

Ασκήσεις Πεπερασμένων Σωμάτων και κρυπτογραφίας
1 Φυλλάδιο

Ασκηση 1. Να υπολογιστεί ένας γεννήτορας των κυκλικών ομάδων $\mathbb{F}_{13}$, $\mathbb{F}_{2^3}$.

Λύση: Το 13 είναι πρώτος. Δοκιμάζουμε αν το $2 \bmod 13$ είναι γεννήτορας υπολογίζοντας τις δυνάμεις του 2: $2, 4, 8, 16 = 3, 32 = 6, 64 = 12, 128 = 11, 256 = 9, 512 = 5, 1024 = 10, 2048 = 7, 4096 = 1$.

Παρατηρούμε ότι η τάξη του 2 (δηλαδή η ελάχιστη δύναμη στην οποία πρέπει να υψωθεί το 2 για να μας δώσει την μονάδα modulo 13 είναι $12 = \phi(13)$ όσα ακριβώς και τα αντιστρέψιμα στοιχεία του $\mathbb{F}_{13}$.

Στις παραπάνω πράξεις δεν χρειάζεται να υπολογίσουμε το 2^i στο $\mathbb{Z}$, είναι ευκολότερο να δουλέψουμε αναδρομικά modulo 13.

Επίσης θα μπορούσαμε να κάνουμε λιγότερες πράξεις παρατηρώντας ότι οι δυνατές τάξεις για το ένα στοιχείο του $\mathbb{F}_{13}$ είναι διαιρέτες του 12. Έτσι θα μπορούσαμε να σταματήσουμε τους υπολογισμούς με το που βρήκαμε ότι $2^6 = 12 = -1$.

Για το σώμα $\mathbb{F}_{2^3}$ παρατηρούμε ότι το 2^3 δεν είναι πρώτος. Το σώμα με 2^3 στοιχεία δεν είναι ο δακτύλιος $\mathbb{Z}/2^3\mathbb{Z}$! Ο τελευταίος για παράδειγμα δεν είναι ακέραια περιοχή. Επιπλέον το $\mathbb{F}_3^*$ έχει $8 - 1 = 7$ αντιστρέψιμα στοιχεία ενώ το $\mathbb{Z}/8\mathbb{Z}$ έχει $\phi(8) = 4$ στοιχεία.

Το σώμα $\mathbb{F}_{2^3}$ είναι μία αλγεβρική επέκταση του $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Δηλαδή είναι της μορφής

$$\mathbb{F}_2[x]/f(x),$$

όπου το $f(x)$ είναι ένα ανάγωγο πολυώνυμο στο $\mathbb{F}_2[x]$ βαθμού 3. Παρατηρούμε ότι το $x^3 + x + 1$ είναι ένα τέτοιο. Είναι ανάγωγο γιατί δεν έχει ρίζα στο $\mathbb{F}_2$ (δοκιμάστε ότι οι δύο πιθανές ρίζες 0, 1 δεν είναι ρίζες) και είναι βαθμού 3 άρα αν δεν είναι ανάγωγο θα είχε ένα γραμμικό παράγοντα.

Τώρα θα πρέπει να διαλέξουμε στοιχεία και να υπολογίσουμε τις διαδοχικές δυνάμεις στοιχείων του $\mathbb{F}_8$ modulo $x^3 + x + 1$ μέχρι να βρούμε ένα στοιχείο με τάξη 7. Έτσι το x έχει δυνάμεις

$$x, x^2, x^3 = x + 1, x^4 = x^2 + x, x^5 = x^3 + x^2 = x^2 + x + 1,$$

$$x^6 = x^3 + x^2 + x = x^2 + 1, x^7 = x^3 + x = 1.$$

Στην πραγματικότητα δεν χρειάζονταν να κάνουμε τον παραπάνω υπολογισμό αφού κάθε στοιχείο που δεν είναι μονάδα είναι γεννήτορας της κυκλικής ομάδας του σώματος αφού οι δυνατές τάξεις ενός στοιχείου διαιρούν το 7.

Έτσι για κάθε πρώτο του Mersenne¹ δηλαδή για κάθε πρώτο της μορφής $2^a - 1$ μπορούμε να δείξουμε ότι κάθε στοιχείο του $\mathbb{F}_{2^a}$ που δεν είναι 0, 1 είναι γεννήτορας της κυκλικής ομάδας $\mathbb{F}_{2^a}^*$.

Άσκηση 2. Να λυθεί η διαφορική εξίσωση (!) $\frac{d}{dx}f = 0$ όπου οι επιτρεπτές λύσεις $f \in k[x]$.

Λύση: Για ένα πολυώνυμο

$$f(x) = \sum_{\nu=0}^n a_{\nu} x^{\nu}$$

παρατηρούμε ότι η παράγωγος του είναι ίση με

$$f'(x) = \sum_{\nu=1}^n \nu a_{\nu} x^{\nu-1}.$$

Άρα θα πρέπει $\nu a_{\nu} = 0$. Σε σώματα χαρακτηριστικής 0 έχουμε ότι το f θα πρέπει να είναι το μηδενικό πολυώνυμο. Σε σώματα χαρακτηριστικής 0 έχουμε την γενικότερη συνθήκη $a_{\nu} = 0$ όταν $p \nmid \nu$.

Άσκηση 3. Θα λέμε ότι ένα πολυώνυμο είναι προσθετικό αν και μόνο αν είναι της μορφής

$$f(x) = \sum_{\nu=0}^n a_{\nu} x^{p^{\nu}}.$$

Αποδείξτε ότι αν ένα πολυώνυμο είναι προσθετικό τότε οι ρίζες του αποτελούν ένα $\mathbb{F}_p$ διανυσματικό χώρο. Αντιστρόφως αποδείξτε ότι αν ένα πολυώνυμο έχει απλές ρίζες που αποτελούν διανυσματικό χώρο τότε είναι προσθετικό.

Λύση: Η μία φορά της άσκησης είναι σχετικά εύκολη: Αρκεί να παρατηρήσουμε ότι αν x, y ρίζες του $f(x)$ τότε αφού ισχύει ότι²

$$(x + y)^{p^{\nu}} = x^{p^{\nu}} + y^{p^{\nu}}$$

έχουμε ότι $f(x + y) = f(x) + f(y) = 0$. Επιπλέον αν $\lambda, \mu \in \mathbb{F}_p$ τότε $\lambda^{p^{\nu}} = \lambda$ για κάθε $\nu \in \{1, 2, 3, 4, \dots\}$ οπότε έχουμε ότι

$$f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$$

και από το οποίο προκύπτει ότι αν $f(x) = f(y) = 0$ τότε και $f(\lambda x + \mu y) = 0$.

¹ http://en.wikipedia.org/wiki/Mersenne_primes

² http://en.wikipedia.org/wiki/Freshmans_dream

Η αντίστροφη φορά της άσκησης είναι αρκετά δύσκολη. Ας υποθέσουμε ότι το $f(x)$ είναι ένα μονικό πολυώνυμο με απλές ρίζες W . Δηλαδή

$$f(x) = \prod_{w \in W} (x - w).$$

Υπολογίζουμε το πολυώνυμο για κάποιο $a \in W$

$$f(x + a) - f(x) - f(a) = f(x + a) - f(x),$$

και παρατηρούμε ότι είναι ίσο με το 0, αφού

$$f(x + a) = \prod_{w \in W} (x + a - w) = \prod_{w - a \in W} (x - w) = \prod_{w \in W} (x - w). \quad (0.1)$$

Σχηματίζουμε για $w \in W$ το πολυώνυμο

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

και παρατηρούμε ότι είναι βαθμού $\deg(f) - 1$ και ότι έχει τόσες ρίζες όσες το $\#W = \deg f$. Άρα $H(x)$ είναι ταυτοτικά ίσο με το 0 (Τα μη μηδενικά πολυώνυμα έχουν τόσες ρίζες όσες και ο βαθμός τους στο $\bar{k}$) και έχουμε ότι

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

Στην εξίσωση (0.1) χρησιμοποιήσαμε ότι αν το w διατρέχει το W τότε και το $w - a$ διατρέχει το W (το a είναι σταθερό στοιχείο του διανυσματικού χώρου W .)

Παραγωγίζοντας την σχέση

$$f(x + a) = f(x) + f(a)$$

έχουμε (α τυχαίο στοιχείο του $\bar{k}$)

$$f'(a) = \left. \frac{d}{dx} \right|_{x=0} f(x + a) = \left. \frac{d}{dx} \right|_{x=0} f(x) = f'(0).$$

Δηλαδή το πολυώνυμο $f'(x)$ έχει άπειρες ρίζες (όλα τα a) και η παράγωγος είναι σταθερά ίση με $c = f'(0)$. Άρα

$$f(x) = cx + \sum_{j=2}^n a_j x^{n_j}$$

όπου τα n_j είναι όλα διαιρετά με p . Στόχος μας είναι να δείξουμε ότι τα n_j είναι δυνάμεις του p . Μπορούμε να γράψουμε

$$f(x) = cx + f_1(x)^p,$$

όπου

$$f_1(x) = \sum_{j=2}^n (a_j)^{1/p} x^{n_j/p}.$$

(Το $(a_j)^{1/p}$ έχει νόημα στο $\bar{k}$.) Παρατηρούμε ότι το f_1 ικανοποιεί και αυτό την εξίσωση

$$f_1(x+y) = f_1(x) + f_1(y)$$

και συνεπώς $f_1(x) = c_2x + f_2(x)$, δηλαδή

$$f(x) = cx + c_2x^p + f_2(x)^p.$$

Συνεχίζουμε επαγωγικά.

Άσκηση 4. Αποδείξτε ότι στην χαρακτηριστική 0 τα ανάγωγα πολυώνυμα δεν έχουν πολλαπλές ρίζες. Τι μπορεί να συμβεί στην πεπερασμένη χαρακτηριστική;
Λύση Γνωρίζουμε ότι αναγκαία και ικανή συνθήκη για να έχει ένα πολυώνυμο f πολλαπλή ρίζα το a θα πρέπει το $f(a) = f'(a) = 0$. Θεωρούμε το ιδεώδες των πολυωνύμων που μηδενίζονται στο a (δείξτε ότι είναι ιδεώδες!). Το ιδεώδες αυτό είναι κύριο της μορφής $f_1k[x]$ δηλαδή κάθε πολυώνυμο που μηδενίζεται στο a πρέπει να διαιρείται με f_1 . Αφού $f(a)$ και f ανάγωγο έχουμε ότι $f_1 = cf$, όπου το $c \in k$. Όμως $f'(a) = 0$ αν το a είναι διπλή ρίζα και συνεπώς $f \mid f'$ δηλαδή $f' = fh$. Όταν η χαρακτηριστική του k είναι 0 με δεδομένο ότι το f δεν είναι σταθερά αυτό δεν μπορεί να συμβεί γιατί το f έχει βαθμό n και η παράγωγος έχει βαθμό $n-1$. Στην χαρακτηριστική p όμως αυτό είναι δυνατόν αφού μπορεί το $f' = 0$ αρκεί το $p \mid n-1$ και (αρκετούς όρους μικρότερου βαθμού).

Παρόλα αυτά θα πρέπει να πάμε σε σώματα της μορφής $\mathbb{F}_p(t)$ για να βρούμε ανάγωγα πολυώνυμα με πολλαπλές ρίζες. Στο $\mathbb{F}_p$ κάθε ανάγωγο πολυώνυμο έχει απλές ρίζες γιατί διαιρεί κάποιο $x^{p^h} - x$ το οποίο έχει απλές ρίζες.

Άσκηση 5. Αποδείξτε ότι σε ένα αντιμεταθετικό δακτύλιο με μονάδα R τα παρακάτω είναι ισοδύναμα: Ένα ιδεώδες I είναι πρώτο αν και μόνο αν R/I αχέραια περιοχή. Ένα ιδεώδες I είναι μέγιστο αν και μόνο αν R/I είναι σώμα. Αποδείξτε ότι αν το $f(x)$ είναι ένα ανάγωγο πολυώνυμο τότε το $K[x]/\langle f \rangle$ είναι σώμα.

Λύση: Αυτό μπορεί να το βρεί κανείς σε οποιοδήποτε βιβλίο Άλγεβρας για

παράδειγμα στον J. Fraleigh, (ΠΕΚ 3η έκδοση) είναι το 5.9 σελ 369, 5.10 σελ. 371)

Άσκηση 6. Αποδείξτε ότι στους δακτυλίους $\mathbb{Z}$ και $F[X]$, όπου F σώμα ένα μη μηδενικό ιδεώδες είναι πρώτο αν και μόνο αν είναι μέγιστο. Ισχύει αυτό γενικά σε κάθε αντιμεταθετικό δακτύλιο;

Λύση: Ισχύει πάντα (σε αντιμεταθετικούς δακτυλίους με μονάδα) ότι ένα μέγιστο είναι πρώτο. Στην περίπτωση του $\mathbb{Z}$ ένα πρώτο ιδεώδες θα δώσει ως πηλίκo μια ακέραια περιοχή που είναι πεπερασμένη άρα σώμα!

Γενικότερα μπορούμε να δώσουμε μια κοινή απόδειξη και για το $\mathbb{Z}$ και για το $F[X]$ βασισμένοι στο ότι και οι δύο δακτύλιοι είναι περιοχές κυρίων ιδεωδών. Έστω R περιοχή κυρίων ιδεωδών. Αν λοιπόν το I είναι πρώτο ιδεώδες τότε το $I = fR$ όπου το f θα είναι ανάγωγο. Αν έχουμε ένα μη μηδενικό στοιχείο $g \bmod I$ τότε τα f, g είναι πρώτα μεταξύ τους και θα παράγουν ένα ιδεώδες ώστε $I = fR \subsetneq \langle f, g \rangle < R$. Όμως $\langle f, g \rangle = tR$ και θα πρέπει $t \mid f$ το οποίο σημαίνει ότι t είναι μονάδα, άρα $\langle f, g \rangle = R$ και συνεπώς μπορούμε να γράψουμε $1 = af + bg$. Τότε το $b \bmod I$ είναι ο αντίστροφος του $g \bmod I$.

Τέλος, παρατηρούμε ότι υπάρχουν δακτύλιοι στους οποίους τα πρώτα ιδεώδη δεν είναι μέγιστα. Για παράδειγμα στον $\mathbb{Z}[x]$ των πολυωνύμων με συνετελεστές στο $\mathbb{Z}$ μπορούμε να θεωρήσουμε τον πυρήνα του ομορφισμού

$$\phi : \mathbb{Z}[x] \rightarrow \mathbb{F}_p[x]$$

ο οποίος στέλνει πολυώνυμο $\sum a_i x^i \in \mathbb{Z}[x]$ σε πολυώνυμο $\sum \bar{a}_i x^i \in \mathbb{F}_p[x]$ θεωρώντας κάθε συντελεστή τους modulo p . Ο πυρήνας $\ker \phi$ είναι ιδεώδες πρώτο και όχι μέγιστο αφού $\mathbb{Z}[x]/\ker \phi \cong \mathbb{F}_p[x]$ είναι ακέραια περιοχή και όχι σώμα.