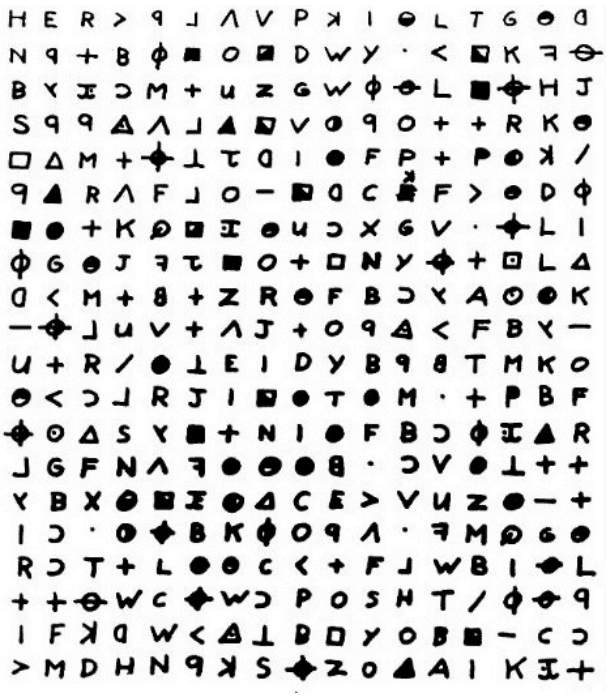
Πεπερασμένα σώματα & Κρυπτογραφία



Σημειώσεις σύμφωνα με τις παραδόσεις του
Αριστείδη Κοντογεώργη

Τσουκνίδας Ιωάννης,
Τμήμα Μαθηματικών
Πανεπιστήμιο Αθηνών, 2012

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή στα πεπερασμένα σώματα

1.1 Μάθημα 1.

Δευτέρα 12.3.2012

Με $\mathbb{Z}$ θα συμβολίζεται ο δακτύλιος των ακεραίων. Ορίζουμε στον δακτύλιο των ακεραίων την εξής σχέση ισοδυναμίας:

$$a \equiv \beta \bmod m \Leftrightarrow m|\beta - a. \tag{1.1}$$

Ισοδύναμα γράφουμε:

$$a \equiv \beta \bmod m \Leftrightarrow \beta - a \in m\mathbb{Z} \tag{1.2}$$

Όπου με $m\mathbb{Z}$ συμβολίζουμε τα πολλαπλάσια του m.

Έστω τώρα ένα στοιχείο $a \in \mathbb{Z}$, ορίζεται έτσι η κλάση ισοδυναμίας του στοιχείου a στον δακτύλιο Z_m ως εξής:

$$\begin{aligned}
[a] &= \{x \in \mathbb{Z} | x \equiv a \bmod m\} && (1.3)\\
&= \{x \in \mathbb{Z} | m|(x-a)\} && (1.4)\\
&= \{x \in \mathbb{Z} | x - a = km\} && (1.5)\\
&= \{km + a \in \mathbb{Z}\} && (1.6)
\end{aligned}$$

Σημείωση. Ισχύει ότι $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$

Το $\mathbb{Z}/\mathbb{Z}m$ έχει τις "καλές" ιδιότητες του σώματος αν ο m είναι πρώτος.

Παράδειγμα 1.1.1. Στα σώματα ισχύει ότι κάθε στοιχείο είναι αντιστρέψιμο, οπότε θεωρώ τον δακτύλιο πηλίκο $\mathbb{Z}/4\mathbb{Z} = \mathbb{Z}_4 = \{0, 1, 2, 3\}$. Αν ο $\mathbb{Z}/4\mathbb{Z}$ ήταν σώμα το 2 θα ήταν αντιστρέψιμο, δηλαδή θα υπήρχε $a \in \mathbb{Z}_4$ ώστε $a \cdot 2 = 1$ όμως για κάθε $a = 0, 1, 2, 3$ παρατηρώ ότι $a \cdot 2 \neq 1$ άρα το $\mathbb{Z}/4\mathbb{Z}$ δεν είναι σώμα.

Απο εδώ και στο εξής θα συμβολίζουμε το $\mathbb{Z}/p\mathbb{Z}$ με $\mathbb{F}_p$ και θα ασχολούμαστε με τις περιπτώσεις όπου ο p είναι πρώτος.

Θεώρημα 1.1.1. *Για κάθε δύναμη πρώτου p^z, όπου p :* πρώτος *και $z \in \mathbb{N}\backslash\{0\}$ υπάρχει ακριβώς (μέχρι ισομορφισμού) ένα σώμα με p^z στοιχεία.*

1.1.1 Στοιχεία αλγεβρικής θεωρίας

Ορισμός 1.1.1 (Πράξη)**.** Μία συνάρτηση $f : A \times A \to A$ όπου A μη κενό σύνολο ονομάζεται *πράξη*.

Παράδειγμα 1.1.2. Η πρόσθεση στο $\mathbb{R}$ +:$\mathbb{R} \times \mathbb{R} \to \mathbb{R}$ είναι πράξη.

Παράδειγμα 1.1.3. Η αφαίρεση: $- : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ στους φυσικούς **δεν** είναι πράξη:

$$1 - 6 = -5 \notin \mathbb{N}$$

Ορισμός 1.1.2 (Ομάδα)**.** Ένα σύνολο G εφοδιασμένο με μία **πράξη** $\oplus : G \times G \to G$ θα λέμε ότι είναι ομάδα αν ικανοποιεί τα εξής:

1. Υπάρχει στοιχείο 0_G ώστε για κάθε $a \in G$ να ισχύει ότι $0 \oplus a = a \oplus 0 = a$.
2. Για κάθε $a \in G$ υπάρχει $a' \in G$ με την ιδιότητα $a \oplus a' = 0_G$.
3. Για κάθε a, β, γ ισχύει η προσεταιριστική: $a \oplus (\beta \oplus \gamma) = (a \oplus \beta) \oplus \gamma$.

Το (G,$\oplus$) ονομάζεται **ομάδα** αν ικανοποιεί τα παραπάνω.

Ορισμός 1.1.3 (Δακτύλιος)**.** Αν μία ομάδα $(G, \oplus)$ εφοδιαστεί με μία ακόμα πράξη, έστω την $\otimes : G \times G \to G$, τότε το $(G, \oplus, \otimes)$ θα λέγεται δακτύλιος με μονάδα αν ικανοποιεί (εκτός από τις ιδιότητες της ομάδας ως προς την $\oplus$) και τα εξής:

1. Υπάρχει στοιχείο $1_G \in G$ τέτοιο ώστε $a \otimes 1_G = 1_G \otimes a = a$ για κάθε $a \in G$.
2. Ισχύει η προσεταιριστική ιδιότητα: $(a \otimes \beta) \otimes \gamma = a \otimes (\beta \otimes \gamma)$ για κάθε $a, \beta, \gamma \in G$.
3. Ισχύει η αριστερή και η δεξιά επιμεριστική ιδιότητα:

$$a \otimes (\beta \oplus \gamma) = a \otimes \beta \oplus a \otimes \gamma \text{ και } (\beta \oplus \gamma) \otimes a = \beta \otimes a \oplus \gamma \otimes a$$

Παρατηρήσεις

1. Αν $a \cdot \beta = \beta \cdot a$ τότε ο δακτύλιος ονομάζεται μεταθετικός ή Αβελιανός.
2. Αν υπάρχει στοιχείο $1_A \in A$ με την ιδιότητα $1_A \cdot a = a \cdot 1_A = a$ για κάθε $a \in A$ τότε το 1_A λέγεται *μοναδιαίο* στοιχείο και ο A λέγεται *δακτύλιος με μοναδιαίο στοιχείο.*

Ορισμός 1.1.4 (Ιδεώδες)**.** Ένα μη κενό υποσύνολο I ενός δακτυλίου R θα λέγεται **ιδεώδες** του R αν ικανοποιεί τα εξής:

1. Για κάθε $a, \beta \in I$ ισχύει ότι $a - \beta \in I$
2. Για κάθε $r \in R$ και για κάθε $a \in I$ ισχύει ότι $r \cdot a \in I$ και $a \cdot r \in I$.

Παρατήρηση. Αν ο δακτύλιος δεν είναι μεταθετικός, ορίζονται οι έννοιες του αριστερού ιδεώδους στο οποίο ισχύει ότι $ra \in I$ και του δεξιού όπου $ar \in I$. Αμφίπλευρο είναι το ιδεώδες που είναι ταυτόχρονα και δεξιό και αριστερό.

Μπορούμε τώρα να ορίσουμε την έννοια του δακτυλίου πηλίκο το οποίο προκύπτει από έναν δακτύλιο R και απο ένα ιδεώδες I του R. Ορίζω μία σχέση ισοδυναμίας σε έναν δακτύλιο R ως εξής:

$$\tau_1 \sim \tau_2 \Leftrightarrow \tau_1 - \tau_2 \in I \tag{1.7}$$

Η $\sim$ είναι σχέση ισοδύναμίας.
(Η απόδειξη παραλείπεται αλλά είναι απλή, αρκεί να δείξετε ότι:

1. $a \sim a$
2. αν $a \sim \beta$ τότε $\beta \sim a$
3. αν $a \sim \beta$ και $\beta \sim \gamma$ τότε $a \sim \gamma$).

Έστω $[\tau]$ η κλάση ισοδυναμίας του τ. Ορίζω:

- $[\tau_1] + [\tau_2] = [\tau_1 + \tau_2]$
- $[\tau_1] \cdot [\tau_2] = [\tau_1 \cdot \tau_2]$.

Πρόταση 1.1.2. *Οι παραπάνω συναρτήσεις ορίζουν πράξεις στο R.*

Απόδειξη. Έχω ότι:

- Αν $\tau_1 \sim \tau_1' \Leftrightarrow \tau_1 - \tau_1' = i_1 \in I \subseteq R$ και
- Αν $\tau_2 \sim \tau_2' \Leftrightarrow \tau_2 - \tau_2' = i_2 \in I$
  Τότε $\tau_1\tau_2 - \tau_1'\tau_2' = \tau_1\tau_2 + \tau_1\tau_2' - \tau_1\tau_2\tau_1'\tau_2' = \tau_1(\tau_2 - \tau_2') - \tau_2(\tau_1' - \tau_1)$.

□

Ορισμός 1.1.5 (Ακέραια περιοχή)**.** Ένας μοναδιαίος, μεταθετικός δακτύλιος R θα λέγεται **ακέραια περιοχή** αν για κάθε $a, \beta \in R$ με $a \cdot b = 0$ ισχύει ότι $a = 0$ η $b = 0$.

Παρατηρήσεις

- Το $\mathbb{Z}$ είναι ακέραια περιοχή.
- Το $\mathbb{Z}_p$ είναι ακέραια περιοχή αν και μόνο αν το p είναι πρώτος.

Πρόταση 1.1.3. *Το $\mathbb{Z}/p\mathbb{Z}$ είναι ακέραια περιοχή αν και μόνο αν ο p είναι πρώτος.*

Απόδειξη. Αν ο n είναι σύνθετος θα είναι της μορφής $n = a \cdot \beta$ με $1 < a, \beta < n$. Έχω ότι $n = 0 \Leftrightarrow a\beta \equiv 0 \mod n$ στον $\mathbb{Z}/n\mathbb{Z}$ ενώ $a \not\equiv 0 \mod n$ και $\beta \not\equiv 0 \mod n$. Δηλαδή δείξαμε ότι αν ο n είναι σύνθετος τότε το πηλίκο δεν είναι σώμα. Δηλαδή αν το πηλικό είναι σώμα τότε τότε ο n είναι πρώτος.

Αντιστρόφως αν ο $n = p$ είναι πρωτός τότε κάθε αριθμός $0 < a < p$ θα είναι πρώτος προς τον p, δηλαδή ο μέγιστος κοινός διαιρέτης του με τον p θα είναι μονάδα δηλαδή θα υπάρχουν x, y ώστε $xa + yp = 1$. Αν υπήρχε β ώστε $a\beta = 0$ τότε η παραπάνω σχέση θα μας έδινε $xa\beta = \beta \equiv 0 \mod p$ δηλαδή το $\beta = 0$. Και συνεπώς ο δακτύλιος είναι ακεραία περιοχή. □

Ορισμός 1.1.6 (Σώμα)**.** Έστω R ένας δακτύλιος. Ο R είναι σώμα αν κάθε μη μηδενικό στοιχείο του είναι αντιστρέψιμο.

Παρατήρηση. Τα $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$ είναι σώματα.

Πρόταση 1.1.4. *Κάθε πεπερασμένη ακέραια περιοχή είναι σώμα.*

Απόδειξη. Έστω R πεπερασμένη ακέραια περιοχή με $R = \{0, 1, a_1, a_2, \dots a_n\}$. Τότε για $z \in R$ με $z \neq 0, 1$ θα έχω ότι το σύνολο $(0, z, za_1, \dots za_n)$ έχει m το πλήθος διαφορετικά ανά δύο στοιχεία του R και $za_i \neq za_j$ αν $a_i \neq a_j$. Αν $za_i = za_j \Leftrightarrow z(a_i - a_j) = 0 \xrightarrow{z\neq 0 \text{και R:ακ. περιοχή}}$ $a_i - a_j = 0 \Leftrightarrow a_i = a_j$. □

1.2 Μάθημα 2.

Τετάρτη 14.3.2012

Σε αυτό το μάθημα ορίζουμε τις έννοιες του ιδεώδους, του σώματος και κάνουμε παραδείγματα. Ορίζουμε τη χαρακτηριστική ενός δακτυλίου, τα πεπερασμένα σώματα, τις επεκτάσεις σωμάτων και κάνουμε μία εισαγωγή στις έννοιες των πολυωνύμων.

Σημείωση: Η κατεύθυνση των ορισμών έχει ακολουθήσει το σχήμα του βιβλίου "Εισαγωγή στην άλγεβρα" του J. B. Fraleigh.

1.2.1 Ιδεώδη

Ορισμός 1.2.1 (ιδεώδες)**.** Ένας υποδακτύλιος N ενός δακτυλίου R που ικανοποιεί τις ιδιότητες:

$$aN \subseteq N \text{ και } Nb \subseteq N \text{ για κάθε } a, b \in R.$$

Παρατήρηση. Με $1 = 1_R$ συμβολίζουμε τη μονάδα του δακτυλίου.

Πρόταση 1.2.1. *Αν* $1_R \in I$ *τότε* $I = R$.

Απόδειξη. Καταρχάς εξ' ορισμού ισχύει ότι $I \subseteq R$. Για τον αντίστροφο εγκλεισμό, παρατηρώ ότι αν $\tau \in R$ τότε $\tau = \tau \cdot 1 \in I$ δηλαδή $R \subseteq I$ που σημαίνει ότι $R = I$. □

Ορισμός 1.2.2 (σώμα)**.** Έστω R ένας δακτύλιος. Τότε ο R ονομάζεται σώμα αν για κάθε στοιχείο $\tau \in R$, $\tau \neq 0$ υπάρχει $\tau' \in R$ ώστε $\tau \cdot \tau' = 1$.

Παράδειγμα 1.2.1. Το $\mathbb{Z}$ είναι δακτύλιος αλλά όχι σώμα μιας και το $2 \in \mathbb{Z}$ δεν είναι αντιστρέψιμο. Δηλαδή δεν υπάρχει $x \in \mathbb{Z}$ με την ιδιότητα $2x \neq 1$.

Ορισμός 1.2.3 (δακτύλιος πηλίκο)**.** Έστω R ένας δακτύλιος και I ένα ιδεώδες του R. Το σύνολο $R/I = \{a + I \text{ όπου } a \in R\}$ ονομάζεται δακτύλιος πηλίκο. Το $a + I$ ονομάζεται είτε κλάση του a modulo I, είτε προσθετικό σύμπλοκο του I, ανάλογα με το σύγγραμμα και είναι το σύνολο $a + I = \{a + x \text{ όπου } x \in I\}$.

Πρόταση 1.2.2. *Αν* R *ένα σώμα, τότε τα μοναδικά ιδεώδη είναι το μηδενικό ιδεώδες* $\{0_R\}$ *και το ίδιο το* R.

Απόδειξη. Αποδεικνύουμε καταρχάς οτι το $\{0_R\}$ και το ίδιο το R είναι ιδεώδη. Πράγματι, για κάθε $\tau \in R$ ισχύει $\tau \cdot 0_R = 0_R$ (το τελευταίο ισχύει από τις ιδιότητες του δακτυλίου: $z \cdot x = z(x + 0_R) = z \cdot x + z \cdot 0_R \Rightarrow z \cdot 0_R = 0_R$). Το R είναι ιδεώδες του ευατού του και η απόδειξη παραλείπεται αλλά μπορεί εύκολα να γίνει με χρήση του ορισμού του δακτυλίου. Μένει να αποδείξουμε ότι το R δεν έχει άλλα ιδεώδη. Έστω ότι υπάρχει I ιδεώδες του R, δηλάδη, $I \triangleleft R$ και $I \neq \{0_R\}$ τότε υπάρχει $x \neq 0, x \in I$ και αφού το R είναι σώμα θα υπάρχει το αντίστροφο του x, έστω $x^{-1} \in R$ ώστε $x^{-1} \cdot x = 1_R$ όμως $x \in I$ άρα $x^{-}1 \cdot x \in I$ άρα και $1_R \in I$ οπότε αφού $1_R \in I$ θα έχουμε $I = R$. Οπότε σε κάθε περίπτωση θα ισχύει το ζητούμενο. □

Ορίζουμε τώρα την αρχή του ελαχίστου η οποία είναι ισοδύναμη με την αρχή της επαγωγής (δηλαδή αν δεχτούμε αξιωματικά ότι ισχύει η μία από τις δύο μπορούμε να αποδείξουμε την άλλη),

Ορισμός 1.2.4 (αρχή του ελαχίστου)**.** Κάθε μη κενό υποσύνολο των φυσικών αριθμών έχει ελάχιστο στοιχείο.

Η αρχή του ελαχίστου χρησιμεύει στην παρακάτω πρόταση.

Πρόταση 1.2.3. *Όλα τα ιδεώδη του $\mathbb{Z}$ είναι της μορφής $n\mathbb{Z}$ με $n \in \mathbb{Z}$.*

Απόδειξη. Έστω $I \triangleleft R$, τότε διακρίνουμε τις εξής περιπτώσεις:

- Αν $I = \{0_R\}$ τότε για κάθε $x \in R$ θα έχω $x \cdot 0 = 0 \cdot x = 0 \in I$ οπότε το I θα είναι της μορφής $I = 0\mathbb{Z}$.
- Αν $I \neq \{0_R\}$ τότε θα υπάρχει $x \in I, x \neq 0$ οπότε και $-x \in I$ άρα το σύνολο $\emptyset \neq \{y \in I, y > 0\} \subseteq \mathbb{N}$. Άρα έχει ελάχιστο στοιχείο $\delta \in I$ και θα δείξουμε ότι $I = \delta\mathbb{Z}$. Αν $x \in I$ τότε ο αλγόριθμος της διαίρεσης του x με το δ είναι $x = \pi\delta + \upsilon$ με $\upsilon < \delta$ και έχω ότι $x, \delta \in I$ άρα και η διαφορά τους $\upsilon = x - \pi\delta$ θα ανήκει στο I, άρα θα είναι $\upsilon = 0$.

□

Ορισμός 1.2.5. Αν R είναι ένας δακτύλιος, τότε το σύνολο των αντιστρέψιμων στοιχείων του συμβολίζεται με:

$$U(R) = \{x \in R \text{ για τα οποία υπάρχει } x^{-1} \in R \text{ ώστε } x \cdot x^{-1} = x^{-1} \cdot x = 1_R\}$$

Ισχύει ότι $U(\mathbb{Z}) = \{-1, +1\}$

Πρόταση 1.2.4. *Ισχύει ότι $U(\mathbb{Z}/m\mathbb{Z}) = \{n \bmod m, (n, m) = 1\}$*

Απόδειξη. Αν $(n, m) = 1$ αν και μόνο αν $x, y \in \mathbb{Z}$ ώστε $xn + ym = 1$. Το τελευταίο όμως είναι ισοδύναμο με το $xn \equiv 1 \mod m$. □

Παράδειγμα 1.2.2. Οι κλάσεις υπολοίπων $\mathbb{Z}/12\mathbb{Z}$ είναι οι παρακάτω: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. Από αυτές τα αντιστρέψιμα στοιχεία είναι τα $U(\mathbb{Z}/12\mathbb{Z}) = \{1, 5, 7, 11\}$.

Οι μονάδες $U(R)$ ενός δακτυλίου με μοναδιαίο στοιχείο, αποτελούν ομάδα με πράξη των πολλαπλασιασμό.

Ορισμός 1.2.6. Η τάξη της $|U(\mathbb{Z}/m\mathbb{Z})|$ θα συμβολίζεται με $\phi(m)$. Η συνάρτηση $m \mapsto \phi(m)$ θα λέγεται η ϕ-συνάρτηση του Euler.

Αν ο p είναι πρώτος τότε το $\mathbb{Z}/p\mathbb{Z}$ είναι σώμα συνεπώς $|U(\mathbb{Z}/p\mathbb{Z})| = p - 1$. Άρα $\phi(p) = p - 1$.

Ορισμός 1.2.7. Μία συνάρτηση $f : R \to S$ ώστε

$$f(x + y) = f(x) + f(y)$$

και

$$f(xy) = f(x)f(y)$$

θα ονομάζεται ομομορφισμός δακτυλίων.

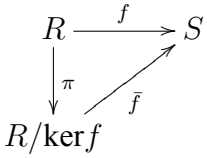
Ο πύρηνας ker$f$ ορίζεται να είναι

$$\text{ker}f = \{x \in R : f(x) = 0\}.$$

Είναι εύκολο να δούμε ότι ο ker f είναι ιδεώδες του R. Πράγματι είναι μη κενό σύνολο αφού $f(0) = 0$ (γιατί?) και επίσης αν $x, y \in \text{ker}f$ τότε $f(x) = f(y) = 0$. Αλλά $f(x + y) = f(x) + f(y) = 0 + 0 = 0$ άρα $f(x + y) = 0$ δηλαδή $x + y \in \text{ker}f$. Παρόμοια αν $x \in R$ και $y \in \text{ker}f$ έχουμε ότι $f(xy) = f(x)f(y) = f(x)0 = 0$.

Έστω $f : R \to S$ ομομορφισμός δακτυλίων. Αποδεικνύεται ότι f είναι 1-1 αν και μόνο αν ker$f = \{0\}$.

Σε κάθε περίπτωση μπορούμε να ορίσουμε το διάγραμμα:



ώστε π επί και η $\bar{f}$ να είναι 1-1. Η συνάρτηση π είναι ο φυσικός επιμορφισμός $\pi(\tau) = \tau$ mod ker$f$ ενώ ορίζουμε την $\bar{f}(\tau \mod \text{ker}f = \bar{f}(\pi(\tau)) = f(\tau)$.

Είναι καλά ορισμένη η f? Αν $\tau \mod \text{ker}\, f = \tau' \mod \text{ker}f$ τότε εξ ορισμού $\tau - \tau' \in \text{ker}f$ συνεπώς $\bar{f}(\tau \mod \text{ker}f) = \bar{f}(\tau' \mod \text{ker}f)$.

Ο πυρήνας

$$\text{ker}\bar{f} = \{\tau \mod \text{ker}f : f(\tau) = 0\} = 0_{R/\text{ker}f},$$

δηλαδή η $\bar{f}$ είναι 1-1. Προφανώς

$$R/\text{ker}f \cong Im(f).$$

1.2.2 Χαρακτηριστική δακτυλίου

(Εισαγωγή στην άλγεβρα, J. B. Fraleigh, σελ. 292)

Παρατηρούμε ότι γνωρίζουμε έναν ομομορφισμό $f : \mathbb{Z} \to R$ αν και μόνο αν γνωρίζουμε το $f(1)$.

Πράγματι, ένας ομομορφισμός f ικανοποιεί την $f(-x) = -f(x)$. Για να το δούμε αυτό βλέπουμε πρώτα ότι $f(0) = 0$. Αυτό γιατί $f(x) = f(x+0) = f(x)+f(0)$ άρα $f(0) = 0$. Στην συνέχεια $0 = f(0) = f(x + (-x)) = f(x) + f(-x)$.

Έτσι $f(n) = f(1 + \ldots 1) = nf(x)$ αν $n \geq 0$ και αφού $f(-x) = -f(x)$ έχουμε ότι $f(-n) = -f(n)$.

Γιά ένα δακτύλιο με μονάδα θεωρούμε τώρα τον ομομορφισμό

$$f : \mathbb{Z} \to R$$

ώστε $f(1_{\mathbb{Z}}) = 1_R$. Ο πυρήνας $\ker f$ είναι ένα κύριο ιδεώδες του $\mathbb{Z}$ και συνεπώς είναι της μορφής $\ker f = n\mathbb{Z}$. Τον γεννήτορα n θα τον ονομάζουμε χαρακτηριστική του δακτυλίου.

Αν ο ομομορφισμός είναι 1-1 τότε $n = 0$ και θα λέμε ότι ο δακτύλιος R είναι χαρακτηριστικής 0. Σε αυτή την περίπτωση το R περιέχει έναν υποδακτύλιο (τον $\mathrm{Im}(f)$) ο οποίος είναι ισόμορφος με το $\mathbb{Z}$. Άρα ο R δεν μπορεί να έχει πεπερασμένα το πλήθος στοιχεία.

Παράδειγμα 1.2.3. Θεωρούμε τον φυσικό επιμορφισμό

$$f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

$$1 \mapsto 1 \bmod n.$$

Ο πυρήνας του είναι το $n\mathbb{Z}$ και συνεπώς η χαρακτηριστική του δακτυλίου $\mathbb{Z}/n\mathbb{Z}$ είναι n.

Παρατηρούμε ότι αν ο δακτύλιος R έχει χαρακτηριστική n τότε περιέχει ένα υποδακτύλιο ισόμορφο με το $\mathbb{Z}/n\mathbb{Z}$ ο οποίος όμως είναι ακεραία περιοχή αν και μόνο αν n είναι πρώτος. Καταλήγουμε λοιπόν στο συμπέρασμα:

Θεώρημα 1.2.5. *Οι ακέραιες περιοχές και τα σώματα έχουν χαρακτηριστική πρώτο αριθμό.*

Υπενθυμίζουμε ότι ένας δακτύλιος λέγεται ακεραία περιοχή αν και μόνο αν $ab = 0 \Rightarrow a = 0$ ή $b = 0$. Επιπλέον τα σώματα είναι ακεραίες περιοχές αφού αν $ab = 0$ αν $a \neq 0$ τότε υπάρχει a^{-1} ώστε $a^{-1}a = 0$ οπότε πολλαπλασιάζοντας την $ab = 0$ με a^{-1} έχουμε ότι $b = 0$.

1.2.3 Πεπερασμένα σώματα

Έχουν χαρακτηριστική πρώτο αριθμό και το $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ως υπόσωμα.

1.2.4 Επεκτάσεις σωμάτων

(Εισαγωγή στην άλγεβρα, J. B. Fraleigh, σελ. 416)

Αν $K \subset L$ τότε το L λέγεται επέκταση του K και το K υπόσωμα του L. Κάθε πεπερασμένο σώμα είναι επέκταση του $\mathbb{F}_p$.

Παρατηρούμε ότι $K \subset L$ είναι επέκταση σωμάτων τότε το L με τις πράξεις

$$L \times L \to L$$

$$(x, y) \mapsto x + y$$

και

$$K \times L \to L$$

$$(\lambda, x) \mapsto \lambda x$$

αποκτά την δομή K-διανυσματικού χώρου. Ονομάζουμε βαθμό της επέκτασης L/K την διάσταση του διανυσματικού χώρου.

$$[L : K] := \dim_K L.$$

Παράδειγμα 1.2.4. Το σώμα $\mathbb{C}$ έχει φυσιολογική δομή $\mathbb{R}$ διανυσματικού χώρου και $[\mathbb{C} : \mathbb{R}] = 2$. Επίσης $[\mathbb{C} : \mathbb{Q}] = \infty$ (γιατί?).

Έστω L ένα πεπερασμένο σώμα. Θεωρούμε το L ως πεπερασμένη επέκταση του $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Αν $[L : \mathbb{F}_p] = n$ τότε μπορώ (διαλέγοντας μία βάση του L) να υποθέσω ότι $L \cong \mathbb{F}_p^n$ δηλαδή το L είναι ισόμορφο ως διανυσματικός χώρος με το σύνολο των διατεταγμένων n-άδων από το σώμα $\mathbb{F}_p$. Συνεπώς

$$\#L = p^n.$$

1.3 Μάθημα 3.

Δευτέρα 19.3.2012

1.3.1 Πολυώνυμα

Σε αυτό το μάθημα προχωράμε στον ορισμό του δακτυλίου των πολυωνύμων, εξετάζουμε τις ιδιότητες των πολυωνύμων πάνω σε ένα σώμα, ορίζουμε τον Ευκλείδειο αλγόριθμο διαίρεσης πολυωνύμων, την έννοια της διαιρετότητας πολυωνύμων, τα ανάγωγα πολυώνυμα και τον μέγιστο κοινό διαιρέτη δύο πολυωνύμων.

Ορισμός 1.3.1 (πολυώνυμο σε έναν δακτύλιο[1])**.** Έστω R ένας δακτύλιος. Ορίζουμε το $f(t)$ με

$$f(t) = \sum_{\nu=0}^{n} a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$$

όπου $a_\nu \in R$. Το μεγαλύτερο $\nu > 0$ για το οποίο ισχύει ότι $a_\nu \neq 0$ ονομάζεται *βαθμός* του πολυωνύμου. Αν $f(t) = a_0$ τότε λέγεται μηδενικού βαθμού.

Τον δακτύλιο των πολυωνύμων με συντελεστές από ένα δακτύλιο R το συμβολίζουμε με $R[x]$.

Πρόταση 1.3.1. *Αν $f(t), g(t)$ είναι πολυώνυμα τότε:*

- *Το άθροισμα τους $f(t) + g(t)$ είναι πολυώνυμο.*
- *Το γινόμενο τους $f(t) \cdot g(t)$ είναι πολυώνυμο στον $F[x]$.*

Απόδειξη. Έστω $f(t) = \sum_{\nu=0}^{n} a_\nu x^n$ και $g(t) = \sum_{\mu=0}^{m} \beta_\mu x^\mu$. Τότε:

[1] *(Εισαγωγή στην άλγεβρα, J. B. Fraleigh, σελ. 316)*

$$f(t)+g(t)=\sum_{\nu=0}^{\min(n,m)}(a_\nu+\beta^\nu)x^\nu+\sum_{\nu=\min(n,m)+1}^{\max(n,m)}(a_\nu+\beta_\nu)x^\nu=$$
$$=\sum_{\nu=0}^{\max(n,m)}(a_\nu+\beta_\nu)x^\nu \text{ όπου αν } \nu>\mu \text{ θα είναι } a_\nu=0 \text{ και αν } \mu>m \text{ θα είναι } \beta_\mu=0. \tag{1.8}$$

$$f(t)\cdot g(t)=\sum_{\nu=0}^{n}\sum_{\mu=0}^{m}a_\nu\beta_\mu x^{\nu+\mu}$$
$$=\sum_{\nu=0}^{n+m}\sum_{\mu=0}^{n+m}a_\nu\beta_{n+m-\mu}x^{\nu+\mu} \tag{1.9}$$

□

Σημείωση. Αν ο δακτύλιος R πάνω στον οποίο "παίρνουμε" των δακτύλιο των πολυωνύμων είναι σώμα τότε ο δακτύλιος των πολυωνύμων **δεν είναι πάντα σώμα** αλλά είναι πάντα **ακέραια περιοχή.** Ο λόγος για τον οποίο δεν είναι σώμα το $F[x]$ είναι ότι το x δεν είναι αντιστρέψιμο στοιχείο στον $F[x]$.

Για τον βαθμό ενός πολυωνύμου ισχύουν τα εξής:

- Τα σταθερά πολυώνυμα έχουν βαθμό 0. Δηλαδή $\deg c=0, c\in F\backslash\{0\}$.
- $\deg(f(x))=\deg(\sum_{\nu=0}^{n}a_\nu x^\nu, a_\nu\neq 0)=n$.
- Το $\deg 0$ δεν ορίζεται.
- $\deg(f+g)\leq\max\{\deg f,\deg g\}$ αλλιώς $f+g=0$.
- $\deg(f\cdot g)=\deg f+\deg g$.

textbfΠαραδείγματα

1. Αν $f(x)=x^5+3x_1$ και $g(x)=6x^7+3x+7$ τότε $\deg f(x)=5, \deg g(x)=7$ και $\deg(f(x))+g(x)=7\leq\max(5,7)$.
2. Αν $f(x)=x^5+6x^2+7$ και $g(x)=-x^5+x^3+10$ τότε $\deg(f(x)+g(x))=3<\max(5,5)$.

Ορισμός 1.3.2 (ισότητα πολυωνύμων)**.** Αν $f(x), g(x)$ δύο πολυώνυμα τότε θα λέμε ότι το f είναι ίσο με το g αν:

- $\deg f(x)=\deg g(x)$ και
- Για κάθε $\nu=0,\ldots,\deg f(x)$ ισχύει ότι $a_\nu=\beta_\nu$.

Αν βρισκόμαστε στον $\mathbb{R}$ ή στον $\mathbb{C}$ τότε τα πολυώνυμα μπορούν να ειδωθούν σαν συναρτήσεις, τις λεγόμενες **πολυωνυμικές συναρτήσεις**, οι οποίες έχουν τη μορφή

$$f:\mathbb{F}\to\mathbb{F}[x]:x\to f(x) \text{ όπου } \mathbb{F}=\mathbb{R} \text{ ή } \mathbb{C} \tag{1.10}$$

Θεώρημα 1.3.2. *Αντίστοιχα με πρίν, τα πολυώνυμα είναι ίσα αν και μόνο αν οι συναρτήσεις είναι ίσες.*

Απόδειξη. Προφανώς, αν τα πολυώνυμα είναι ίσα ($f(x) = g(x)$) τότε και οι αντίστοιχες συναρτήσεις είναι ίσες ($f = g$).

Αντιστρόφως αν οι συναρτήσεις είναι ίσες θα δείξω ότι και τα πολυώνυμα είναι ίσα. Πράγματι,

- Έχω ότι $f(0) = g(0) \Leftrightarrow a_n \cdot 0 \dots a_1 \cdot 0 + a_0 = \beta_n \cdot 0 + \cdots + \beta_1 \cdot 0 + \beta_0 \Leftrightarrow a_0 = \beta_0$.
- Έχω ότι $f'(0) = g'(0) \Leftrightarrow \cdots \Leftrightarrow a_1 = \beta_1$
- Έχω ότι $f''(0) = g''(0) \Leftrightarrow \cdots \Leftrightarrow 2a_2 = 2\beta_2$

$\dots$

- Έχω ότι $f^{(n)}(0)g^{(n)}(0) \Leftrightarrow n!a_n = n!\beta_n$ □

Σημείωση. Η παραπάνω ισοδυναμία δεν ισχύει στα πεπερασμένα σώματα: έστω $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ και θεωρώ το πολυώνυμο $x^3 - x \in \mathbb{F}_3[x]$. Υπολογίζω τις τιμές του πολυωνύμου:

$$0^3 - 0 = 0 \tag{1.11}$$
$$1^3 - 1 = 0 \tag{1.12}$$
$$2^3 - 2 = 6 = 0 \text{ απο το μικρό θεώρημα του Fermat.} \tag{1.13}$$

Έτσι έχουμε ότι το $x^3 - x \in \mathbb{F}_3$ επάγει τη μηδενική συνάρτηση χωρίς να είναι το μηδενικό πολυώνυμο.

1.3.2 Αλγόριθμος της διαίρεσης

Ορισμός 1.3.3 (αλγόριθμος της διαίρεσης)**.** Αν $a(x), \beta(x) \in \mathbb{F}[x]$ τότε υπάρχουν $\pi(x), \upsilon(x) \in \mathbb{F}[x]$ με τις ιδιότητες:

- $a(x) = \beta(x) \cdot \pi(x) + \upsilon(x)$ και
- $\upsilon(x) = 0$ ή $\deg(\upsilon(x)) < \deg(\beta(x))$

Τα $\pi(x), \upsilon(x)$ είναι μοναδικά.

Απόδειξη. Έστω $A = \{a(x) - \beta(x)\tau(x) : t \in \mathbb{F}[x]\}$

- Αν $0 \in A$ τότε υπάρχει $\tau \in \mathbb{F}[x]$ ώστε $a(x) - \beta(x)\tau(x) = 0$ οπότε $\pi(x) = \tau(x)$ και $\upsilon(x) = 0$.
- Αν $0 \notin A$ τότε οι βαθμοί των στοιχείων του A, είναι υποσύνολο του $\mathbb{N}$, μη κενό και έχει ελάχιστο στοιχείο. Έστω $\upsilon(x)$ ώστε το $\upsilon(x) = a(x) - \beta(x)\pi(x)$ να είναι το ελάχιστο στοιχείο του συνόλου. Θα δείξω ότι $\deg \upsilon(x) < \deg \beta(x)$. Έστω ότι $\deg \upsilon(x) \geq \deg \beta(x)$. Υποθέτουμε ότι $\upsilon(x)$ έχει τη μορφή $\upsilon(x) = a_n x^n + a_{n-1}x^{n-1+\cdots+a_0}$ και το $\beta(x) = \beta_m x^m + \beta_{m-1}x^{m-1} + \cdots + \beta_0$.

Παρατηρούμε ότι το πολυώνυμο

$$a_n\beta_m^{-1}x^{n-m}b(x)$$

έχει βαθμό ίσο με $\deg \upsilon(x)$. Έδω χρησιμοποιήσαμε το ότι το στοιχείο β_m είναι αντιστρέψιμο ως μη μηδενικό στοιχείο σώματος και το ότι $n-m \geq 0$. Στην συνέχεια

$$g(x) = \upsilon(x) - \beta_m^{-1}a_n x^{n-m}\beta(x) \in \mathbb{F}[x]$$

με $\deg g(x) < \deg \upsilon(x)$. Δηλαδή έχουμε βρεί ένα στοιχείο του A το οποίο έχει μικρότερο βαθμό από αυτόν που υποθέσαμε ελάχιστο, άτοπο.

Για να αποδείξω τη μοναδικότητα του υπολοίπου αρκεί να υποθέσω οτι υπάρχει και $\upsilon'(x)$ ώστε:

$$\begin{cases} a(x) = \beta(x)\cdot\pi(x) + \upsilon(x), \upsilon(x) = 0 \text{ ή } \deg\upsilon(x) < \deg\beta(x) \\ a(x) = \beta(x)\cdot\pi(x) + \upsilon'(x), \upsilon'(x) = 0 \text{ ή } \deg\upsilon'(x) < \deg\beta(x) \end{cases}$$

Οπότε

$$\beta(x)(\pi(x) - \pi'(x)) = \upsilon'(x) - \upsilon(x)$$

Και διακρίνω τις εξής περιπτώσεις:

- Αν $\upsilon'(x) - \upsilon(x) = 0$ τότε το $F[x]$ είναι ακέραια περιοχή όπότε θα είναι $\pi(x) - \pi'(x) = 0$.
- Αν $\upsilon'(x) - \upsilon(x) \neq 0$ τότε $\deg(\upsilon'(x) - \upsilon(x)) \geq \deg\beta(x)$ και αφού $\upsilon'(x) - \upsilon(x) \neq 0$ θα είναι και $\pi(x) - \pi'(x) \neq 0$. Οπότε θα έχουμε:

  $$\deg\beta(x) > \deg(\upsilon(x) - \upsilon'(x)) = \deg\beta(x) + \deg(\pi(x) - \pi'(x)) \geq \deg\beta(x)$$

  Το οποίο είναι άτοπο.

□

Ορισμός 1.3.4. Θα λέμε ότι το πολυώνυμο $f \in F[x]$ διαιρεί το πολυώνυμο $g \in F[x]$, και θα γράφουμε $f|g$, αν υπάρχει $\pi(x) \in F[x]$ ώστε $f(x) = g(x)\cdot\pi(x)$.

Παρατηρήσεις

1. Κάθε πολυώνυμο διαρεί το 0:

   $$f(x)|0 \Leftrightarrow 0 = f(x)\cdot 0.$$

2. Αν $\phi(x)|\theta(x)$ τότε $\theta(x) = \phi(x)\cdot\pi(x)$ και $\deg\theta(x) \geq \deg\phi(x)$.

3. Αν
   $$\left.\begin{matrix}\phi(x)|\theta(x)\\ \theta(x)|\phi(x)\end{matrix}\right\} \text{τότε } \deg\phi(x) = \deg\theta(x) \iff \phi(x) = c\theta(x), c \in F.$$

4. Ένα πολυώνυμο θα λέγεται μονικό αν είναι της μορφής

   $$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

   δηλαδή αν $a_n = 1$.

5. Κάθε πολυώνυμο μπορεί να γραφεί στη μορφή $f(x) = c \cdot g(x)$ όπου $c \in F$ και g μονικό πολυώνυμο. Η λογική επιλογής του g και του c είναι απλή: παίρνω $c = a_n$ και παρατηρήστε ότι το a_n είναι αντιστρέψιμο γιατί $a_n \in F$ και το F είναι σώμα, άρα επιλέγω τώρα $g = a_n^{-1} f$.

6. Αν $f|g$ και $g|h$ τότε θα ισχύει η μεταβατική ιδιότητα: $f|h$.
Πράγματι,
$$\left.\begin{array}{l} f|g \Rightarrow g = \pi f \\ g|h \Rightarrow h = qg \end{array}\right\} \Rightarrow h = q\pi f \Rightarrow f|h.$$

7. Αν $f|\theta_1$ και $f|\theta_2$ τότε $f|(\pi_1\theta_1 + \pi_2\theta_2)$

8. Το $\mathbb{Z}$ είναι περιοχή κύριων ιδεωδών.

9. Το $F[x]$ είναι περιοχή κύριων ιδεωδών.

   Απόδειξη. Έστω ιδεώδες I του $F[x](I \lhd F[x])$ και $I \neq 0$ (αν $I = 0$ τότε θα ήταν $I = 0F[x]$). Θα θεωρήσουμε $a(x)$ το οποίο:

   (a) $a(x) \neq 0$

   (b) είναι ελάχιστου βαθμού στο I.

   Έστω τώρα g τυχόν στοιχείο. Τότε $g = \pi \cdot a + \upsilon$ και αν $\upsilon \neq 0$ τότε το υ ανήκει στο ιδεώδες και έχει μικρότερο βαθμό από το $a(x)$, άτοπο. □

1.3.3 Ανάγωγα πολυώνυμα

Ορίζουμε τώρα την έννοια του ανάγωγου πολυωνύμου στον δακτύλιο των πολυωνύμων $\mathbb{F}[x]$.

Ορισμός 1.3.5. Ένα πολυώνυμο f ονομάζεται **ανάγωγο** αν, $f = a \cdot \beta$ τότε $a \in \mathbb{F}$ ή $\beta \in \mathbb{F}$.

Το αν είναι ανάγωγο ένα πολυώνυμο σχετίζεται με το χώρο $\mathbb{F}$ στον οποίο βρισκόμαστε. Για παράδειγμα, το πολυώνυμο $f(x) = x^2 - 2$ είναι ανάγωγο στο $\mathbb{Q}$ καθώς $\sqrt{2} \notin \mathbb{Q}$ ενώ δεν είναι ανάγωγο στο $\mathbb{R}$ καθώς $f(x) = (x - \sqrt{2})(x + \sqrt{2})$.

Παρατήρηση. Αν το $\mathbb{F}$ είναι αλγεβρικά κλειστό τότε τα ανάγωγα πολυώνυμα είναι πρωτοβάθμια.

Σημείωση. Ένα σώμα $\mathbb{F}$ ονομάζεται αλγεβρικά κλειστό αν κάθε πολυώνυμο $f(x) \in \mathbb{F}[x]$ έχει μία ρίζα στο $\mathbb{F}[x]$. Έτσι το $\mathbb{C}$ είναι αλγεβρικά κλειστό ενώ το $\mathbb{R}$ δεν είναι καθώς το πολυώνυμο $x^2 + 1$ δεν έχει ρίζα στο $\mathbb{R}$.

1.3.4 Μέγιστος κοινός διαιρέτης πολυωνύμων

Ορισμός 1.3.6. Έστω δύο πολυώνυμα f, g εκ των οποίων το ένα τουλάχιστον είναι διαφορετικό του μηδενός. Ο μέγιστος κοινός διαιρέτης των f, g είναι ένα πολυώνυμο δ το οποίο ικανοποιεί τα εξής:

- $\delta|f$ και $\delta|g$

- το δ είναι μονικό.
- Αν $\delta' | f$ και $\delta' | g$ τότε $\delta' | \delta$.

Πρόταση 1.3.3. *Ο μέγιστος κοινός διαιρέτης των f, g είναι ο γεννήτορας του κυρίου ιδεώδους που παράγουν τα f, g. Δηλαδή, $\delta\mathbb{F}[x] = \langle f, g \rangle$ όπου το δ στο $\delta\mathbb{F}[x]$ είναι ο μέγιστος κοινός διαιρέτης των f, g και $\langle f, g \rangle$ είναι όλες οι εκφράσεις που μπορώ να σχηματίσω απο τα f, g : $af + \beta g, a, \beta \in \mathbb{F}[x]$.*

Απόδειξη. Αν $\delta \in \langle f, g \rangle$ τότε το δ θα είναι στη μορφή $\delta = af + \beta g$ και έστω $\delta' | f, \delta' | g$ τότε θα είναι $\delta' | \delta$ από την 3η ιδιότητα του μέγιστου κοινού διαιρέτη. Επίσης αν $f, g \in \delta\mathbb{F}[x]$ τότε θα είναι $\delta | f$ και $\delta | g$ οπότε $\delta | af + \beta g$ οπότε $\delta | \delta'$ □

Στον δακτύλιο των ακεραίων ο μέγιστος κοινός διαιρέτης δύο αριθμών γράφεται στη μορφή

$$\text{μκδ}(x, y) = ax + \beta y, \text{ για κάποια } a, \beta \in \mathbb{Z}.$$

Ανάλογα στον δακτύλιο των πολυωνύμων ο μέγιστος κοινός διαιρέτης δύο πολυωνύμων έχει τη μορφή:

$$\text{μκδ}(f(x), g(x)) = af(x) + \beta g(x) \text{ όπου } a, \beta \in \mathbb{F}[x]$$

1.4 Μάθημα 4.

Τετάρτη 21.3.2012

Ο βασικός μας στόχος σε αυτό το κεφάλαιο είναι να αποδείξουμε ότι κάθε μη σταθερό πολυώνυμο έχει μία ρίζα σε μία κατάλληλη επέκταση του σώματος μας.

Έστω δύο πολυώνυμα f, g στον δακτύλιο $F[x]$ των πολυωνύμων. Τότε ισχύει ότι $\text{μκδ}(f, g) = \delta F[x]$ όπου $\delta F[x]$ είναι ο γεννήτορας του κύριου ιδεώδους που παράγουν τα f, g[2]. Επιπλέον $\text{εκπ}(f, g) = fF[x] \cap gF[x] = \pi F[x]$ όπου με π συμβολίζουμε το ελάχιστο κοινό πολλαπλάσιο.

Παράδειγμα 1.4.1. $12\mathbb{Z} \cap 3\mathbb{Z} = 12\mathbb{Z}$. Δηλαδή οι αριθμοί που είναι ταυτόχρονα πολλαπλάσια του 12 και πολλαπλάσια του 3 είναι ακριβώς τα πολλαπλάσια του ελάχιστου κοινού πολλαπλασίου που εδώ τυχαίνει να είναι το 12.

1.4.1 Επέκταση σώματος

Ορίζουμε τώρα την επέκταση ενός σώματος *(Εισαγωγή στην άλγεβρα, J. B. Fraleigh, σελ. 416)*

Ορισμός 1.4.1 (επέκταση σώματος)**.** Ένα σώμα E λέγεται **επέκταση σώματος** ενός σώματος F αν $F \leq E$, δηλαδή αν το F είναι υπόσωμα του E.

[2]Πρόταση 1.3.4

Έστω τώρα ένα στοιχείο $c \in E$ και απεικόνιση $\phi_c : F[x] \to E : f(x) \mapsto f(c)$. Η παραπάνω απεικόνιση είναι ομομορφισμός:

$$\begin{aligned} \phi_c(f+g) &= (f+g)(c) = f(c) + g(c) = \phi_c f + \phi_c g \\ \phi_c(f \cdot g) &= (f \cdot g)(c) = f(c) \cdot g(c) = \phi_c(f) \cdot \phi_c(g) \end{aligned} \tag{1.14}$$

Παρατηρήσεις

1. Αν ο πυρήνας της ϕ_c είναι διαφορετικός του κενού (δηλαδή $\ker \phi_c \neq \emptyset$) τότε το c λέγεται **αλγεβρικό** πάνω από το το F. Αν το c είναι αλγεβρικό πάνω απο το F τότε υπάρχει πολυώνυμο $f \in F$ ώστε $f \in \ker \phi_c$, δηλαδή $f(c) = 0$. Αν ένα στοιχείο δεν είναι αλγεβρικό πάνω απο το F τότε λέγεται υπερβατικό πάνω από το F.

2. Ο πυρήνας $\ker \phi_c$ είναι κύριο ιδεώδες του F:

$$\ker \phi_c = fF[x] \tag{1.15}$$

   όπου $f \in \ker \phi_c$.

3. Ισχύει η εξής ισοδυναμία:

$$g(c) = 0 \Leftrightarrow f \mid g. \tag{1.16}$$

1.4.2 Αλγεβρική επέκταση σώματος

(Εισαγωγή στην άλγεβρα, J. B. Fraleigh, σελ. 447)

Μία επέκταση E/F λέγεται αλγεβρική αν κάθε $a \in E$ είναι αλγεβρικό στοιχείο υπέρ του F.

Ορισμός 1.4.2 (Πεπερασμένη επέκταση)**.** Αν μία επέκταση E ενός σώματος F έχει πεπερασμένη διάσταση n ως διανυσματικός χώρος πάνω από το F, τότε το F λέγεται πεπερασμένη επέκταση βαθμού n πάνω από το F. Θα συμβολίζουμε με $[E : F]$ το βαθμό n του E πάνω από το F.

Θεώρημα 1.4.1. *Αν E/F μια πεπερασμένη επέκταση σώματος και K/E τότε το K είναι μία πεπερασμένη επέκταση σώματος του F και*

$$[K : F] = [K : E][E : F]$$

Στο μάθημα της γραμμικής άλγεβρας έχουμε συναντήσει το τύπο

$$\dim_{\mathbb{R}} V = \dim_{\mathbb{C}} V \cdot \dim_{\mathbb{R}} \mathbb{C}$$

που είναι μια ειδική μορφή του παραπάνω θεωρήματος.

Θεώρημα 1.4.2. *Αν $[E : F] < \infty$ τότε η E/F είναι αλγεβρική.*

Απόδειξη. Έστω $x \in E$ και θεωρώ τις δυνάμεις με βάση x: $1, x, x^2, x^3, \ldots, x^n$. Αν επιλέξουμε ένα αρκετά μεγάλο n ώστε $n > [E : F]$ τότε τα $1, x, x^2, \ldots x^n$ θα είναι γραμμικά εξαρτημένα.

Απο τη γραμμική άλγεβρα είναι γνωστό ότι *το μέγιστο πλήθος των γραμμικά ανεξάρτητων διανυσμάτων είναι* $\dim V$, άρα θα υπάρχουν $\lambda_1, \lambda_2, \ldots, \lambda_n \in F$ με $(\lambda_1, \lambda_2, \ldots, \lambda_n) \neq 0$ ώστε

$$\lambda_n x^n + \lambda_{n-1} x^{n-1} + \cdots + \lambda_1 x + \lambda_0 = 0 \tag{1.17}$$

και αν παρατηρήσατε, η σχέση 1.17 ορίζει ένα πολυώνυμο f το οποίο για το μηδενίζεται στο x άρα $f \in \ker \phi_x$ άρα το x είναι αλγεβρικό στοιχείο και αφού η επιλογή του x ήταν τυχαία θα ισχύει ότι η επέκταση του F στο E είναι αλγεβρική.

□

Παρατήρηση. Το αντίθετο του παραπάνω θεωρήματος δεν ισχύει. Δηλαδή υπάρχουν αλγεβρικές επεκτάσεις που δεν είναι πεπερασμένες.

Για παράδειγμα το σώμα $\bar{\mathbb{Q}}$ των αλγεβρικών αριθμών είναι μία άπειρου βαθμού αλγεβρική επέκταση του $\mathbb{Q}$.

Δίνουμε τώρα των ορισμό την αλγεβρικής κλειστότητας [3]

Ορισμός 1.4.3 (κλειστότητα)**.** Για ένα σώμα K η **αλγεβρική κλειστότητα** του K ορίζεται να είναι το μικρότερο σώμα που περιέχει το K ώστε κάθε πολυώνυμο $f \in K[x]$ να έχει όλες τις ρίζες του στο $\bar{K}$, όπου με $\bar{K}$ συμβολίζουμε την αλγεβρική κλειστότητα του K.

Παράδειγμα 1.4.2. Εξετάζω αν υπάρχει η αλγεβρική κλειστότητα του $\mathbb{Q}$:
Θεωρώ το σύνολο:

$$\Sigma = \{\mathbb{Q} \subset A \text{ όπου } A \text{ σώμα και όλες οι ρίζες κάθε πολυωνύμου στο } \mathbb{Q}[x] \text{ ανήκουν στο } A\}$$

Παρατηρήστε ότι $\Sigma \neq \emptyset$ διότι $\mathbb{C} \in \Sigma$. Άρα

$$\bar{\mathbb{Q}} = \bigcap_{A \in \Sigma} A \tag{1.18}$$

Θεώρημα 1.4.3. *Για κάθε ανάγωγο πολυώνυμο $f \in F[x]$ υπάρχει επέκταση K του F στην οποία το f αποκτά ρίζα.*[4]

Σημείωση. Η απόδειξη του παραπάνω θεωρήματος λόγω μεγέθους παραλείπεται αλλά μπορεί να βρεθεί στο *(Εισαγωγή στην άλγεβρα, J. B. Fraleigh, σελ. 417)*

Η επιλογή της κατάλληλης επέκτασης σώματος θα γίνεται θεωρώντας:

$$E = K[x]/f(x)K[x] \tag{1.19}$$

Για παράδειγμα ας εξετάσουμε το $\mathbb{R}$ και το πολυώνυμο $x^2 + 1$. Το σύνολο

$$E = \mathbb{R}[x]/\langle x^2 + 1 \rangle$$

είναι σώμα και εξετάζω

[3] στο βιβλίο του Fraleigh αποδίδεται σαν θήκη και ο ορισμός είναι στη σελίδα 453.
[4] το παραπάνω θεώρημα είναι γνωστό στη βιβλιογραφία σαν θεώρημα του Kronecker.

Σημείωση. Με $f(x) \bmod (x^2+1)$ θα συμβολίζουμε το υπόλοιπο της διαίρεσης του $f(x)$ με x^2+1.

Δίνουμε τώρα τους ορισμούς του πρώτου και του μέγιστου ιδεώδους που χρειάζονται για το επόμενο θεώρημα.

Ορισμός 1.4.4 (πρώτο ιδεώδες)**.** Ένα ιδεώδες P είναι πρώτο αν για κάθε $f, g \in P$ ισχύει ότι $f \in P$ ή $g \in P$.

Ορισμός 1.4.5 (μέγιστο ιδεώδες)**.** Ένα ιδεώδες P είναι μέγιστο αν για κάθε άλλο ιδεώδες I του ίδιου δακτυλίου με $P \leq I \leq R$ ισχύει ότι $P = I$ ή $P = R$.

Θεώρημα 1.4.4. *Έστω R μεταθετικός δακτύλιο και P ιδεώδες του $R (P \lhd R)$. Τότε:*

- *Ο δακτύλιος πηλίκο R/P είναι ακέραια περιοχή αν και μόνο το P είναι πρώτο.*
- *Ο δακτύλιος πηλίκο R/P είναι σώμα αν και μόνο αν το P είναι μέγιστο.*

Θεώρημα 1.4.5. *Σε ένα δακτύλιο πολυωνύμων τα παρακάτω είναι ισοδύναμα:*

- *Το πολυώνυμο f είναι ανάγωγο.*
- *Το $fR[x]$ είναι μέγιστο.*
- *Ο δακτύλιος πηλίκο $R/fR[x]$ είναι σώμα.*

Η απόδειξη της πρώτης ισοδυναμίας βρίσκεται στο βιβλίο *Εισαγωγή στην άλγεβρα* του *Fraleigh* στη σελίδα 374. Η απόδειξη της δεύτερης ισοδυναμίας είναι στο ίδιο βιβλίο στη σελίδα 369.

Διατυπώνουμε τώρα ένα θεώρημα που είναι γνωστό σαν «το όνειρο του πρωτοετή» (“The Freshman dream”):

Θεώρημα 1.4.6. *Σε ένα σώμα χαρακτηριστικής $p > 0$ ισχύει ότι:*

$$(a+\beta)^{p^n} = a^{p^n} + \beta^{p^n}$$

Απόδειξη. Για $n = 1$ έχουμε Ισχύει ότι $(a+\beta)^p = \sum_{\tau=0}^{p} \binom{p}{\tau} a^\tau \beta^{p-\tau}$ όπου $\binom{p}{\tau} = \frac{p!}{\tau!(p-\tau)!}$ για $1 \leq \tau \leq p-1$ όμως βρισκόμαστε σε ένα σώμα χαρακτηριστικής p άρα όλα τα πολλαπλάσια του p θα είναι ίσα με το μηδέν, άρα και $\binom{p}{\tau} = 0$ για $1 \leq \tau \leq p-1$ οπότε έχω ότι

$$(a+\beta)^p = \binom{p}{0} a^0 \beta^p + \binom{p}{p} a^p b^0 = a^p + \beta^p$$

Για γενικό n παρατηρούμε ότι

$$(a+b)^{p^n} = ((a+b)^p)^{p^{n-1}} = (a^p + b^p)^{p^{n-1}},$$

και η απόδειξη γίνεται με επαγωγή.

□

1.5 Μάθημα 5.

Δευτέρα 26.3.2012

Έστω E/F επέκταση σωμάτων. Για κάθε $c \in E$ θεωρούμε την συνάρτηση $F[x] \to E$, $f(x) \mapsto f(c)$. Ο δακτύλιος $F[c]$ είναι σώμα αν και μόνο αν το c είναι αλγεβρικό υπέρ του F.

Γενικά με $F[c]$ θα συμβολίζουμε όλες τις πολυωνυμικές εκφράσεις που μπορούμε να σχηματίσουμε με στοιχεία του F και με το c ενώ με $F(c)$ θα συμβολίζουμε τις ρητές εκφράσεις. Αν το $F[c]$ είναι σώμα τότε $F[c] = F(c)$.

Ισχύει ότι ο βαθμός επέκτασης $[F(c) : F]$ είναι ίσος με τον βαθμό του ελαχίστου πολυωνύμου του c.

Θεώρημα 1.5.1. *Για κάθε πολυώνυμο $f(x) \in K[x]$ υπάρχει επέκταση που όλες οι ρίζες του σώματος να ανήκουν σε αυτή. Θα λέμε* σώμα ριζών *το μικρότερο δυνατό σώμα με αυτή την ιδιότητα.*

Στην πραγματικότητα αν γνωρίζουμε ότι υπάρχουν αλγεβρικά κλειστά σώματα που περιέχουν το K τότε το σύνολο των σωμάτων στα οποία υπάρχουν όλες οι ρίζες του πολυωνύμου f είναι μη κενό. Το ελάχιστο σώμα μπορεί να οριστεί ως:

$$E := \cap_{A \in I} A,$$

όπου

$$I = \{\text{το σύνολο των σωμάτων ώστε όλες οι ρίζες του } f \text{ να ανήκουν σε αυτό.}\}$$

Στην γενική περίπτωση μπορούμε να δουλέψουμε με επαγωγή στον βαθμό. Αν το πολυώνυμο μας έχει βαθμό 1 τότε οι ρίζες του ανήκουν στο σώμα K και δεν χρειάζεται να θεωρήσουμε επέκταση. Ας υποθέσουμε ότι για κάθε πολυώνυμο βαθμού $k < n$ και για κάθε σώμα F' υπάρχει μια επέκταση E ώστε όλες οι ρίζες του να ανήκουν στο . Αν f είναι πολυώνυνο βαθμού n τότε μπορούμε να θεωρήσουμε έναν ανάγωγο παράγοντα του g. Στο σώμα $K[x]/\langle g \rangle$ το g έχει μία ρίζα ρ. Άρα στο (ρ) έχουμε ότι το $f = (x - \rho)h(x)$ και το $h(x)$ είναι βαθμού $n - 1$ άρα υπάρχει επέκταση E του $K(\rho)$ στην οποία το f να έχει όλες του τις ρίζες και να διασπάται σε γινόμενο πρωτοβαθμίων παραγόντων.

Ισχύει ότι

Θεώρημα 1.5.2. *Δύο σώματα ριζών του πουλυωνύμου F είναι ισόμορφα.*

Αποδείξαμε ότι ισχύει το "θεώρημα του Fermat"

Θεώρημα 1.5.3. *Σε κάθε σώμα F με p^n στοιχεία για κάθε $a \in F$ ισχύει ότι*

$$a^{p^n} = a.$$

Έστω ένα σώμα με p^n στοιχεία. Το θεώρημα του Fermat μας δίνει ότι οι ρίζες του πολυώνυμου $x^{p^n} - x$ είναι ακριβώς το F. Πράγματι κάθε $a \in F$ είναι ρίζα του $x^{p^n} - x$ και σε σώμα ένα πολυώνυμο βαθμού n έχει το πολύ n ρίζες.

Κάνοντας χρήση του θεωρήματος 1.5.2 βλέπουμε ότι δύο οποιαδήποτε σώματα με p^n στοιχεία είναι αναγκαστικά ισόμορφα.

Θεωρούμε τον τελεστή παραγώγισης

$$\frac{d}{dx} : K[x] \to K[x]$$

$$f = \sum_{\nu=0}^{n} a_\nu x^\nu \mapsto \sum_{\nu=1}^{n} \nu a_\nu x^{\nu-1}.$$

Ο παραπάνω ορισμός δεν απαιτεί καθόλου την έννοια του όριου. Επιπλέον μπορούμε να αποδείξουμε ότι ικανοποιεί τις ιδιότητες της παραγώγου δηλαδή

$$\frac{d}{dx}(f+g) = \frac{d}{dx}f + \frac{d}{dx}g$$

και

$$\frac{d}{dx}(fg) = f\frac{d}{dx}g + g\frac{d}{dx}f.$$

Πρόταση 1.5.4. *Ένα πολυώνυμο έχει διπλή ρίζα στο a αν και μόνο αν $\frac{d}{dx}f(a) = 0$.*

Απόδειξη. Αν $f(x) = (x-a)^n g(x)$ με $n \geq 2$ τότε

$$\frac{d}{dx}(x-a)^n g(x) = n(x-a)^{n-1}g(x) + (x-a)^n \frac{d}{dx}g,$$

και η παραπάνω ποσότητα μηδενίζεται στο a.

Αντιστρόφως αν $f(a) = 0$ και $\frac{d}{dx}f(a) = 0$ τότε γράφουμε

$$f(x) = (x-a)h(x), \quad \frac{d}{dx}f = h(x) + (x-a)\frac{d}{dx}h(x)$$

και συμπεραίνουμε ότι $h(a) = 0$ δηλαδή έχουμε διπλή ρίζα στο a.

□

Θεώρημα 1.5.5. *Η πολλαπλασιαστική ομάδα ενός πεπερασμένου σώματος είναι μία κυκλική ομάδα.*

Απόδειξη. Γνωρίζουμε ότι η πολλαπλασιαστική ομάδα G του σώματος είναι αβελιανή με τάξη $p^n - 1$. Από το θεώρημα ταξινόμησης των πεπερασμένων αβελιανών ομάδων αυτή θα είναι της μορφής

$$G = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}.$$

Έστω m το έλαχιστο κοινό πολλαπλάσιο των $n_1, \ldots, n_r$. Ισχύει ότι $m < n_1 \cdot n_2 \cdots n_r$. Ας θεωρήσουμε ένα στοιχείο $a = (a_1, \ldots, a_r)$ όπου τα a_i είναι στοιχεία των ομάδων $\mathbb{Z}/n_i\mathbb{Z}$. Παρατηρούμε ότι $a_i^{n_i} = 1$ και συνεπώς $a_i^m = 1$. Άρα $a^m = 1$. Όμως σε ένα σώμα η εξίσωση $x^m = 1$ έχει το πολύ m ρίζες άρα $m = q - 1$. Αυτό σημαίνει ότι $(n_i, n_j) = 1$ και ότι η ομάδα G είναι κυκλική. □

Ορισμός 1.5.1. Κάθε γεννήτορας της κυκλικής ομάδας F^* θα λέγεται πρωταρχικό στοιχείο.

Παράδειγμα 1.5.1. Στο σώμα με επτά στοιχεία έχουμε $\mathbb{F}_7^* = \{1, 2, 3, 4, 5, 6\}$. Παρατηρούμε ότι οι δυνάμεις του 2 είναι $\{2, 2^2 = 4, 2^3 = 8 = 1$, άρα το 2 δεν μπορεί να παράγει όλοκληρη την πολλαπλασιαστική ομάδα. Παρατηρούμε ότι οι δυνάμεις του 3 είναι $3, 3^2 = 9 = 2 \mod 7$ και το 3 είναι γεννήτορας.

Πρόταση 1.5.6. *Σε μια κυκλική ομάδα με γεννήτορα a και τάξη m το στοιχείο a^i έχει τάξη $m/(i, m)$.*

Απόδειξη. Πράγματι αν s είναι η τάξη του a^i τότε $a^{is} = 1$ και έτσι $m \mid is$. Συνεπώς $m/(i, m) \mid s$ (γιατί; κάντε ανάλυση σε πρώτους παράγοντες!) Από την άλλη $(a^i)^{m/(i,m)} = a^{im/(i,m)} = 1$. Άρα $s \mid m/(i, m)$ το οποίο ολοκληρώνει την απόδειξη. □

Σε μία κυκλική ομάδα με τάξη m υπάρχουν $\phi(m)$ γεννήτορες. Συνεπώς ένα σώμα με p^n στοιχεία έχει $\phi(p^n - 1)$ πρωταρχικά στοιχεία.

Πρόταση 1.5.7. *Για κάθε p^n δύναμη πρώτου υπάρχει σώμα με p^n στοιχεία*

Απόδειξη. Θεωρούμε το σώμα ριζών του πολυωνύμου $x^{p^n} - x \in \mathbb{F}_p[x]$. Παρατηρούμε ότι οι p^n απλές ρίζες του (η παράγωγος είναι σταθερά) αποτελούν σώμα αφού το άθροισμα δύο ριζών και το γινόμενο δύο ριζών είναι ρίζα. Ας θυμηθούμε ότι σε σώματα χαρακτηριστικής p ισχύει ότι $(a + b)^{p^n} = a^{p^n} + b^{p^n}$. Άρα το σώμα ριζών είναι το σύνολο των ριζών που έχει ακριβώς p^n στοιχεία. □

Πρόταση 1.5.8. *Αν έχουμε ένα υπόσωμα K ένος σώματος F με p^n στοιχεία τότε το υπόσωμα θα έχει p^d στοιχεία με $d \mid n$. Αντιστρόφως για κάθε $d \mid n$ υπάρχει μοναδικός υπόσωμα του F με p^d στοιχεία.*

Απόδειξη. Το υπόσωμα K θα είναι επίσης πεπερασμένης χαρακτηριστική και θα έχει p^d στοιχεία, όπου $d = [K : \mathbb{F}_p]$. Ισχύει ότι $n = [F : \mathbb{F}_p] = [F : K][K : \mathbb{F}_p]$ άρα $d \mid n$.

Αντιστρόφως αν $d \mid n$ τότε $p^d - 1 \mid p^n - 1$. Πράγματι

$$(p^n - 1) = (p^d)^{n/d} - 1 = (p^d - 1)(1 + p^d + p^{2d} + \cdots + p^{d(n/d-1)}).$$

Άρα $x^{p^d-1} - 1 \mid x^{p^n-1}$ και συνεπώς $x^{p^d} - x \mid x^{p^n} - x$. Το σώμα ριζών του $x^{p^d} - x$ έχει p^d στοιχεία και δεν υπάρχει άλλο αφού κάθε άλλο στοιχείο ενός σώματος με p^d στοιχεία θα έπρεπε να είναι ρίζα του $x^d - x$. □

Το πλήθος των υποσωμάτων ενός σώματος με p^n στοιχεία είναι ίσο με το πλήθος των διαιρετών του n.

Πρόταση 1.5.9. *Για κάθε F πεπερασμένο σώμα με p^k το πλήθος στοιχεία και κάθε n υπάρχει ανάγωγο πολυώνυμο βαθμού n.*

Απόδειξη. Γνωρίζουμε ότι υπάρχει σώμα με p^{nk} στοιχεία. Ένα πρωταρχικό στοιχείο ζ του E έχει την ιδιότητα $E = F(\zeta)$. Ο βαθμός της επέκτασης $F(\zeta)/F$ είναι ίσος με τον βαθμό του

ελαχίστου πολυωνύμου του ζ δηλαδή n. Το ελάχιστο πολυώνυμο του ζ είναι το ζητούμενο ανάγωγο πολυώνυμο. □

Θεώρημα 1.5.10. *Έστω F ένα πεπερασμένο σώμα με p^n το πλήθος στοιχεία. Θεωρούμε ένα ανάγωγο πολυώνυμο $\sigma(x) \in F[x]$. Αν ζ είναι μία ρίζα του τότε το σώμα ριζών του είναι το $F(\zeta)$.*

Απόδειξη. Το σώμα $F(\zeta)$ μας δίνει ένα σώμα με p^{nd} στοιχεία όπου d είναι ο βαθμός του $\sigma(x)$. Άρα το $F(\zeta)$ είναι το σώμα ριζών του $x^{p^{nd}} - x$. Το $\sigma(x)$ διαιρεί το $x^{p^{nd}} - x$. Συνεπώς όλες οι ρίζες του $\sigma(x)$ είναι και ρίζες του $x^{p^{nd}} - x$. □

Παρατήρηση. Σε σώματα χαρακτηριστικής μηδέν το θεώρημα 1.5.10 δεν είναι σωστό. Θεωρήστε το $x^3 - 2 \in \mathbb{Q}[x]$. Επισυνάπτοντας την ρίζα $\sqrt[3]{2} \in \mathbb{R}$ στο $\mathbb{Q}$ έχουμε το σώμα $\mathbb{Q}(\sqrt[3]{2})$. Το σώμα αυτό δεν περιέχει τις άλλες ρίζες $\sqrt[3]{2}\omega$ και $\sqrt[3]{2}\omega^2$ όπου ω είναι μία πρωταρχική τρίτη ρίζα του 1.

Πρόταση 1.5.11. *Έστω F σώμα με q στοιχεία και $\sigma(x)$ ανάγωγο πολυώνυμο βαθμού d. Το $\sigma(x) \mid x^{q^n} - x$ αν και μόνο αν $d \mid n$.*

Απόδειξη. Το σώμα $F(c)$ όπου c ρίζα του $\sigma(x)$ είναι σώμα με q^d στοιχεία. Το σώμα ριζών του $x^{q^n} - x$ με q^n έχει ένα υπόσωμα με q^d στοιχεία αν και μόνο αν $d \mid n$. □

Θεώρημα 1.5.12. *Έστω F σώμα με $q = p^n$ το πλήθος στοιχεία και c μία ρίζα του ανάγωγου πολυωνύμου $\sigma(x)$ βαθμού d. Όλες οι ρίζες του $\sigma(x)$ είναι οι $c, c^q, c^{q^2}, \ldots, c^{q^{d-1}}$.*

Απόδειξη. Παρατηρήστε ότι η απεικόνιση $x \mapsto x^q$ διατηρεί σταθερό το σώμα F συνεπώς στέλνει ρίζες του σ σε ρίζες του σ. □

Παρατήρηση. Παρατηρήστε ότι το παραπάνω θεώρημα είναι το ανάλογο του γνωστού θεωρήματος σχετικά με τις ρίζες πολυωνύμων $\sigma(x) \in \mathbb{R}[x]$. Αν έχουμε μια ρίζα c τότε και ο συζυγής $\bar{c}$ είναι ρίζα.

1.6 Μάθημα 6.

Τετάρτη 28.3.2012

Θεώρημα 1.6.1. *Αν f είναι ένα πολυώνυμο τότε ισχύει η εξής ισοδυναμία:*

$$\textit{Το } f \textit{ έχει πολλαπλή ρίζα στο } a \iff f(a) = 0 \textit{ και } \frac{\mathrm{d}f}{\mathrm{d}x}(a) = 0$$

Απόδειξη. Ξεκινώ με τη δεξιά φορά ($\Rightarrow$). Αφού το f έχει πολλαπλή ρίζα στο a θα έχει την εξής μορφή:

$$f(x) = (x-a)^n h(x) \tag{1.20}$$

η οποία αν την παραγωγίσω παίρνει τη μορφή:

$$\frac{\mathrm{d}f}{\mathrm{d}x} = n(x-a)^{n-1}h(x) + (x-a)^n \frac{\mathrm{d}}{\mathrm{d}x}h(x) \tag{1.21}$$

Οπότε για $x = a$ θα έχω:

$$\frac{\mathrm{d}f}{\mathrm{d}x}(a) = 0 \tag{1.22}$$

Αντίστροφα τώρα, αν $f(a) = 0$ θα ισχύει ότι $f(x) = (x-a)h(x)$ άρα

$$\frac{\mathrm{d}f}{\mathrm{d}x} = (x-a)\frac{\mathrm{d}h(x)}{dx} + h(x) \tag{1.23}$$

οπότε για $x = a$ θα έχω

$$\frac{\mathrm{d}f}{dx}(a) = 0 + h(a) \tag{1.24}$$

και αφού $\dfrac{\mathrm{d}f}{dx}(a) = 0$ θα έχω ότι

$$h(a) = 0 \tag{1.25}$$

Οπότε το $h(x)$ θα είναι της μορφής $h(x) = (x-a)g(x)$ και η f θα είναι:

$$f(x) = (x-a)h(x) = (x-a)^2 g(x) \tag{1.26}$$

□

Παρατήρηση. Χρησιμοποιήθηκε το ότι: $f(a) = 0 \iff (x-a) \mid f(x)$

Πόρισμα. Το παραπάνω θεώρημα είναι αρκετά χρήσιμο καθώς μας επιτρέπει να γνωρίζουμε πότε ένα πολυώνυμο έχει απλές ρίζες. Για παράδειγμα, το $x^{p^n} - x$ έχει απλές ρίζες μιας και $\dfrac{\mathrm{d}}{\mathrm{d}x}(x^{p^n} - x) = p^n x^{p^n - 1} \equiv -1 \neq 0$

Θεώρημα 1.6.2. *Το σύνολο των ριζών του $x^{p^n} - x$ είναι σώμα.*

Απόδειξη. Θα δείξουμε ότι αν ρ, σ ρίζες τότε και τα $\rho + \sigma, \rho \cdot \sigma$ είναι ρίζες.

- Αφού το ρ είναι ρίζα του $x^{p^n} - x$ θα ισχύει ότι $\rho^{p^n} = \rho$
- Αφού το σ είναι ρίζα του $x^{p^n} - x$ θα ισχύει ότι $\sigma^{p^n} = \sigma$ Άρα θα έχω ότι:

$$(\rho + \sigma)^{p^n} = \rho^{p^n} + \sigma^{p^n} \tag{1.27}$$

και

$$(\rho \cdot \sigma)^{p^n} = \rho^{p^n} \cdot \sigma^{p^n} \tag{1.28}$$

Το σύνολο των ριζών του $x^{p^n} - x$ είναι σώμα με p^n στοιχεία (αφού οι ρίζες είναι απλές). Δηλαδή δείξαμε ότι για κάθε p^n υπάρχει ένα σώμα με p^n στοιχεία

$$\begin{array}{ccc} \mathbb{F}_{p^n} & \longleftarrow & \text{σώμα ριζών του } x^{p^n} - x \\ \Big\downarrow n & & \\ \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} & & \end{array}$$

Όπου n είναι ο βαθμός της επέκτασης με $\dim[\mathbb{F}_{p^n} : \mathbb{F}_p]$. Το σώμα ριζών είναι μοναδικό μέχρι ισομορφισμού. Άρα οποιαδήποτε δύο σώματα με p^n στοιχεία είναι ισόμορφα.

Δεύτερη απόδειξη. Έστω K, L δύο σώματα με p^n στοιχεία. Η πολλαπλασιαστικες ομάδες του K και του L, σύμφωνα με το θεώρημα 1.5.5, είναι δύο κυκλικές ομάδες με γεννήτορες $\langle a \rangle$ και $\langle \beta \rangle$ αντίστοιχα. Έστω τώρα $f : K^* \to L^*$ με $a \mapsto b$??

□

1.7 Μάθημα 7.

Δευτέρα 2.4.2012

1.7.1 Επανάληψη στα πεπερασμένα σώματα

(Εισαγωγή στην άλγεβρα, J. B. Fraleigh, σελ. 469)

Στο μάθημα αυτό θα κάνουμε μία επανάληψη όσων έχουν ειπωθεί στα προηγούμενα μαθήματα. Καταρχάς μιλάμε για σώματα πεπερασμένου πλήθους στοιχείων. Θα επαναλάβουμε κάποιες χαρακτηριστικές ιδιότητες των σωμάτων αυτών:

1. Αν E ένα πεπερασμένο σώμα χαρακτηριστικής p, τότε το E θα περιέχει ακριβώς p^n στοιχεία.
2. Για κάθε p^n δύναμη πρώτου υπάρχει μοναδικό (μέχρι ισομορφισμού) σώμα με p^n στοιχεία. Αυτό είναι το σώμα ριζών του $x^{p^n} - x$, δηλαδή κάθε στοιχείο του $\mathbb{F}_{p^n}$ ικανοποιεί την $x^{p^n} - x = 0$. Αντίστροφα, αν ψάχνω ένα σώμα με p^n στοιχεία αρκεί να θεωρήσω το σώμα ριζών του $x^{p^n} - x$.
3. Μιας και το σώμα με πλήθος στοιχείων p^n είναι μοναδικό, επιλέξαμε να το συμβολίζουμε με $\mathbb{F}_{p^n}$.
4. Στην περίπτωση που ο p είναι πρώτος ισχύει ότι $\mathbb{F}_{p^n} = \mathbb{Z}/p\mathbb{Z}$.

   Σημείωση. **Δεν** ισχύει ότι $\mathbb{F}_{p^n} = \mathbb{Z}/p^n\mathbb{Z}$.
5. Η πολλαπλασιαστική ομάδα όλων των μη μηδενικών στοιχείων ενός πεπερασμένου σώματος, με τον πολλαπλασιασμό του σώματος είναι κυκλική. Δηλαδή η,

   $$\mathbb{F}^*_{p^n} = \mathbb{F}_{p^n} \backslash \{0\}$$

   είναι κυκλική τάξης $p^n - 1$.
6. Κάθε γεννήτορας της κυκλικής αυτής ομάδας λέγεται πρωταρχικό στοιχείο.
7. Το ελάχιστο πολυώνυμο που παράγεται από το πρωταρχικό στοιχείο λέγεται πρωταρχικό πολυώνυμο.
8. Υπάρχουν $\phi(p^n - 1)$ πρωταρχικές ρίζες της κυκλικής ομάδας $\mathbb{F}^*_{p^n}$, όπου $\phi(p^n - 1)$ είναι το πλήθος των $\{i, 0 \leq i < p^n - 1 : (i, p^n - 1) = 1\}$.

Θεώρημα 1.7.1. *Έστω $\sigma(x)$ ανάγωγο και μονικό πολυώνυμο στο $\mathbb{F}_q$, όπου με q απο εδώ και στο εξής θα συμβολίζουμε το p^n. Τότε θα ισχύει η ισοδυναμία:*

$$\sigma(x) = x^{q^n} - x \text{ αν και μόνο αν } \deg \sigma(x) = d \mid n.$$

Απόδειξη. Το ανάγωγο πολυώνυμο $\sigma(x)$ ορίζει μία επέκταση βαθμού d στο $\mathbb{F}_q$. Παρατηρούμε ότι ισχύει: $\sigma(x) \mid x^{q^n} - x$ αν και μόνο αν κάθε ρίζα του $\sigma(x)$ είναι και ρίζα του $x^{q^n} - x$. Το $\sigma(x)$ μπορεί να γραφεί στη μορφή $\prod(x - p_i)$ και το $x^{q^n} - x$ στη μορφή $\prod(x - p)$ με $p \in \mathbb{F}_{q^n}$. Το σώμα ριζών του $\sigma(x)$ είναι υπόσωμα του σώματος ριζών του $x^{q^n} - x$ αν και μόνο αν $d \mid n$

$\mathbb{F}_{q^n}$ ⟵ σώμα ριζών του $x^{q^n} - x$

$\downarrow$

$\mathbb{E}$ ⟵ σώμα ριζών του $\sigma(x)$

$\downarrow$

$\mathbb{F}_q$

??? □

Πρόταση 1.7.2. *Έστω ένα πολυώνυμο f του $\mathbb{R}[x]$. Τότε αν $\rho \in \mathbb{C}$ είναι μία ρίζα του f, τότε και ο συζυγής $\bar{\rho}$ είναι ρίζα του f.*

Παρατήρηση. Η απόδειξη της παραπάνω πρότασης βρίσκεται στο βιβλίο "Εισαγωγή στην άλγεβρα" του Fraleigh, στη σελίδα 479 (απόδειξη του πορίσματος 2).

Πρόταση 1.7.3. *'Εστω ένα πολυώνυμο f του $\mathbb{F}_q[x]$. Τότε αν $\rho \in E$ (όπου E:επέκταση του $\mathbb{F}_q$) είναι ρίζα του f, τότε και το ρ^q είναι ρίζα του f.*

Ορίζουμε τώρα τον *αυτομορφισμό του Frobenius* (σελ. 485 στο βιβλίο):

Ορισμός 1.7.1. Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα χαρακτηριστικής p. Τότε η απεικόνιση $\sigma_p : \mathbb{F} \to \mathbb{F}$ που ορίζεται από την $\sigma_p(a) = a^p$ ονομάζεται **αυτομορφισμός του Frobenius** επί του $\mathbb{F}$.

1.8 Παράθεμα????

$z = \cos\theta + i\sin\theta$,$z^n = \cos(n\theta) + i\sin(n\theta) = e^{in\theta}$ Άρα $z = \cos\left(2\pi\frac{k}{n}\right) + i\sin(2\pi\frac{k}{n})$ και $\zeta_n = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$ άρα κάθε ν-οστή ρίζα είναι της μορφής ζ_n^k.

1.9 Μάθημα 8.

Δευτέρα 23.4.2012

Με $a_q(d)$ συμβολίζουμε το πλήθος των αναγώγων πολυωνύμων βαθμού d στο $\mathbb{F}_q$. Το $a_q(d)$ είναι ίσο με $\frac{1}{n}\sum_{d|n}\mu(d)q^{\frac{n}{d}}$.

Το $\mathbb{F}$ είναι πεπερασμένο σώμα όταν το q είναι δύναμη πρώτου: $q = p^d$.

Θεώρημα 1.9.1. *Το πολυώνυμο $f(x)$ είναι πρωταρχικό για κάποια επέκταση E του $\mathbb{F}$ βαθμού d αν και μόνο αν ισχύει ταυτόχρονα ότι: $f(x) \mid x^{q^{d-1}} - 1$ και $f(x) \nmid x^k - 1$ για $k < q^{d-1}$.*

Το $E^* = E\backslash\{0\}$ είναι κυκλική ομάδα. Το $\zeta \in E^*$ θα λέγεται πρωταρχικό στοιχείο αν και μόνο αν $\langle\zeta\rangle = \{\zeta^i, i \in \mathbb{Z}\} = E^*$ δηλαδή αν το ζ είναι γεννήτορας της ομάδας E^*. Το ελάχιστο πολυώνυμο του ζ θα έγεται πρωταρχικό πολυώνυμο. Δηλαδή πρωταρχικό πολυώνυμο είναι το ελάχιστο πολυώνυμο ενός πρωταρχικού στοιχείου.

Σημείωση. Το ζ δεν είναι μοναδικό πρωταρχικό γιατί το ζ^k είναι πρωταρχικό αν $(k, |\zeta|) = 1$, όπου με $|\zeta|$ συμβολίζουμε την τάξη του ζ.

Δίνουμε τώρα την απόδειξη του παραπάνω θεωρήματος.
Απόδειξη. Έστω $f(x)$ ανάγωγο πολυώνυμο βαθμού d. Τότε το $f(x)$ διαρεί το $x^{q^{d-1}} - 1$ (έχει αποδειχθεί). Επίσης, το σώμα ριζών του f έχει q^d στοιχεία (από γνωστό θεώρημα). Αν $f(x) \nmid x^k - 1$ για κάθε $k < q^d - 1$ τότε καμιά ρίζα του f δεν έχει την ιδιότητα $\zeta^k = 1$ δηλαδή οι ρίζες του f έχουν τη σωστή τάξη $\zeta^{q^{d-1}} - 1$.

Αντίστροφα, υποθέτουμ ε ότι το ανάγωγο $f(x)$ είναι πρωταρχικό δηλαδή ελάχιστο πολυώνυμο κάποιου πρωταρχικού στοιχείου του E. Θα δείξουμε ότι $f(x) \nmid x^k - 1$ για $k < q^d - 1$. Αν το ζ είναι ρίζα του $f(x)$ τότε όλες οι ρίζες του $f(x)$ είναι οι $\zeta, \zeta^q, \zeta^{q^2}, \ldots \zeta^{q^{d-1}}$ (από γνωστό θεώρημα). Το σώμα ριζών του $f(x)$ έχει q^d στοιχεία και είναι ίσο με το E που έχει επίσης q^d στοιχεία. Το $f(x) \nmid x^k - 1$ γιατί διαφορετικά θα ήταν $\zeta^k = 1$ το οποίο δε γίνεται γιατί το ζ είναι γεννήτορας της κυκλικής ομάδας E^*.

□

1.9.1 N-οστές ρίζες της μονάδας

Έστω $\mathbb{F}$ ένα σώμα χαρακτηριστικής p. Το x θα λέγεται n-οστή ρίζα της μονάδας αν και μόνο αν $x^n = 1$. Αν το n είναι δύναμη της χαρακτηριστικής (π.χ. $n = p^h$) τότε υπάρχει μόνο μία n-οστή ρίζα του 1, το 1. Αυτό φαίνεται καθαρότερα αν σκεφτούμε ότι, αναζητούμε τις ρίζες γ για τις οποίες $\gamma^{p^h} - 1 = 0 \iff (x-1)^{p^n}$ το οποίο έχει μοναδική ρίζα το $x = 1$.

Αν το n είναι στη μορφή $n = p^n \cdot m$ με $(m, p) = 1$ τότε θα έχω:

$$x^n - 1 = 0 \iff x^{p^n m} - 1 = 0 \iff (x^m - 1)^{p^n} = 0 \iff x^m - 1 = 0 \tag{1.29}$$

Δηλαδή έχω τόσες n-οστές ρίζες της μονάδας όσες το κομμάτι του n που είναι πρώτο προς το p. Στη συνέχεια ψάχνουμε τις n-οστές ρίζες του 1.

Έστω $(n, p) = 1$. Με E_n συμβολίζουμε το σύνολο των n-οστών ριζών της μονάδας. Το πλήθος των στοιχείων του E_n είναι n (σε κατάλληλη επέκταση του $\mathbb{F}$). Αυτό εξηγείται αν

αναλογιστούμε ότι το πολυώνυμο $f(x) = x^n - 1$ έχει απλές ρίζες αφού $f'(x) = nx^{n-1}$ (το οποίο έχει μοναδική ρίζα το 0). Το $x^n - 1$ και το nx^{n-1} δεν έχουν κοινές ρίζες.

Εξετάζουμε τώρα τις ιδιότητες του E_n.

1. Η E_n είναι κυκλική τάξης n μιας και $E_n < E^*$ όπου E είναι το σώμα ριζών του $x^n - 1$. Το E^n είναι κυκλική άρα και το E_n (αφού είναι υποομάδα κυκλικής ομάδας).

2. Αν $[E : \mathbb{F}] = s$ (E το σώμα ριζών του $x^n - 1$) τότε το s είναι ο μικρότερος θετικός ώστε $q^s \equiv 1 \bmod n$.
   Απόδειξη. Αφού το πλήθος των στοιχείων του E είναι q^s θα έχω ότι το πλήθος των στοιχείων του E^* είναι $q^s - 1$, άρα $n \mid q^s - 1$ (από το θεώρημα του Lagrange) οπότε $q^s \equiv 1 \bmod n$. Αντιστρόφως, έστω ότι $n \mid q^r - 1$ τότε $x^n - 1 \mid x^{q^r - 1} - 1$. Το σώμα ριζών E του $x^n - 1$ περιέχεται σε κάθε σώμα με q^r στοιχεία αρκεί να ισχύει ότι $n \mid q^r - 1$. Το ελάχιστο σώμα E θα έρθει στον ελάχιστο s για τον οποίο ισχύει $n \mid q^s - 1$. □

   Έστω ω ένας γεννήτορας της E_n. Κάθε στοιχείο της E_n είναι δύναμη του ω. Η τάξη του $|\omega^k| = \dfrac{n}{(n,k)}$. Αν $(k, n) = 1$ τότε $|\omega^k| = n$ άρα το ω^k είναι και αυτός γεννήτορας. Τους γεννήτορες του E_n θα τους λέμε πρωταρχικές ρίζες της μονάδας και είναι $\phi(n)$ στο πλήθος.

Παράδειγμα 1.9.1. Θα υπολογίσουμε τις τέταρτες ρίζες του 1. Έχουμε ότι $x^4 - 1 = 0 \iff (x^2 - 1)(x^2 + 1) = 0$. Στο σώμα των μιγαδικών $\mathbb{C}$ έχω ότι $i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$ άρα το i είναι ένας γεννήτορας της κυκλικής ομάδας με τέσσερα στοιχεία, άρα και πρωταρχική ρίζα. Η τάξη του i^2 είναι

$$|i^2| = \frac{4}{(4,2)} = 2 \tag{1.30}$$

, του i^3 είναι

$$|i^3| = \frac{4}{(3,4)} = 4 \tag{1.31}$$

και του i^4 είναι

$$|i^4| = \frac{4}{(4,4) = 1} \tag{1.32}$$

Συγκρίνουμε τώρα τις κυκλικές υποομάδες E_n και E. Το E_n είναι η ομάδα που παράγεται από το ω, όπου ω: η πρωταρχική n-ρίζα του 1. Το E είναι η ομάδα που παράγεται απο το ζ: το οποίο είναι μια πρωταρχική ρίζα. Η τάξη του $|\omega|$ είναι n, ενώ του $|\zeta| = q^s - 1$. Επίσης, $\omega = \zeta^k$ για κάποιο k αφού $\omega \in \langle\zeta\rangle = E^*$. Η τάξη του ζ^k είναι:

$$|\zeta^k| = \frac{q^s - 1}{(k, q^s - 1)} \tag{1.33}$$

από το θεώρημα του Lagrange. Επειδή ξέρω ότι $n \mid q^s - 1$ θα έχω $q^s - 1 = nr$ θα έχω

$$|\zeta^k| = \frac{nr}{(k, nr)} = n \tag{1.34}$$

για να ισχύει αυτό θα πρέπει να είναι $(k, nr) = r$ δηλαδή το k να είναι $k = rm$ και $(m, n) = 1$.

Θεώρημα 1.9.2. *Αν ζ είναι ένα πρωταρχικό στοιχείο του σώματος ριζών E του $x^n - 1$ στο $\mathbb{F}[x]$, τότε το σύνολο των πρωταρχικών ριζών του είναι το:*

$$\Omega = \{\zeta^k, k = \frac{q^s - 1}{n} \cdot m, m < n, (m, n) = 1\}$$

Οδηγούμαστε στο ακόλουθο πόρισμα:

Πόρισμα. Αν Φ το σύνολο των πρωταρχικών στοιχείων του E τότε ισχύει ότι $\Omega \cap \Phi = \emptyset$ εκτός αν $n = q^s - 1$ οπότε θα ισχύει ότι $\Omega = \Phi$.

Δίνουμε τώρα την απόδειξη του παραπάνω θεωρήματος.
Απόδειξη. Έχουμε το $x^n - 1 \subset \mathbb{F}[x]$. Στο σώμα E το $x^n - 1$ έχει απλές ρίζες. Στο $\mathbb{F}$ δεν έχει όλες τις ρίζες του (εκτός αν $n \mid q - 1$). Το $x^n - 1$ είναι γινόμενο των ελαχίστων πολυωνύμων των ριζών του 1. Έστω $\omega = \zeta^{\frac{q^s-1}{n}}$ πρωταρχική n-οστή ρίζα του 1. Όλες οι ρίζες του $x^n - 1$ είναι οι: $1, \omega, \omega^2, \dots \omega^{n-1}$. Αν $m_\omega(x)$ είναι το ελάχιστο πολυώνυμο τις ρίζας ω τότε $m_\omega(x) = (x - \omega)(x - \omega^q) \dots (x - \omega^{q^{d-1}})$ άρα ο d είναι ο μικρότερος ακέραιος για τον οποίο ισχύει ότι $\omega^{q^d} - \omega = 0$, δηλαδή $q^d \equiv 1 \bmod n$. Ομοίως για κάθε ω υπάρχει το ελάχιστο πολυώνυμο $m_{\omega_i}(x) = (x - \omega^i)(x - \omega^{iq}) \dots (x - \omega^{iq^{d_i - 1}})$ ώστε $\omega^{iq^{d_i}} \equiv \omega \iff iq^{d_i} \equiv i \bmod n$. Δηλαδή, $x^n - 1 = \prod_{i \in I} m_{\omega^i}(x)$. □

Θυμηθείτε ότι αν ω είναι μία ρίζα του $x^n - 1$ τότε όλες οι ρίζες του είναι δυνάμεις του ω. Ανάμεσα σε αυτές υπάρχουν και μή πρωταρχικές ρίζες οι οποίες έχουν τάξη m, όπου $m \mid n$ και ικανοποιούν πολυώνυμα της μορφής $x^m - 1$.

Ορισμός 1.9.1. Έστω $\mathbb{F}$ ένα σώμα με q στοιχεία όπου $(n, q) = 1$. Κυκλοτομικό πολυώνυμο[5] τάξης h επί του $\mathbb{F}$ ονομάζεται το μονικό πολυώνυμο $Q_n(x)$ το οποίο έχει σαν ρίζες τις πρωταρχικές k-ρίζες του 1. Δηλαδή το Q είναι της μορφής:

$$Q_k(x) = (x - \zeta_1) \dots (x - \zeta_{\phi(k)}) \subset E[x]$$

Θα δείξουμε ότι το k-οστό κυκλοτομικό πολυώνυμο ανήκει στο $\mathbb{F}[x]$. Πράγματι, αν για κάποιο ζ ισχύει $Q_k(\zeta) = 0$ τότε το ζ θα είναι ρίζα ενός αναγώγου $m_i(x)$ και οι ρίζες του $m_i(x)$ θα είναι τα $\zeta, \zeta^q, \zeta^2, \dots$ για τα οποία ισχύει ότι $(q, k) = 1$. Αυτές είναι επίσης πρωταρχικές k-ρίζες του 1, μιας και $\frac{k}{q^t, k} = 1$, άρα $m_i \mid Q_k$, δηλαδή τα Q_k είναι γινόμενα των $m_i \in \mathbb{F}[x]$, άρα και τα $Q_k \in \mathbb{F}[x]$.

Παρατήρηση. Ο υπολογισμός των Q_k γίνεται με αναδρομικό τρόπο: στο $x^2 - 1$ για παράδειγμα, έχουμε ότι θα είναι της μορφής:

$$x^2 - 1 = Q_1(x)Q_2(x) \tag{1.35}$$

οπότε το $Q_1(x) = x - 1$ και $Q_2(x) = x + 1$ μιας και $Q_1 \neq Q_2$ αν $p \neq 2$. Για το $x^3 - 1$ θα έχουμε:

$$x^3 - 1 = Q_1(x)Q_3(x) \tag{1.36}$$

άρα θα είναι $Q_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1$.

[5] Fraleigh, σελ. 546

1.10 Μάθημα 9.

Δεύτερα 30.4.2012

1.10.1 Τετραγωνικός νόμος αντιστροφής

Σημείωση: Μέρος τον ορισμών για αυτό το μάθημα έχει παρθεί από το βιβλίο "Elementary Number Theory: Primes, Congruences, and Secrets" του W. Stein, στο οποίο θα γίνονται οι αναφορές.

(Elementary Number Theory: Primes, Congruences, and Secrets, W. Stein, σελ. 70)

Δίνουμε πρώτα τον ορισμό του τετραγωνικού υπολοίπου.

Ορισμός 1.10.1 (τετραγωνικό υπόλοιπο)**.** Έστω p ένας πρώτος αριθμός. Ένας ακέραιος a που δεν είναι πολλαπλασίο του p, είναι *τετραγωνικό υπόλοιπο* του p αν ο a είναι τετράγωνο κάποιου αριθμού mod$p$. Αν ο a δεν είναι τετράγωνο κάποιου αριθμού mod$p$ τότε λέγεται *τετραγωνικό μή-υπόλοιπο* mod$p$.

Για να γίνει περισσότερο κατανοητή η έννοια του τετραγωνικού υπολοίπου, σκεφτείτε ότι συνδέεται με τις λύσεις της ισοδυναμίας

$$x^2 \equiv a \bmod p \tag{1.37}$$

Ερώτηση. Πότε η παραπάνω ισοδυναμία έχει λύση;

Απάντηση. Ουσιαστικά μιλάμε για δύο διαφορετικά προβλήματα. Τα εξής:

- Έστω ένας πρώτος p. Ποιοί ακέραιοι a της κλάσης modulo 5 είναι τετράγωνα κάποιον x. Για παράδειγμά, για $a = 3$ στην κλάση modulo 5 δεν υπάρχει x ώστε $x^2 \equiv 3 \bmod 5$. Πράγματι, η κλάση των (μη μηδενικών) υπολοίπων του 5 είναι οι αριθμοί $1, 2, 3, 4$. Τα τετράγωνα τους είναι:

  $$1^2 = 1, \qquad 2^2 = 4, \qquad 3^2 = 9 \equiv 4 \mod 5, \qquad 4^2 = 16 \equiv 1 \mod 5 \tag{1.38}$$

  Άρα δεν υπάρχει ακέραιος της κλάσης modulo 5 που να αφήνει τετραγωνικό υπόλοιπο 3. Τα τετραγωνικά υπόλοιπα είναι τα $a = 1$ και $a = 4$.

- Το δεύτερο πρόβλημα εξετάζει το αντίστροφο, δηλαδή: δοθέντος ενός ακέραιου a, ποιοί πρώτοι p "έχουν" τον a ως τετραγωνικό υπόλοιπο;

Εμείς θα ασχοληθούμε με το πρώτο πρόβλημα.

Ορίζουμε τώρα το σύμβολο του Legendre ως εξής:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{αν } p \mid a, \\ +1 & \text{αν το } a \text{ είναι τετραγωνικό υπόλοιπο, και} \\ -1 & \text{αν το } a \text{ δεν είναι τετραγωνικό υπόλοιπο} \end{cases} \tag{1.39}$$

Παρατήρηση. Αν το a είναι ή όχι τετραγωνικό υπόλοιπο εξαρτάται από την κλάση του $a \bmod p$.

Παράδειγμα 1.10.1. Υπολογίζουμε τις λύσεις τις $x^2 \equiv a \bmod 5$.

- Αν $a = 0$ τότε $\left(\frac{0}{5}\right) = 0$ γιατί $5 \mid 0$.
- Αν $a = 1$ τότε $\left(\frac{1}{5}\right) = 1$ γιατί η ισοδυναμία $x^2 \equiv 1 \bmod 5$ έχει λύση (π.χ. την $x = 4$).
- Αν $a = 2$ τότε $\left(\frac{2}{5}\right) = -1$ γιατί η $x^2 = 2$ δεν έχει λύσεις.
- Αν $a = 3$ τότε $\left(\frac{3}{5}\right) = -1$ γιατί η $x^2 = 3$ δεν έχει λύσεις.
- Αν $a = 4$ τότε $\left(\frac{4}{5}\right) = 1$ γιατί η ισοδυναμία $x^2 \equiv 4 \bmod 5$ έχει λύση (π.χ. την $x = 3$). Άρα για $a = 1, 4$ ή αλλιώς, $a = \pm 1$, η ισοδυναμία έχει λύσεις.

Παρατηρήστε ότι το σύμβολο του Legendre εξαρτάται μόνο από το $a \bmod p$. Οπότε είναι σωστό να ορίσουμε το $\left(\frac{a}{p}\right)$ για $a \in \mathbb{Z}/p\mathbb{Z}$.

Ορίζουμε την απεικόνιση:

$$\psi : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\} \text{ με } \psi(a) \mapsto \left(\frac{a}{p}\right) \tag{1.40}$$

Πρόταση 1.10.1. *Η παραπάνω απεικόνιση είναι ομομορφισμός ομάδων, το οποίο ισοδυναμεί με το ότι ισχύει:*

$$\left(\frac{a\beta}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{\beta}{p}\right) \tag{1.41}$$

Απόδειξη. Έχω ότι η $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{F}^*$ είναι μία κυκλική ομάδα άρα υπάρχει g ώστε η $(\mathbb{Z}/p\mathbb{Z})$ να είναι της μορφής:

$$\{g, g^2 \dots g^{(p-1)/2}, g^{(p+1)/2}, \dots g^{p-1} = 1\} \tag{1.42}$$

Αφού ο $p - 1$ είναι άρτιος, τα τετράγωνα των στοιχείων του $(\mathbb{Z}/p\mathbb{Z})^*$ είναι τα

$$g^2, g^4, \dots g^{(p-1)/2 \cdot 2} = 1, g^{p+1} = g^2, \dots g^{2(2(p-1))} \tag{1.43}$$

Το οποίο σημαίνει ότι τα τέλεια τετράγωνα του $(\mathbb{Z}/p\mathbb{Z})^*$ είναι τα g^i με i : άρτιος και τα μη τέλεια τετράγωνα είναι τα g^i με i: περιττός. Αυτό σημαίνει ότι η ψ είναι ομομορφισμός καθώς: το άθροισμα δύο περιττών είναι άρτιος, το άθροισμα δύο άρτιων είναι άρτιος και το άθροισμα ενός περιττού με έναν άρτιο είναι περιττό. □

Παρατήρηση. Παρατηρήστε ότι ο πυρήνας της ψ είναι τα $g \in (\mathbb{Z}/p\mathbb{Z})^*$ για τα οποία ισχύει ότι $\psi(a) = 1$, δηλάδη τα τετραγωνικά υπόλοιπα του p.

Παραθέτουμε τώρα τον τετραγωνικό νόμο αντιστροφής, τον οποίο απέδειξε ο Gauss σε ηλικία 19 ετών.

Θεώρημα 1.10.2 (τετραγωνικός νόμος αντιστροφής)**.** *Έστω p, q δύο περιττοί, πρώτοι αριθμοί. Τότε*

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

Επίσης,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \text{ και } \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Έστω τώρα p ένας περιττός πρώτος και a ακέραιος που δε διαιρείται από τον p. Ο Euler χρησιμοποίησε την ύπαρξη των πρωταρχικών ριζών για να δείξει ότι το $\left(\frac{a}{p}\right)$ είναι ισότιμο με το $a^{(p-1)/2}$ modulo p. Αυτή η ισοτιμία θα χρησιμεύσει στην απόδειξη του τετραγωνικού νόμου αντιστροφής.

Πρόταση 1.10.3 (κριτήριο Euler)**.** *Ισχύει ότι*

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \tag{1.44}$$

δηλαδή

$$\left(\frac{a}{p}\right) = 1 \iff a^{\frac{p-1}{2}} \equiv 1 \bmod p \tag{1.45}$$

Απόδειξη. Ισχύει ότι $\left(\frac{a}{p}\right)$ και $a^{p-1} \equiv \mod p$ οπότε $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$. Η απεικόνιση $\phi : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ με $\phi(a) = a^{\frac{p-1}{2}}$ είναι ένας ομομορφισμός ομάδων. Η απεικόνιση ψ είναι η απεικόνιση που ορίσαμε στην 1.40. Αν $a \in \ker\psi$ τότε $a = b^2$ για κάποιο $b \in (\mathbb{Z}/p\mathbb{Z})^*$ οπότε

$$\phi(a) = a^{(p-1)/2} = (b^2)^{(p-1)/2} = b^{p-1} = 1. \tag{1.46}$$

□

Κατά συνέπεια είναι $\ker\psi \subseteq \ker\phi$. Θα δείξω ότι $\ker\psi = \ker\phi$. Ο $\ker\psi$ έχει διάσταση 2 (από την 1.40) στο $\mathbb{Z}/p\mathbb{Z}$. Εφόσον ο πυρήνας ενός ομομορφισμού είναι ομάδα από μόνος του και η τάξη μιας υποομάδας διαιρεί την τάξη της ομάδας, θα ισχύει είτε ότι $\ker\phi = \ker\psi$ ή $\phi = 1$. Αν $\phi = 1$ το πολυώνυμο $x^{(p-1)/2} - 1$ έχει $p-1$ ρίζες στο σώμα $\mathbb{Z}/p\mathbb{Z}$ το οποίο είναι άτοπο. Κατά συνέπεια ισχύει ότι $\ker\phi = \ker\psi$.

Ορίζουμε τα αθροίσματα Gauss τώρα για να αποδείξουμε τον τετραγωνικό νόμο αντιστροφής. Καταρχάς, έχουμε δώσει τον ορισμό μιας $\nu-$οστής ρίζας της μονάδας αλλά τον επαναλαμβάνουμε, όπως υπάρχει και στο *Elementary Number Theory: Primes, Congruences, and Secrets, W. Stein, σελ. 81.*

Ορισμός 1.10.2 (άθροισμα Gauss)**.** Μία $\nu-$οστή ρίζα της μονάδας είναι ένας μιγαδικός αριθμός ζ για τον οποίο ισχύει ότι $\zeta^\nu = 1$. Μία ρίζα της μονάδας ζ είναι μία πρωταρχική $\nu-$οστή ρίζα της μονάδας αν το ν είναι ο μικρότερος θετικός ακέραιος για τον οποίο ισχύει ότι $\zeta^\nu = 1$.

Αν τώρα το ζ είναι μία πρωταρχική ρίζα της μονάδας ορίζουμε τα αθροίσματα του Gauss:

Ορισμός 1.10.3. Έστω ένα περιττός πρώτος p. Το άθροισμα Gauss ενός ακεραίου a είναι το

$$g_a = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta^{an}$$

όπου ζ: μία πρωταρχική ρίζα της μονάδας.

Πρόταση 1.10.4. *Για κάθε a που **δεν** διαιρείται από τον p, τότε*

$$g_a^2 = (-1)^{(p-1)/2} p.$$

Και για να αποδείξουμε την πρόταση, δίνουμε μερικά λήμματα.

Λήμμα 1.10.5. *Για κάθε ακέραιο a ισχύει ότι*

$$\sum_{n=0}^{p-1} \zeta^{an} = \begin{cases} p & \text{αν } a \equiv 0 \pmod p, \\ 0 & \text{αλλιώς} \end{cases}$$

Απόδειξη. Αν $p \mid a$ τότε ισχύει ότι ζ^a τότε $\zeta^a \equiv 1$, οπότε το άθροισμα είναι το πλήθος τον αθροισμάτων, το οποίο είναι p. Αν $p \nmid a$ τότε χρησιμοποιώντας την ταυτότητα

$$x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1) \tag{1.47}$$

με $x = \zeta^a$. Έχουμε ότι $\zeta^a \neq 1$, οπότε $\zeta^a - 1 \neq 0$ και

$$\sum_{n=0}^{p-1} \zeta^{an} = \frac{\zeta^{ap} - 1}{\zeta^a - 1} = \frac{1-1}{\zeta^a - 1} = 0 \tag{1.48}$$

□

Λήμμα 1.10.6. *Αν x, y ακέραιοι, τότε*

$$\sum_{n=0}^{p-1} \zeta^{(x-y)n} = \begin{cases} p & \text{αν } x \equiv y \pmod p, \\ 0 & \text{αλλιώς.} \end{cases}$$

Απόδειξη. Από το προηγούμενο λήμμα 1.10.6, θέτοντας $a = x - y$. □

Λήμμα 1.10.7. *Ισχύει ότι* $g_0 = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) = 0.$

Η απόδειξη υπάρχει στο *Elementary Number Theory: Primes, Congruences, and Secrets, W. Stein, σελ. 84.*

Λήμμα 1.10.8. *Για κάθε ακέραιο a ισχύει ότι*

$$g_a = \left(\frac{a}{p}\right) g_1$$

Απόδειξη. Όταν $a \equiv 0 \pmod{p}$, είμαστε στην περίπτωση του λήμματος 1.10.7, οπότε υποθέτουμε ότι $a \not\equiv 0 \pmod{p}$. Τότε $\left(\frac{a}{p}\right) g_a = \left(\frac{a}{p}\right) \sum_{n=0}^{p-1} \left(\frac{a}{p}\right) \zeta^{an} = \sum_{n=0}^{p-1} \left(\frac{an}{p}\right) \zeta^{an} = \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) \zeta^{m} = g_1$. Χρησιμοποιήσαμε το ότι ο πολλαπλασιασμός με a είναι ένας αυτομορφισμός του $\mathbb{Z}/p\mathbb{Z}$. Τελικά, πολλαπλασιάζουμε και τα δύο μέλη με $\left(\frac{a}{p}\right)$ και χρησιμοποιούμε το ότι $\left(\frac{a}{p}\right)^2 = 1$. □

Δίνουμε τώρα την απόδειξη της πρότασης 1.10.4.
Απόδειξη. Έχουμε ότι

$$g_a g_{-a} = \left(\frac{a}{p}\right) g_1 \left(\frac{-a}{p}\right) g_1 = \left(\frac{-1}{p}\right) \left(\frac{a}{p}\right) g^2 \tag{1.49}$$

όπου

$$\left(\frac{a}{p}\right) = 1 \tag{1.50}$$

οπότε και από το κριτήριο του Euler έχουμε ότι

$$-1^{\frac{p-1}{2}} g_1^2 \tag{1.51}$$

□

Και τελειώνουμε με την απόδειξη του τετραγωνικού νόμου αντιστροφής.

Απόδειξη. 'Εστω q ένας περιττός πρώτος με $q \neq p$. Θέτουμε $p^* = (-1)^{(p-1)/2} p$ οπότε θα ισχύει ότι $p^* = g_1^2$ όπου $g_1 = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^n$. Ισχύει από θεωρία ότι

$$(p^*)^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) \pmod{q}. \tag{1.52}$$

Έχουμε ότι $g^{q-1} = (g^2)^{(q-1)/2} = (p^*)^{(q-1)/2}$ οπότε αν πολλαπλασιάσουμε και τα δύο μέλη της εξίσωσης με g θα προκύψει η ισοτιμία

$$g^q \equiv g \left(\frac{p^*}{q}\right) \pmod{q} \tag{1.53}$$

το οποίο σημαίνει ότι

$$g^q - g \left(\frac{p^*}{q}\right) \equiv 0 \pmod{q} \tag{1.54}$$

Ο δακτύλιος $\mathbb{Z}/p\mathbb{Z}$ έχει χαρακτηριστική q, οπότε αν $x, y \in \mathbb{Z}[\zeta]$ τότε $(x+y)^q \equiv x^q + y^q \pmod{q}$. Αν το εφαρμόσουμε αυτό στην προηγούμενη ισοδυναμία θα έχουμε ότι

$$g^q = \left(\sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^n\right)^q \equiv \sum_{n=0}^{p-1} \left(\frac{n}{p}\right)^q \zeta^{nq} \equiv \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^{nq} \equiv g_4 \pmod{q}. \tag{1.55}$$

Επιπλέον, από προηγούμενο λήμμα έχω ότι

$$\left(\frac{q}{p}\right) g \equiv \left(\frac{p^*}{q}\right) g \pmod{q} \tag{1.56}$$

Εφόσον ισχύει ότι $g^2 = p^*$ και $p \neq q$ μπορούμε να διαγράψουμε το g και από τα δύο μέλη για να καταλήξουμε στο ότι $\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \pmod{q}$ και τέλος έχουμε ότι

$$\left(\frac{p^*}{q}\right) = \left(\frac{(-1)^{(p-1)/2} p}{q}\right) = \left(\frac{-1}{q}\right)^{(p-1)/2} \left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2} \cdot \frac{p-1}{2}} \cdot \left(\frac{p}{q}\right). \tag{1.57}$$

□

1.11 Μάθημα 10.

Τετάρτη 2.5.2012

Άσκηση: Να αποδειχθεί ότι το 3 είναι τετράγωνο mod$p$ για $p > 3$ αν $p \equiv 1, 11 \pmod{12}$.

Υπόδειξη: Καταρχάς ας θυμηθούμε ότι το σύμβολο Legendre $\left(\frac{k}{p}\right)$ εξετάζει αν η ισοτιμία $x^2 \equiv k \bmod p$ έχει ή όχι λύση και εξαρτάται από την κλάση $k \bmod p$.

Ο τετραγωνικός νόμος αντιστροφής μας επιτρέπει να δούμε την περιοδικότοτητα στα p. Στην άσκηση ουσιαστικά έχουμε ότι $k = 3$ και μας ζητάει να υπολογίσουμε το $\left(\frac{3}{p}\right)$ για κάθε p.

$$\left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{p-1}{2}} \cdot \left(\frac{p}{3}\right) \tag{1.58}$$

δηλαδή

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right) \tag{1.59}$$

Με αυτόν τον τρόπο, τα p που έχω να μελετήσω γίνονται πεπερασμένα γιατί αρκεί να δω την κλάση του $p \bmod 3$. Τώρα κοιτάω πότε την ισοδυναμία $x^2 \equiv p \bmod 3$. Οι αριθμοί $\{0, 1, 2\}$ της κλάσης modulo3 γίνονται $0, 1$ και $4 \equiv 1 \bmod 3$. Άρα οι λύσεις είναι τα $\{0, 1\}$. Θυμηθείτε τώρα ότι αν $p > 3$ τότε θα ο p θα είναι ισότιμος είτε με 1, είτε με -1 modulo 3 οπότε θα είναι

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{αν } p \equiv 1 \bmod 3, \\ -1 & \text{αν } p \equiv -1 \bmod 3 \end{cases} \tag{1.60}$$

Τώρα για το $(-1)^{\frac{p-1}{2}}$, αφού ο p είναι περιττός θα έχω ότι $p-1 \equiv 0 \bmod 4 \iff \dfrac{p-1}{2} \in 2\mathbb{Z}$ και $p-1 \equiv 2 \bmod 4 \iff \dfrac{p-1}{2} \notin 2\mathbb{Z}$. Οπότε θα είναι

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{αν } p \equiv 1 \bmod 4, \\ -1 & \text{αν } p \equiv 3 \bmod 4 \end{cases} \tag{1.61}$$

Τα επιτρεπτά $p \bmod 12$ είναι τα $1, 5, 7, 11$ οπότε υπολογίζοντας για κάθε p τα $(-1)^{\frac{p-1}{2}}$, $\left(\dfrac{p}{3}\right)$ και πολλαπλασιάζοντας τα βρίσκουμε ότι $p \equiv 1, 11 \bmod 12$ το οποίο ολοκληρώνει την απόδειξη.

1.11.1 Primality testing

Ας υποθέσουμε ότι έχουμε έναν αριθμό n με πολλές χιλιάδες ψηφία και θέλουμε να ελέγξουμε αν είναι πρώτος. Ένας διαιρέτης του n θα είναι μικρότερος ή ίσος από το $\sqrt{n}$ άρα θα πρέπει να δοκιμάσω όλους τους πρώτους που είναι μικρότεροι από το $\lfloor n \rfloor$. Το πρόβλημα εντοπισμού τον παραγόντων του n γίνεται δυσκολότερο αν ισχύει ότι $n = p \cdot q$ με $p \sim q \sim \sqrt{n}$. Ένας σύνθετος αριθμός, για να είναι δύσκολο να παραγοντοποιηθεί δεν θα πρέπει να έχει μικρούς διαιρέτες. Θέλουμε δηλαδή ο μικρότερος πρώτος διαιρέτης να είναι όσο γίνεται μεγαλύτερος.

Δίνουμε τώρα ένα θεώρημα για πρώτους.

Θεώρημα 1.11.1. *Ένας ακέραιος $p > 1$ είναι πρώτος αν και μόνο αν για κάθε $a \not\equiv 0 \pmod p$ ισχύει ότι*

$$a^{p-1} \equiv 1 \pmod p$$

Το παραπάνω θεώρημα δίνει ένα εύκολο κριτήριο για να βρίσκουμε αριθμούς που δεν είναι πρώτοι: Αν p είναι ένας υποψήφιος και βρώ ένα a ώστε $a^{p-1} \not\equiv 1 \pmod p$ τότε ο p δεν είναι πρώτος. Το πρόβλημα πλέον είναι το εξής:
Πρόβλημα: Πώς θα υπολογίσουμε το a^{p-1} και γενικότερα το $a^m \pmod p$.

Ένας αποτελεσματικός τρόπος υπολογισμού του $a^m \mod p$ είναι το να γράψουμε το m σε δυαδική μορφή. Σε αυτή τη μορφή υπάρχει ένας δείκτης i και m ένας ακέραιος. Δίνουμε τον παρακάτω αλγόριθμο ο οποίος υπάρχει στο *Elementary Number Theory: Primes, Congruences, and Secrets, W. Stein, σελ. 35*
.

Αλγόριθμος(υπολογισμός δύναμης). Έστω a και n δύο ακέραιοι και m ένας μη αρνητικός ακέραιος. Ο παρακάτω αλγόριθμος υπολογίζει το a^m modulo n.

1. (Δυαδική μορφή) Γράφουμε το m σε δυαδική μορφή, οπότε θα είναι $a^m = \prod_{\varepsilon=1} a^{2^1} \pmod n$.
2. (Υπολογισμός δυνάμεων) Υπολογίζουμε τα $a, a^2, a^{2^2} = (a^2)^2, a^{2^3} = (a^{2^2})^2$ κλπ, μέχρι το a^{2^r}, όπου $r+1$ είναι ο αριθμός τον δυαδικών ψηφιών του m.
3. (Πολλαπλασιασμός δυνάμεων) Πολλαπλασιάζουμε τα a^i για τα οποία ισχύει ότι $\varepsilon_i = 1$, δουλεύοντας modulo n.

Παράδειγμα 1.11.1.

i	m	ε_i	$2^{2^i} \bmod 323$
0	322	0	2
1	161	1	4
2	80	0	16
3	40	0	256
4	20	0	290
5	10	0	120
6	5	1	188
7	2	0	137
8	1	1	35

Επιλέγουμε αυτά για τα οποία $\varepsilon_i = 1$ και πολλαπλασιάζουμε 2^{2^i} μεταξύ τους. Οπότε έχουμε

$$4 \cdot 188 \cdot 35 \equiv 157 \bmod 323 \tag{1.62}$$

άρα ο 323 δεν είναι πρώτος.