγεται **κυκλικός** αν ισχύει η ιδιότητα

$$(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \in C \Rightarrow (\alpha_{n-1}, \alpha_0, \alpha_1, \ldots, \alpha_{n-2}) \in C$$

Η συνάρτηση Z: $\mathbf{F}_q^n \to \mathbf{F}_q^n$ με τύπο $Z(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) = (\alpha_{n-1}, \alpha_0, \alpha_1, \ldots, \alpha_{n-2})$ θα λέγεται **κυκλική μετατόπιση**.

(7.36) Παρατήρηση Μπορούμε να ταυτίσουμε το διάνυσμα $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ με το πολυώνυμο $\alpha_0 + \alpha_1 X + \ldots + \alpha_{n-1} X^{n-1}$. Επίσης, ο $\mathbf{F}_q$ – δ.χ. $\mathbf{F}_q^n = \{(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$, όπου $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbf{F}_q\}$ είναι δακτύλιος με τις πράξεις της πρόσθεση και του πολλαπλασιασμού κατά συντεταγμένες. Μπορώ να ταυτίσω το δακτύλιο $\mathbf{F}_q^n$ με το δακτύλιο $W_n = \dfrac{F_q[X]}{< X^n - 1 >}$ και το δακτύλιο $V_n = \{ \alpha_0 + \alpha_1 X + \ldots + \alpha_{n-1} X^{n-1} \mid X^n = 1, \alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbf{F}_q\}$.

Τότε, ισχύει το εξής, ο γραμμικός κώδικας $C \le V_n$ είναι κυκλικός αν και μόνο αν ο C είναι ιδεώδες του δακτυλίου V_n.

(7.37) Θεώρημα Έστω C μη-μηδενικό ιδεώδες του V_n. Τότε υπάρχει μοναδικό πολυώνυμο $g \in V_n$ τέτοιο ώστε

(i) Το g(X) να διαιρεί το $X^n - 1$ στο $\mathbf{F}_q[X]$.
(ii) $C = \langle g(X) \rangle = \{g(X)h(X) \mid h(X) \in \mathbf{F}_q[X]\}$.
(iii) g μονικό

Απόδειξη

Επειδή το C είναι μη-μηδενικό ιδεώδες έπεται ότι υπάρχουν μη-μηδενικά πολυώνυμα που ανήκουν στο C. Έστω g μονικό πολυώνυμο το οποίο ανήκει στο C και είναι ελάχιστου βαθμού. Θα αποδείξουμε ότι $C = \langle g(X) \rangle$ και ότι το g(X) διαιρεί το $X^n - 1$ στο $\mathbf{F}_q[X]$.

Έστω $f \in C$. Θα αποδείξουμε ότι είναι πολλαπλάσιο του g. Λόγω της Ευκλείδειας διαίρεσης, έχουμε: $f = g\pi + r$ για κάποια $\pi, r \in \mathbf{F}_q[X]$ με $r = 0$ ή $\deg r < \deg g$. Αν $r \neq 0$ τότε $r = f - g\pi \in C$ αφού C ιδεώδες και επομένως $g\pi \in C$. Όμως, $r \in C$ έπεται ότι $f = g\pi$ δηλαδή $f \in \langle g \rangle$ οπότε $C \leq \langle g \rangle$.
Επίσης, επειδή το g ανήκει στο ιδεώδες C έπεται ότι $gh \in C$ για κάθε $h \in \mathbf{F}_q[X]$ και επομένως, $\langle g \rangle \leq C$. Συνδυάζοντας τα δύο τελευταία συμπεράσματα έχουμε $C = \langle g \rangle$.

Εφαρμόζουμε Ευκλείδεια διαίρεση στο $X^n - 1$ και g(X):

$$X^n - 1 = g(X)\pi(X) + r(X) \text{ για κάποια } \pi(X), r(X) \in \mathbf{F}_q[X] \text{ με } r = 0 \text{ ή } \deg r < \deg g.$$

Παίρνουμε την τελευταία σχέση mod $X^n - 1$: $0 = \overline{g}\overline{\pi} + \overline{r}$, όπου με $\overline{g}, \overline{\pi}, \overline{r}$ συμβολίζουμε το κάθε πολυώνυμο mod $X^n - 1$. Επειδή $\deg r < n$ και $\deg g < n$ έχουμε ότι: $0 = g\overline{\pi} + r$. Αν $r \neq 0$ τότε έχουμε $r = g(-\overline{\pi}) \in C$ το οποίο είναι άτοπο, άρα $r = 0$ και $X^n - 1 = g\pi$ απ' όπου προκύπτει ότι το g(X) διαιρεί το $X^n - 1$ στο $\mathbf{F}_q[X]$.

□

Συμπέρασμα Γνωρίζουμε όλους τους κυκλικούς κώδικες μήκους n αν γνωρίζουμε όλους τους διαιρέτες του $X^n - 1$ στο $\mathbf{F}_q[X]$.

(7.38) Ορισμός Το πολυώνυμο g θα λέγεται **πολυώνυμο γεννήτορας** του κυκλικού κώδικα C και τα στοιχεία του C θα λέγονται **κωδικές λέξεις**, **κωδικά πολυώνυμα** ή **κωδικά διανύσματα**.

Θέλουμε να φτιάξουμε κώδικα τύπου (n, k). Ψάχνουμε να βρούμε πολυώνυμο g(X) στο $\mathbf{F}_q[X]$ τέτοιο ώστε το g(X) να διαιρεί το $X^n - 1$ και $m = \deg g(X) = n - k$. Υποθέτουμε ότι υπάρχει τέτοιο g(X) αλλιώς παίρνουμε κάποιο g(X) που να διαιρεί το $X^n - 1$ με $\deg g(X) = m = n - k$ και φτιάχνουμε κώδικα (n, k) όπου $k = n - m$.

Η κωδικοποίηση γίνεται ως εξής: Το διάνυσμα $v = (v_0, v_1, \ldots, v_{k-1})$ το αντικαθιστούμε με τοπολυώνυμο $v(X) = v_0 + v_1X + \ldots + v_{k-1}X^{k-1}$, το πολλαπλασιάζουμε με το πολυώνυμο g(X) και το πολυώνυμο που βρίσκουμε το κάνουμε διάνυσμα.

Για παράδειγμα ας πάρουμε n = 6 και q = 2. Τότε $X^n - 1 = X^6 - 1$ στο $\mathbf{F}_2$ [X]. Έστω $g = X^3 - 1 = X^3 + 1$ το οποίο διαιρεί το $X^6 - 1$. Ο κώδικας C = <g> είναι ένας (n, k) = (n, n – m) κώδικας. δηλαδή ένας (6, 3) κώδικας. Τότε έχουμε

$000 \mapsto (0 + 0X + 0X^2)(1 + X^3) = 0 + 0X + 0X^2 + 0X^3 + 0X^4 + 0X^5 \mapsto 000000$
$100 \mapsto (1 + 0X + 0X^2)(1 + X^3) = 1 + X^3 \mapsto 100100$
$010 \mapsto X(1 + X^3) = X + X^4 \mapsto 010010$
$110 \mapsto (1 + X)(1 + X^3) = 1 + X + X^3 + X^4 \mapsto 110110$
$001 \mapsto X^2(1 + X^3) = X^2 + X^5 \mapsto 001001$
$101 \mapsto (1 + X^2)(1 + X^3) = 1 + X^2 + X^3 + X^5 \mapsto 101101$
$011 \mapsto (1 + X^2)(1 + X^3) = 1 + X^2 + X^3 + X^5 \mapsto 101101$
$111 \mapsto (1 + X + X^2)(1 + X^3) = 1 + X + X^2 + X^3 + X^4 + X^5 \mapsto 111111$

Για να δείξουμε πως γίνετε η αποκωδικοποίηση ας αρχίσουμε με ένα παράδειγμα. Έστω $g = 1 + X^2 + X^3$ το οποίο διαιρεί το $X^7 - 1$ στο $\mathbf{F}_2$ [X]. Δηλαδή n = 7 και m = deg(g) = 3. Επομένως, k = n – m = 7 – 3 = 4. Συνεπώς ο κυκλικός κώδικας C = <g> είναι ένας (7, 4)-κώδικας.

Το μήνυμα α = 1010 αντιστοιχεί στο πολυώνυμο $1 + X^2$ και αν το πολλαπλασιάσουμε με g παίρνουμε $(1 + X^2)(1 + X^2 + X^3) = 1 + X^2 + X^2 + X^4 + X^3 + X^5 = 1 + X^3 + X^4 + X^5$. Οπότε το μήνυμα κωδικοποιείται στο 1001110.

Ας υποθέσουμε ότι το μήνυμα που πήραμε είναι το ω = 1100001 το οποίο αντιστοιχεί στο πολυώνυμο $1 + X + X^6$. Διαιρούμε το πολυώνυμο με το πολυώνυμο g και βρίσκουμε ότι: $1 + X + X^6 = g(X + X^2 + X^3) + (X^2 + 1)$. Το γεγονός ότι στη διαίρεση εμφανίζεται υπόλοιπο, σημαίνει ότι το ω δεν είναι κωδική λέξη, άρα θα πρέπει να διορθωθεί.

(7.39) Αλγόριθμος αποκωδικοποίησης

Έστω C = <g> ένας κυκλικός (n, k)-κώδικας t-διόρθωσης λαθών.

(i) Διαιρούμε το μήνυμα ω, που πήραμε με το g και βρίσκουμε υπόλοιπο r.
(ii) Για $0 \le i \le n - 1$ υπολογίζουμε το $S_i = X^i r \pmod g$ μέχρι να βρούμε κάποιο S_j τέτοιο ώστε $w(S_j) \le t$. Τότε το $X^{n-j} S_j \bmod (X^n - 1)$ είναι το πιο πιθανό λάθος.

(7.40) Παράδειγμα Έστω n = 15 και $g = 1 + X^4 + X^6 + X^7 + X^8$ ορισμένο στο $\mathbf{F}_2[X]$. Αφού m = deg(g) = 8 έπεται ότι k = 15 – 8 = 7 και ότι ο κωδικας C = <g> είναι ένας (15, 7)-κώδικας. Αποδεικνύεται ότι η ελάχιστη απόσταση του κώδικα είναι $d = d_{min}(C) = 5$. Επομένως ο κώδικας διορθώνει $t = \left[\frac{d-1}{2}\right] = 2$ λάθη. Υποθέτουμε ότι πήραμε το διάνυσμα v = 100111000000000. Το πολυώνυμο που αντιστοιχεί στο v είναι το $u = 1 + X^3 + X^4 + X^5$. Επειδή deg u < deg g = 8, δεν χρειάζεται να διαιρέσω το u με g διότι $u = g \cdot 0 + u$. Οπότε r = u ενώ το βάρος του διανύσματος v είναι w(v) = 4 > 2 = t. Έχουμε:

$S_1 = X \cdot r = X(1 + X^3 + X^4 + X^5) = X + X^4 + X^5 + X^6$ οπότε $w(S_1) = 4 > 2 = t$.
$S_2 = X^2 \cdot r = X^2(1 + X^3 + X^4 + X^5) = X^2 + X^5 + X^6 + X^7$ οπότε $w(S_2) = 4 > 2 = t$.

$S_3 = X^3 \cdot r = X^3 (1 + X^3 + X^4 + X^5) = X^3 + X^6 + X^7 + X^8 \pmod g = X^3 + X^6 + X^7 + X^6 + X^7 + X^4 + 1 \pmod g = 1 + X^3 + X^4$ οπότε $w(S_3) = 3 > 2 = t$.
$S_4 = X^4 \cdot r = X\, S_3 = X + X^4 + X^5$ οπότε $w(S_4) = 3 > 2 = t$.
$S_5 = X^5 \cdot r = X\, S_4 = X^2 + X^5 + X^6$ οπότε $w(S_5) = 3 > 2 = t$.
$S_6 = X^6 \cdot r = X\, S_5 = X^3 + X^6 + X^7$ οπότε $w(S_6) = 3 > 2 = t$.
$S_7 = X^7 \cdot r = X\, S_6 = X^4 + X^7 + X^8 \pmod g = X^4 + X^7 + X^7 + X^6 + X^4 + 1 \pmod g = 1 + X^6$ οπότε $w(S_7) = 2 \leq t$.

Επομένως, το $X^{15-7}\, S_7 = X^8\, S_7 = X^8 (X^6 + 1) = X^{14} + X^8 \bmod (X^{15} - 1)$ είναι το πιο πιθανό λάθος. Οπότε, αποκωδικοποιούμε στο $f = u + X^{14} + X^8 = 1 + X^3 + X^4 + X^5 + X^{14} + X^8$. Δηλαδή μας στάλθηκε η κωδική λέξη: 100111001000001 και το μήνυμα που μας στάλθηκε ήταν το $f / g = 1 + X^3 + X^5 + X^6$ δηλαδή το 1001011.

ΤΕΛΟΣ