Περιεχόμενα

Κεφάλαιο 5

Πολυώνυμα
Πρόχειρες Σημειώσεις

Στο κεφάλαιο αυτό [1] μελετάμε βασικές ιδιότητες των πολυωνύμων με συντελεστές πραγματικούς ή μιγαδικούς αριθμούς.

[1] Τα παρακάτω έχουν ληφθεί, με μερικές αλλαγές, από το βιβλίο *Μια Εισαγωγή στη Γραμμικής Άλγεβρα*, Βάρσος, Δεριζιώτης, Εμμανουήλ, Μαλιάκας, Μελάς, Ταλέλλη, Εκδόσεις Σοφία 2012.

5.1 Υπενθυμίσεις

Στα επόμενα υπενθυμίζουμε τη σχετική ορολογία και τις βασικές ιδιότητες των πολυωνύμων.

Εδώ δεν δίνουμε ένα μαθηματικό ορισμό του πολυωνύμου, αλλά απλώς τα πολυώνυμα θα τα θεωρούμε ως εκφράσεις της μορφής

$$a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

όπου n είναι ένας μη αρνητικός ακέραιος αριθμός και τα $a_i, i = 0, 1, \ldots, n$, τα οποία ονομάζονται ***συντελεστές*** του πολυωνύμου, είναι ακέραιοι, ρητοί, πραγματικοί ή μιγαδικοί αριθμοί. Οι εκφράσεις της μορφής $a_i x^i$ λέγονται όροι του πολυωνύμου ή ***μονώνυμα***.

Στα επόμενα συνήθως, εκτός αν αναφέρεται διαφορετικά, θα ασχολούμαστε με πολυώνυμα με συντελεστές από το σύνολο $\mathbb{F}$, *όπου με* $\mathbb{F}$ *θα παριστάνουμε είτε το σύνολο* $\mathbb{R}$ *των πραγματικών αριθμών είτε το σύνολο* $\mathbb{C}$ *των μιγαδικών αριθμών*. Το δε σύνολο όλων των πολυωνύμων με συντελεστές από το σύνολο $\mathbb{F}$ θα συμβολίζεται με $\mathbb{F}[x]$.

Για το σύμβολο x, έχει επικρατήσει η ονομασία ***μεταβλητή*** του πολυωνύμου.

Δύο πολυώνυμα

$$a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0,$$

$$b_m x^m + b_{m-1}x^{m-1} + \cdots b_1 x + b_0$$

με $n \geq m$ είναι ***ίσα*** αν $a_i = b_i$ για όλα τα $i = 0, 1, \ldots, m$ και $a_{n+1} = ... = a_n = 0$.

Εδώ πρέπει να διευκρινισθεί ότι μπορούμε να "παρεμβάλουμε" ή να "παραβλέπουμε" όρους της μορφής $0x^i$ και το πολυώνυμο να παραμένει το ίδιο.

Συνεπώς κάθε μη μηδενικό πολυώνυμο $a(x) \in \mathbb{F}$ έχει μοναδική παράσταση της μορφής

$$a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

με $a_i \in \mathbb{F}$ και $a_n \neq 0$.

Αν $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ με $a_n \neq 0$, το μη αρνητικό ακέραιο n τον ονομάζουμε ***βαθμό*** του πολυωνύμου και το συμβολίζουμε με $\deg(a(x)) = n$.

Τον όρο $a_n x^n$ τον ονομάζουμε ***μεγιστοβάθμιο όρο*** του πολυωνύμου και το συντελεστή a_n ***μεγιστοβάθμιο συντελεστή***.

Αν ο μεγιστοβάθμιος συντελεστής σε ένα πολυώνυμο είναι το 1, τότε το πολυώνυμο ονομάζεται ***μονικό***.

Αν $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ με $a_n \neq 0$, τότε το πολυώνυμο $a_n^{-1}a(x)$ προφανώς είναι μονικό και το ονομάζουμε το ***αντίστοιχο μονικό πολυώνυμο*** του $a(x)$.

Στην περίπτωση που το πολυώνυμο είναι μηδενικού βαθμού, δηλαδή έχουμε πολυώνυμο της μορφής $a(x) = a_0$, τότε αυτό ονομάζεται ***σταθερό*** πολυώνυμο. Τώρα αν όλοι οι συντελεστές ενός πολυωνύμου είναι μηδενικοί, τότε το πολυώνυμο αυτό ονομάζεται το ***μηδενικό*** πολυώνυμο και συνήθως συμβολίζεται ως 0. Για το μηδενικό πολυώνυμο, αφού όλοι οι συντελεστές του είναι ίσοι με το μηδέν, δεν ορίζουμε βαθμό. Όπως βλέπουμε το σύνολο συντελεστών μπορεί να θεωρηθεί ότι αποτελείται από τα σταθερά πολυώνυμα και με αυτή την έννοια έχουμε $\mathbb{F} \subseteq \mathbb{F}[x]$.

Αν $a(x), b(x) \in \mathbb{F}[x]$ τότε παρεμβάλλοντας , αν χρειάζεται, μηδενικούς όρους της μορφής $0x^i$, μπορούμε να υποθέσουμε ότι

$$a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

$$b(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0.$$

Υπενθυμίζουμε ότι στο σύνολο $\mathbb{F}[x]$ όλων των πολυωνύμων ορίζεται η ***πρόσθεση*** πολυωνύμων και ο ***πολλαπλασιασμός*** πολυωνύμων ως εξής.

- $a(x) + b(x) = (a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0)$
  λέγεται ***άθροισμα*** των πολυωνύμων $a(x)$ και $b(x)$ και συμβολίζεται με $(a + b)(x)$. Δηλαδή το άθροισμα δύο πολυωνύμων είναι το πολυώνυμο που έχει ως συντελεστές το άθροισμα *ομοβαθμίων* συντελεστών.

- $a(x)b(x) = c_r x^r + c_{r-1}x^{r-1} + \cdots + c_1 x + c_0$, όπου $c_0 = a_0 b_0$, $c_1 = a_0 b_1 + a_1 b_0$ και γενικά
  $$c_k = a_0 b_k + a_1 b_{k-1} + ... + a_{k-1} b_1 + a_k b_0$$
  λέγεται ***γινόμενο*** των πολυωνύμων $a(x)$ και $b(x)$ και συμβολίζεται με $(ab)(x)$ (ή με $a(x)b(x)$).

Για παράδειγμα, αν $a(x) = x^4 + 3x^3 + x$ και $b(x) = 2x^3 - x + 1$ έχουμε $a(x)b(x) = 2x^7 + 6x^6 - x^5 + 3x^3 - x^2 + x$.

Πρόταση 5.1.1. *Στο σύνολο $\mathbb{F}[x]$ η πρόσθεση και ο πολλαπλασιασμός ικανοποιούν τις ακόλουθες ιδιότητες για κάθε $a(x), b(x), c(x) \in \mathbb{F}[x]$:*

1. $(a(x) + b(x)) + c(x) = a(x) + (b(x) + c(x))$.
2. $a(x) + b(x) = b(x) + a(x)$.
3. $a(x) + 0 = 0 + a(x) = a(x)$.
4. *Για κάθε $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0 \in \mathbb{F}[x]$ υπάρχει το $-a(x) = (-a_n)x^n + (-a_{n-1})x^{n-1} + \cdots (-a_1)x + (-a_0) \in \mathbb{F}[x]$ τέτοιο ώστε $a(x) + (-a(x)) = (-a(x)) + a(x) = 0$.*
5. $(a(x)b(x))c(x) = a(x)(b(x)(x))$.
6. $a(x)b(x) = b(x)a(x)$.
7. $a(x)1 = 1a(x) = a(x)$.
8. $(a(x) + b(x))c(x) = a(x)c(x) + b(x)c(x)$.

Απόδειξη. Όλες οι αποδείξεις είναι άμεσες εκτός ίσως από την τελευταία, η οποία αφήνεται ως άσκηση. □

Για το βαθμό και τις πράξεις έχουμε την ακόλουθη πρόταση.

Πρόταση 5.1.2. *Έστω $a(x)$ και $b(x)$ μη μηδενικά πολυώνυμα, τότε ισχύει:*

1. *Είτε $a(x) + b(x) = 0$ είτε $\deg(a(x) + b(x)) \leq \max(\deg a(x), \deg b(x))$.*
   Η ανισότητα στην προηγούμενη σχέση είναι γνήσια μόνο στην περίπτωση που τα δύο πολυώνυμα έχουν τον ίδιο βαθμό και αντίθετους μεγιστοβάθμιους συντελεστές
2. $\deg(a(x)b(x)) = \deg a(x) + \deg b(x)$.
3. $\deg(a(x)^k) = k \deg a(x)$ *για κάθε θετικό ακέραιο* k.

Απόδειξη. Άσκηση. □

5.2 Διαιρετότητα, Ανάγωγα πολυώνυμα

Στα επόμενα θα δούμε ότι στο σύνολο $\mathbb{F}[x]$ ισχύει ένας αλγόριθμος ***διαίρεσης*** πολυωνύμων ανάλογος με τον γνωστό αλγόριθμο της διαίρεσης στο σύνολο $\mathbb{Z}$ των ακεραίων αριθμών. Αυτό μας δίνει τη δυνατότητα να διαπιστώσουμε ότι τα δύο σύνολα $\mathbb{Z}$ και $\mathbb{F}[x]$ έχουν σημαντικές *ομοιότητες*.

Έστω $a(x), b(x) \in \mathbb{F}[x]$. Θα λέμε ότι το $a(x)$ ***διαιρεί*** $b(x)$ και θα συμβολίζουμε $a(x)|b(x)$ αν υπάρχει $\pi(x) \in \mathbb{F}[x]$ τέτοιο ώστε $b(x) = a(x)\pi(x)$.

Πολλές φορές αντί να πούμε ότι το $a(x)$ διαιρεί το $b(x)$ λέμε ότι το $b(x)$ είναι ***πολλαπλάσιο*** του $a(x)$ ή ότι το $b(x)$ ***διαιρείται*** από το $a(x)$.

Ας δούμε μερικές άμεσες συνέπειες του προηγούμενου ορισμού, τις οποίες θα χρησιμοποιούμε συχνά στα επόμενα χωρίς ιδιαίτερη αναφορά.

1. Το μηδενικό πολυώνυμο διαιρείται από κάθε άλλο πολυώνυμο. Πράγματι, για κάθε $a(x) \in \mathbb{F}[x]$ ισχύει $a(x)0 = 0$.
Το μηδενικό πολυώνυμο 0 διαιρεί μόνο το μηδενικό πολυώνυμο.

2. Υποθέτουμε ότι $a(x)|b(x)$. Τότε υπάρχει μοναδικό $\pi(x) \in \mathbb{F}[x]$ τέτοιο ώστε $b(x) = a(x)\pi(x)$.

Πράγματι αν υπήρχε και ένα άλλο $\pi'(x) \in \mathbb{F}[x]$ με $b(x) = a(x)\pi'(x)$, τότε θα είχαμε

$$b(x) = a(x)\pi(x) = a(x)\pi'(x).$$

Δηλαδή $a(x)(\pi(x) - \pi'(x)) = 0$ και επειδή το $a(x)$ δεν είναι το μηδενικό πολυώνυμο έχουμε $\pi(x) - \pi'(x) = 0$, άρα $\pi(x) = \pi'(x)$.

3. Αν $a(x)|b(x)$, τότε $\deg(a(x)) \leq \deg(b(x))$.

Πράγματι, αυτό είναι σαφές από την Πρόταση 5.1.2.

4. Κάθε (μη μηδενικό) σταθερό πολυώνυμο c διαιρεί κάθε άλλο πολυώνυμο. Πράγματι, για κάθε $\varphi(x) \in \mathbb{F}[x]$ έχουμε $a(x) = c(c^{-1}a(x))$.

5. Αν $a(x)|b(x)$ και $b(x)|c(x)$, τότε το $a(x)|c(x)$. 6. Υποθέτουμε ότι το $a(x)|b_1(x)$ και $a(x)|b_2(x)$. Τότε $a(x)$ διαιρεί το $\alpha(x)b_1(x) + \beta(x)b_2(x)$, για όλα τα $\alpha(x), \beta(x) \in \mathbb{F}[x]$. (γιατί;).

Ένα μη σταθερό πολυώνυμο $p(x) \in \mathbb{F}[x]$ θα λέγεται ***ανάγωγο*** επί του $\mathbb{F}$ (ή ανάγωγο στο $\mathbb{F}[x]$) αν οι μόνοι διαιρέτες του στο $\mathbb{F}[x]$ είναι τα σταθερά πολυώνυμα και τα πολυώνυμα της μορφής $cp(x)$, $c \in \mathbb{F}$.

Ισοδύναμα το πολυώνυμο $p(x) \in \mathbb{F}[x]$ είναι ανάγωγο επί του $\mathbb{F}$ αν από τη σχέση $p(x) = a(x)b(x)$, με $a(x), b(x) \in \mathbb{F}[x]$ προκύπτει ότι ένα από τα $a(x), b(x)$ είναι σταθερό πολυώνυμο.

Παραδείγματα

Η έννοια του αναγώγου πολυωνύμου είναι σημαντική στη μελέτη των πολυωνύμων. Όπως θα δούμε στα επόμενα, τα ανάγωγα πολυώνυμα έχουν ιδιότητες ανάλογες με τις ιδιότητες των πρώτων αριθμών στους ακεραίους. Συγκεκριμένα ισχύει το εξής σημαντικό θεώρημα.

Θεώρημα 5.2.1. *Κάθε μη σταθερό πολυώνυμο $a(x) \in \mathbb{F}[x]$ γράφεται ως γινόμενο μιας σταθεράς και μονικών αναγώγων πολυωνύμων στο $\mathbb{F}[x]$ κατά μοναδικό τρόπο. Συγκεκριμένα υπάρχουν μοναδικά μονικά ανάγωγα πολυώνυμα $p_i(x) \in \mathbb{F}[x], i = 1, 2, \ldots, n$ και μοναδικό $c \in \mathbb{F}$ τέτοια ώστε, αν δεν ληφθεί υπόψη η σειρά των παραγόντων, $a(x) = cp_1(x)p_2(x)\cdots p_n(x)$.*

Η μοναδικότητα στο παραπάνω θεώρημα θα αποδειχθεί αργότερα καθώς χρειαζόμαστε ενδιάμεσα αποτελέσματα. Έτσι θα δώσουμε όλη την απόδειξη αργότερα.

Το επόμενο θεώρημα, γνωστό ως ***Ευκλείδεια διαίρεση*** (ή ***ταυτότητα διαίρεσης πολυωνύμων***) είναι πολύ σημαντικό στη μελέτη ιδιοτήτων των πολυωνύμων.

Θεώρημα 5.2.2. *Έστω $a(x), b(x) \in \mathbb{F}[x]$ με $a(x) \neq 0$. Τότε υπάρχουν μοναδικά $\pi(x), \upsilon(x) \in \mathbb{F}[x]$ τέτοια ώστε $b(x) = a(x)\pi(x) + \upsilon(x)$ και ή $\upsilon(x) = 0$ ή $\deg(\upsilon(x)) < \deg(a(x))$.*

Απόδειξη. Ύπαρξη. Έστω ότι το πολυώνυμο $a(x)$ διαιρεί το $b(x)$. Τότε προφανώς από τη σχέση $b(x) = a(x)\pi(x)$ έχουμε ότι τα $\pi(x)$ και $\upsilon(x) = 0$ πληρούν τις υποθέσεις του Θεωρήματος.

Υποθέτουμε ότι το $a(x)$ δεν διαιρεί το $b(x)$ και έστω

$$\mathcal{A} = \{b(x) - a(x)\tau(x)\},$$

όπου $\tau(x) \in \mathbb{F}[x]\}$. Έστω $\upsilon(x) = b(x) - a(x)\pi(x)$ ένα στοιχείο του συνόλου $\mathcal{A}$ με τον μικρότερο δυνατό βαθμό. Τότε προφανώς $b(x) = a(x)\pi(x) + \upsilon(x)$.

Θα δείξουμε ότι $\deg(\upsilon(x)) < \deg(a(x))$.

Πράγματι, υποθέτουμε ότι

$$\upsilon(x) = b(x) - a(x)\pi(x) = a_n x^n + a_{n-1}x^{n-1} +, \cdots + a_1 x + a_0,$$

$$a(x) = b_m x^m + b_{m_{-1}} x^{m-1} + \cdots + b_1 x + b_0$$

και

$$\deg(\upsilon(x)) = n \geq m = \deg(a(x)).$$

Τότε τα πολυώνυμα

$$\upsilon(x),\ (a_n b_m^{-1})x^{n-m}a(x)$$

είναι του ιδίου βαθμού και έχουν αντίθετους συντελεστές, επομένως το πολυώνυμο

$$\upsilon(x) - (a_n b_m^{-1})x^{n-m}a(x),$$

έχει βαθμό μικρότερο απο το βαθμό του $\upsilon(x)$ και επιπλέον

$$\upsilon(x) - (a_n b_m^{-1})x^{n-m}a(x) = b(x) - (\pi(x) + (a_n b_m^{-1})x^{n-m})a(x) \in \mathcal{A}.$$

Τούτο είναι άτοπο από την εκλογή του πολυωνύμου $\upsilon(x)$ ως πολυώνυμο με τον μικρότερο βαθμό από όλα τα πολυώνυμα που ανήκουν στο σύνολο $\mathcal{A}$. Επομένως $\deg(\upsilon(x)) < \deg(a(x))$.

Μοναδικότητα. Τα πολυώνυμα $\pi(x)$ και $\upsilon(x)$ με την ιδιότητα $b(x) = a(x)\pi(x) + \upsilon(x)$ και $\deg(\upsilon) < \deg(a(x))$ είναι μοναδικά. Πραγματι, υποθέτουμε ότι εκτός από τα $\pi(x)$ και $\upsilon(x)$ υπάρχουν και τα πολυώνυμα $\pi'(x)$ και $\upsilon'(x)$ τέτοια ώστε

$$b(x) = a(x)\pi'(x) + \upsilon'(x)$$

και

$$\deg(\upsilon'(x)) < \deg(a(x))$$

Τότε αφαιρώντας κατά μέλη τις σχέσεις $b(x) = a(x)\pi(x)+\upsilon(x)$ και $b(x) = a(x)\pi'(x)+\upsilon'(x)$ έχουμε

$$a(x)(\pi(x) - \pi'(x)) = \upsilon'(x) - \upsilon(x).$$

Αν $\upsilon'(x) - \upsilon(x) \neq 0$, τότε και $\pi(x) - \pi'(x) \neq 0$, οπότε από την Πρόταση 5.1.2 έχουμε ότι $\deg(\upsilon'(x) - \upsilon(x)) \geq \deg(a(x))$. Τούτο είναι άτοπο, αφού $\deg(\upsilon(x) - \upsilon'(x)) \leq \max(\deg(\upsilon(x)), \deg(\upsilon'(x))) < \deg(a(x))$. Άρα $\upsilon(x) = \upsilon'(x)$ και $\pi(x) = \pi'(x)$. □

Το πολυώνυμα $\pi(x)$ και $\upsilon(x)$ στο προηγούμενο Θεώρημα ονομάζονται αντίστοιχα το ***πηλίκο*** και το ***υπόλοιπο*** της διαίρεσης του πολυωνύμου $b(x)$ δια του πολυωνύμου $a(x)$.

Παρατηρήσεις 5.2.3.

1. Στο προηγούμενο Θεώρημα, αν $b(x) = 0$ ή $\deg(b(x)) < \deg(a(x))$, τότε προφανώς $\pi(x) = 0$ και $\upsilon(x) = b(x)$.

2. Αν δούμε προσεκτικά την απόδειξη του προηγουμένου Θεωρήματος, θα αναγνωρίσουμε τη γνωστή σε όλους μας μέθοδο διαίρεσης πολυωνύμων. Θα δώσουμε ένα παράδειγμα, όπου τούτο θα φανεί καλύτερα.

Παράδειγμα. Έστω

$$b(x) = 4x^5 - 3x^4 - 7x^2 + 6 \text{ και } a(x) = x^3 + 7x^2 + 3x - 2.$$

Θέλουμε να κάνουμε την Ευκλείδεια διαίρεση του $b(x)$ με το $a(x)$. Παρατηρούμε ότι ο βαθμός του $b(x)$ είναι μεγαλύτερος από το βαθμό του $a(x)$ επομένως πρέπει να βρούμε ένα πολυώνυμο $\pi(x)$ τέτοιο ώστε $\deg(b(x) - a(x)\pi(x)) < \deg(a(x))$.

Ο μεγιστοβάθμιος συντελεστής του $b(x)$ είναι 4, πολλαπλασιάζουμε το πολυώνυμο $a(x)$ με το μονώνυμο $4x^{5-3}$, το αποτέλεσμα $(4x^{5-3})\cdot a(x) = 4x^5+28x^4+12x^3-8x^2$ το αφαιρούμε από το $b(x)$ και έχουμε

$$b(x) - (4x^{5-3}) \cdot a(x) = -31x^4 - 12x^3 + x^2 + 6.$$

Το πολυώνυμο $\pi_1(x) = 4x^2$ είναι ένα "ενδιάμεσο" πηλίκο και το πολυώνυμο

$$\upsilon_1(x) = b(x) - (4x^{5-3}) \cdot a(x) = -31x^4 - 12x^3 + x^2 + 6$$

είναι ένα "ενδιάμεσο " υπόλοιπο.

Παρατηρούμε ότι ο βαθμός του $\upsilon_1(x) = -31x^4-12x^3+x^2+6$ είναι μεγαλύτερος από το βαθμό του $a(x)$, επομένως επαναλαμβάνουμε την προηγούμενη διαδικασία μέχρι να προκύψει ενδιάμεσο υπόλοιπο 0 ή βαθμού μικρότερου του βαθμού του $a(x)$. Το τελευταίο ενδιάμεσο πηλίκο και το τελευταίο ενδιάμεσο υπόλοιπο είναι το ζητούμενο πηλίκο και το ζητούμενο υπόλοιπο.

Σχηματικά η προηγούμενη διαδικασία θα μπορούσε να περιγραφεί ως εξής

$4x^5$	$-3x^4$	$+0x^3$	$-7x^2$	$+0x$	$+6$	x^3+7x^2+3x-2
$4x^5$	$+28x^4$	$+12x^3$	$-8x^2$			$4x^2-31x+205$
	$-31x^4$	$-12x^3$	$+x^2$	$+0x$	$+6$	
	$-31x^4$	$-217x^3$	$-93x^2$	$+62x$		
		$205x^3$	$+94x^2$	$-62x$	$+6$	
		$205x^3$	$+143x^2$	$+615x$	-410	
			$-1341x^2$	$-677x$	$+416$	

5.3 Μέγιστος κοινός διαιρέτης

Πριν δώσουμε τον ορισμό του μέγιστου κοινού διαιρέτη πολυωνύμων, θα θέλαμε να παρατηρήσουμε ότι, αν $a(x), b(x) \in \mathbb{F}[x]$, τότε, όπως έχουμε επισημάνει, κάθε σταθερό μη μηδενικό πολυώνυμο c διαιρεί και τα δύο πολυώνυμα. Δηλαδή για τα πολυώνυμα αυτά υπάρχουν *κοινοί διαιρέτες*. Επομένως υπάρχουν κοινοί διαιρέτες δύο πολυωνύμων οι οποίοι είναι μονικά πολυώνυμα.

Ορισμός 5.3.1. *Έστω $a(x)theta(x) \in \mathbb{F}[x]$ όχι και τα δύο μηδενικά πολυώνυμα, ένα πολυώνυμο $d(x) \in \mathbb{F}[x]$ θα λέγεται* ***μέγιστος κοινός διαιρέτης*** *των $a(x)$ και $b(x)$ αν:*
(i) $d(x)|a(x)$ και $d(x)|b(x)$. Δηλαδή το πολυώνυμο $d(x)$ είναι κοινός διαιρέτης των $a(x)$ και $b(x)$.
(ii) Το $d(x)$ είναι μονικό πολυώνυμο.
(iii) Αν $\delta(x) \in \mathbb{F}[x]$ με $\delta(x)|a(x)$ και $\delta(x)|b(x)$, τότε $\delta(x)|d(x)$.

Θα δείξουμε ότι ο μέγιστος κοινός διαιρέτης δύο πολυωνύμων, εκ των οποίων τουλάχιστον το ένα είναι μη μηδενικό, υπάρχει και είναι μοναδικός.

Το μέγιστο κοινό διαιρέτη δύο πολυωνύμων $a(x)$ και $b(x)$ θα τον συμβολίζουμε με $d(x) = \text{μκδ}(a(x), b(x))$ ή απλά $d(x) = (a(x), b(x))$

Μπορούμε να δούμε εύκολα ότι αν υπάρχει μκδ των $a(x)$ και $b(x)$, τότε αυτός είναι μοναδικός. Πράγματι υποθέτουμε ότι υπάρχουν δύο πολυώνυμα $d_1(x)$ και $d_2(x)$ με τις ιδιότητες του ορισμού. Τότε από τις (i) και (iii) του ορισμού έχουμε ότι $d_1(x)|d_2(x)$ και $d_2(x)|d_1(x)$. Δηλαδή υπάρχει $c \in \mathbb{F}[x]$ τέτοιο ώστε $d_1(x) = cd_2(x)$. Αλλά τα $d_1(x), d_2(x)$ είναι μονικά. Άρα $d_1(x) = d_2(x)$.

Πριν αποδείξουμε ότι ο μκδ δύο πολυωνύμων υπάρχει επισημαίνουμε ότι αν και τα δύο πολυώνυμα είναι μηδενικά πολυώνυμα, τότε ο μκδ δεν ορίζεται, αφού η (iii) στον ορισμό δεν ικανοποιείται (γιατί;).

Θα αποδείξουμε τώρα ένα Θεώρημα το οποίο όχι μόνο μας εξασφαλίζει την ύπαρξη του μκδ δύο πολυωνύμων, αλλά μας δίνει και μία έκφραση του ως "γραμμικό" συνδυασμό των δύο πολυωνύμων.

Θεώρημα 5.3.2. *Έστω $a(x), b(x) \in \mathbb{F}[x]$ όχι και τα δύο μηδενικά πολυώνυμα. Τότε υπάρχει ο μέγιστος κοινός διαιρέτης $d(x)$ των $a(x)$ και $b(x)$ και επιπλέον υπάρχουν $\alpha(x), \beta(x) \in \mathbb{F}[x]$ τέτοια ώστε*

$$d(x) = \alpha(x)a(x) + \beta(x)b(x).$$

Απόδειξη. Έστω

$$\mathcal{U} = \{\lambda(x)a(x) + \kappa(x)b(x) \mid \lambda(x), \kappa(x) \in \mathbb{F}[x]\}.$$

Παρατηρούμε ότι στο σύνολο $\mathcal{U}$ ανήκουν τα πολυώνυμα $a(x)$ και $b(x)$ (γιατί ;). Επίσης στο σύνολο $\mathcal{U}$ ανήκουν μονικά πολυώνυμα. Πράγματι αν $\eta(x) = \lambda(x)a(x) + \kappa(x)b(x)$ είναι ένα μη μηδενικό στοιχείο του $\mathcal{U}$ με συντελεστή του μεγιστοβαθμίου όρου c, τότε το πολυώνυμο $c^{-1}\eta(x) = (c^{-1}\lambda(x))a(x) + (c^{-1}\kappa(x))b(x)$ είναι μονικό και ανήκει στο σύνολο $\mathcal{U}$.

Από τις προηγούμενες παρατηρήσεις έπεται ότι μπορούμε να επιλέξουμε ένα στοιχείο $d(x) = \alpha(x)a(x) + \beta(x)b(x)$ του $\mathcal{U}$, το οποίο να είναι μονικό και να έχει τον μικρότερο βαθμό από όλα τα μη μηδενικά στοιχεία του $\mathcal{U}$.

Το $d(x)$ είναι μονικό, άρα πληροί τη συνθήκη (ii) του ορισμού.

Έστω $\delta(x) \in \mathbb{F}[x]$ με $\delta(x)|a(x)$ και $\delta(x)|b(x)$, τότε προφανώς το $\delta(x)|d(x)$. Άρα το $d(x)$ πληροί τη συνθήκη (iii) του ορισμού.

Απομένει να αποδείξουμε τη συνθήκη (i).

Έστω $\tau(x) = \lambda(x)a(x) + \kappa(x)b(x)$ ένα στοιχείο του συνόλου $\mathcal{U}$, θα δείξουμε ότι $d(x)|\tau(x)$.

Από τον αλγόριθμο διαίρεσης πολυωνύμων υπάρχουν μοναδικά $\pi(x), \upsilon(x) \in \mathbb{F}[x]$ τέτοια ώστε $\tau(x) = \pi(x)d(x) + \upsilon(x)$ με $\upsilon(x) = 0$ ή $\deg(\upsilon(x)) < \deg(d(x))$. Επομένως έχουμε

$$\upsilon(x) = \tau(x) - \pi(x)d(x) = \lambda(x)a(x) + \kappa(x)b(x) - \pi(x)(\alpha(x)a(x) + \beta(x)b(x))$$

$$= (\lambda(x) - \pi(x)\alpha(x))a(x) + (\kappa(x) - \pi(x)\beta(x))b(x) \in \mathcal{U}.$$

Υποθέτουμε ότι το $\upsilon(x)$ δεν είναι το μηδενικό πολυώνυμο, αν c είναι ο συντελεστής του μεγιστοβαθμίου όρου του, τότε το πολυώνυμο $c^{-1}\upsilon(x)$ είναι μονικό, ανήκει στο $\mathcal{U}$ και έχει βαθμό ίσο με τον βαθμό του $\upsilon(x)$, ο οποίος είναι γνήσια μικρότερος από το βαθμό του $d(x)$. Αυτό είναι άτοπο από την επιλογή του πολυωνύμου $d(x)$. Αρα $\upsilon(x) = 0$. Δηλαδή το $d(x)$ είναι κοινός διαιρέτης όλων των στοιχείων του συνόλου $\mathcal{U}$, άρα και των $a(x)$ και $b(x)$. □

Παρατηρήσεις 5.3.3.

1. Όπως προκύπτει από τον ορισμό και προηγούμενες παρατηρήσεις ο μκδ δύο πολυωνύμων έχει το μεγαλύτερο βαθμό από όλους τους κοινούς διαιρέτες των δύο πολυωνύμων.

2. Έστω $a(x)$ και $b(x)$ δύο πολυώνυμα με το $a(x)|b(x)$. Τότε μκδ $(a(x), b(x)) = c^{-1}a(x)$, όπου c είναι ο συντελεστής του μεγιστοβαθμίου όρου του $a(x)$.

3. Έστω $a(x)$ και $b(x)$ δύο πολυώνυμα και c_1, c_2 δύο μη μηδενικά στοιχεία του συνόλου $\mathbb{F}$. Τότε μκδ $(a(x), b(x)) =$ μκδ $(c_1a(x), c_2b(x))$ (γιατί ;).

Ευκλείδειος Αλγόριθμος

Το προηγούμενο Θεώρημα δεν μας δίνει ένα τρόπο υπολογισμού του μκδ δύο πολυωνύμων $a(x)$ και $b(x)$, πολύ δε περισσότερο πώς μπορούμε να υπολογίσουμε πολυώνυμα συντελεστές $\alpha(x)$ και $\beta(x)$ τέτοια ώστε μκδ $(a(x), b(x)) = \alpha(x)a(x) + \beta(x)b(x)$.

Η επόμενη πρόταση αποτελεί το κύριο βήμα στον αλγόριθμο –γνωστό ως **Ευκλείδειο Αλγόριθμο**– που υπολογίζει το μέγιστο κοινό διαιρέτη δύο πολυωνύμων (και συνεπώς εξασφαλίζει και την υπαρξή του).

Πρόταση 5.3.4. *Έστω $a(x)$ και $b(x)$ μη μηδενικά πολυώνυμα. Αν $\upsilon(x)$ είναι το υπόλοιπο της διαίρεσης του $b(x)$ δια του $a(x)$, τότε*

$$\mu\kappa\delta(b(x), a(x)) = \mu\kappa\delta\ (\upsilon(x), a(x)).$$

Απόδειξη. Από την ταυτότητα της διαίρεσης έχουμε ότι υπάρχει $\pi(x) \in \mathbb{F}[x]$ τέτοιο ώστε

$$b(x) = \pi(x)a(x) + \upsilon(x).$$

Έστω $d_1(x) = \mu\kappa\delta(b(x), a(x))$ και $d_2(x) = \mu\kappa\delta\ (\upsilon(x), a(x))$. Τότε προφανώς το $d_1(x)$ είναι ένας κοινός διαιρέτης των $\upsilon(x) = b(x) - \pi(x)a(x)$ και $a(x)$, άρα $d_1(x)|d_2(x)$. Επίσης το πολυώνυμο $d_2(x)$ είναι ένας κοινός διαιρέτης των $a(x)$ και $b(x) = \pi(x)a(x) + \upsilon(x)$, άρα $d_2(x)|d_1(x)$. Όποτε, επειδή τα $d_1(x)$ και $d_2(x)$ είναι μονικά έχουμε ότι $d_1(x) = d_2(x)$. □

Για το υπόλοιπο $\upsilon(x)$ έχουμε ότι $\upsilon(x) = 0$ ή $\deg(\upsilon(x)) < \deg(a(x))$. Οπότε, εφαρμόζοντας διαδοχικά την προηγούμενη Πρόταση, σε πεπερασμένα βήματα θα φτάσουμε σε μηδενικό υπόλοιπο. Το προτελευταίο (μονικό) υπόλοιπο αυτής της διαδικασίας είναι ο ζητούμενος μκδ .

Πράγματι, έστω $b(x), a(x) \in \mathbb{F}[x]$ με το $a(x)$ μη μηδενικό, τότε από τον αλγόριθμο της διαίρεσης διαδοχικά έχουμε

$b(x) = \pi_1(x)a(x) + \upsilon_1(x), \quad \deg(\upsilon_1(x)) < \deg(a(x))$
$a(x) = \pi_2(x)\upsilon_1(x) + \upsilon_2(x), \quad \deg(\upsilon_2(x)) < \deg(\upsilon_1(x))$
$\upsilon_1(x) = \pi_3(x)\upsilon_2(x) + \upsilon_3(x), \quad \deg(\upsilon_3(x)) < \deg(\upsilon_2(x))$
$\upsilon_2(x) = \pi_4(x)\upsilon_3(x) + \upsilon_4(x), \quad \deg(\upsilon_4(x)) < \deg(\upsilon_3(x))$
....
$\upsilon_{n-2}(x) = \pi_n(x)\upsilon_{n-1}(x) + \upsilon_n(x), \quad \deg(\upsilon_n(x)) < \deg(\upsilon_{n-1}(x))$
$\upsilon_{n-1}(x) = \pi_{n+1}(x)\upsilon_n(x) + 0.$

Μετά από n βήματα, ο αριθμός των οποίων δεν ξεπερνά τον βαθμό του $a(x)$, το τελευταίο υπόλοιπο $\upsilon_{n+1}(x)$ είναι το μηδενικό πολυώνυμο, αφού
$\deg(a(x)) > \deg(\upsilon_1(x)) > \deg(\upsilon_2(x)) > \deg(\upsilon_3(x)) > \cdots$

Εφαρμόζοντας διαδοχικά την προηγούμενη Πρόταση έχουμε

$\mu\kappa\delta(b(x), a(x)) = \mu\kappa\delta(a(x), \upsilon_1(x)) = \mu\kappa\delta(\upsilon_1(x), \upsilon_2(x)) = \cdots = \mu\kappa\delta(\upsilon_n(x), 0)$. Οπότε το αντίστοιχο μονικό πολυώνυμο του $\upsilon_n(x)$ είναι ο ζητούμενος μέγιστος κοινός διαιρέτης.

Για τον υπολογισμό των πολυωνύμων συντελεστών $\alpha(x)$ και $\beta(x)$ στην έκφραση $\mu\kappa\delta\ (a(x), b(x)) = \alpha(x) \cdot a(x) + \beta(x) \cdot b(x)$. Εργαζόμαστε ως εξής. Ξεκινώντας από την προτελευταία σχέση έχουμε

$\upsilon_n(x) = \upsilon_{n-2}(x) - \pi_n(x)\upsilon_{n-1}(x)$.

Αλλά $\upsilon_{n-1}(x) = \upsilon_{n-3}(x) - \pi_{n-1}(x)\upsilon_{n-2}(x)$ και $\upsilon_{n-2}(x) = \upsilon_{n-4}(x) - \pi_{n-2}(x)\upsilon_{n-3}(x)$, οπότε αντικαθιστώντας στην προηγούμενη σχέση έχουμε μια παράσταση της μορφής

$\upsilon_n(x) = \beta_{n-3}(x)\upsilon_{n-4}(x) + \alpha_{n-2}(x)\upsilon_{n-3}(x)$. Συνεχίζοντας με την ίδια διαδικασία καταλήγουμε σε μια παράσταση της μορφής

$\upsilon_n(x) = \beta_2(x)\upsilon_1(x) + \alpha_3(x)\upsilon_2(x)$ και τελικά $\upsilon_n(x) = \beta_1(x)b(x) + \alpha_2(x)a(x)$.

Έστω r ο μεγιστοβάθμιος συντελεστής του $\upsilon_n(x)$, τότε προφανώς τα ζητούμενα πολυώνυμα συντελεστές είναι $\alpha(x) = r^{-1}\alpha_2(x)$ και $\beta(x) = r^{-1}\beta_1(x)$.

Παράδειγμα 5.3.5. Έστω $a(x), b(x) \in \mathbb{R}[x]$ όπου

$$a(x) = x^4 + 2x^3 + 2x - 1 \text{ και } b(x) = x^5 + +x^4 + x^3 + 2x^2 + 1.$$

Θα υπολογίσουμε τον $\mu\kappa\delta(a(x), b(x))$, χρησιμοποιώντας τον Ευκλείδειο αλγόριθμο, και θα προσδιορίσουμε πολυώνυμα $f(x)$ και $g(x)$ τέτοια ώστε $\mu\kappa\delta(a(x), b(x)) = a(x)f(x) + b(x)g(x)$.
Με διαδοχικές Ευκλείδειες διαιρέσεις βρίσκουμε τα εξής

$$\begin{aligned} b(x) &= (x-1)a(x) + 3x^3 + 3x \\ a(x) &= \frac{1}{3}(x+2)(3x^3+3x) - x^2 - 1 \\ -3x^3 + 3x &= (-3)(-x^2-1) + 0. \end{aligned}$$

Το τελευταίο μη μηδενικό υπόλοιπο είναι το $-x^2 - 1$. Το αντίστοιχο μονικό πολυώνυμο αυτού είναι ο ζητούμενους μκδ. Άρα

$$\mu\kappa\delta(a(x), b(x)) = x^2 + 1.$$

Για να προσδιορίσουμε πολυώνυμα $f(x)$ και $g(x)$, ώστε $\mu\kappa\delta(f(x), g(x)) = a(x)f(x) + b(x)g(x)$, γράφουμε την προτελευταία ισότητα ως

$$x^2 + 1 = -a(x) + \frac{1}{3}(x+2)(3x^2+3x)$$

και αντικαθιστούμε το $3x^2 + 3x$ από την πρώτη,

$$x^2 + 1 = -a(x) + \frac{1}{3}(x+2)(b(x) - (x-1)a(x))$$

Άρα

$$x^2 + 1 = (-1 - \frac{1}{3}(x+2)(x-1))a(x) + \frac{1}{3}(x+2)b(x).$$

και μπορούμε να θέσουμε $f(x) = -1 - \frac{1}{3}(x+2)(x-1)$ και $g(x) = \frac{1}{3}(x+2) + 2$.

Παρατήρηση. Μπορούμε να ορίσουμε τον μέγιστο κοινό διαιρέτη περισσοτέρων, από δύο, πολυωνύμων.

Έστω $a_i(x) \in \mathbb{F}[x]$, $i = 1, 2, \ldots, n$ όχι όλα μηδενικά πολυώνυμα. Ένα πολυώνυμο $d(x) \in \mathbb{F}[x]$ θα λέγεται ***μέγιστος κοινός διαιρέτης*** των $a_i(x)$, $i = 1, 2, \ldots, n$ αν:

(i) $d(x)|a_i(x)$, $i = 1, 2, \ldots, n$. Δηλαδή το πολυώνυμο $d(x)$ είναι κοινός διαιρέτης των $a_i(x)$.

(ii) Το $d(x)$ είναι μονικό πολυώνυμο.

(iii) Αν $\delta(x) \in \mathbb{F}[x]$ με $\delta(x)|a_i(x)$, $i = 1, 2, \ldots, n$, τότε $\delta(x)|d(x)$. Δηλαδή κάθε κοινός διαιρέτης των $a_i(x)$ είναι διαιρέτης του $d(x)$.

Αποδεικνύεται ότι ο μέγιστος κοινός διαιρέτης των πολυωνύμων $a_i(x) \in \mathbb{F}[x]$, $i = 1, 2, \ldots, n$, εκ των οποίων τουλάχιστον το ένα είναι μη μηδενικό, υπάρχει και είναι μοναδικός. Θα συμβολίζεται δε $d(x)\mu\kappa\delta(a_1(x), a_2(x), \ldots, a_n(x))$ ή απλά $d(x) = (a_1(x), a_2(x), \ldots, a_n(x))$.

Η ύπαρξη, η μοναδικότητα και ο υπολογισμός του μέγιστου κοινού διαιρέτη περισσοτέρων των δύο πολυωνύμων βασίζεται στην εξής απλή παρατήρηση.
Έστω $a(x), b(x), c(x) \in \mathbb{F}[x]$, μη μηδενικά πολυώνυμα, τότε υπάρχει ο μέγιστος κοινός διαιρέτης $d(x)$ των $a(x), b(x), c(x)$ και ισχύει

$$d(x) = \text{μκδ}(\text{μκδ}(a(x), b(x)), c(x)).$$

Πράγματι έστω $d_1(x) = \text{μκδ}(a(x), b(x))$ και $d_2(x) = \text{μκδ}(d_1(x), c(x))$.

Έστω $\delta(x)$ ένας κοινός διαιρέτης των $a(x)$, $b(x)$ και $c(x)$, άρα $\delta(x)|d_1(x)$ είναι όμως και διαιρέτης του $c(x)$, επομένως $\delta(x)|d_2(x)$.

Αλλά $d_2(x)|d_1(x)$ και το $d_1(x)$ διαιρεί το $a(x)$ και το $b(x)$, άρα το $d_2(x)$ είναι ένας κοινός διαιρέτης των $a(x)$ και $b(x)$, επίσης το $d_2(x)|c(x)$. Άρα το $d_2(x)$ είναι ένας κοινός διαιρέτης των $a(x), b(x)$ και $c(x)$, ο οποίος διαιρείται από τον (τυχαίο) κοινό διαιρέτη $\delta(x)$. Συνεπώς $d_2(x) = \text{μκδ}(a(x), b(x), c(x))$.

Από την προηγούμενη έκφραση του μκδ των πολυωνύμων $a(x), b(x), c(x)$ εύκολα προκύπτει ότι και στην περίπτωση αυτή ισχύει ένα θεώρημα ανάλογο με το Θεώρημα 5.3.2.

5.4 Απόδειξη του θεωρήματος ανάλυσης πολυωνύμων

Δύο πολυώνυμα $b(x), a(x) \in \mathbb{F}[x]$ θα λέγονται ***σχετικά πρώτα*** ή ***πρώτα μεταξύ τους*** αν μκδ $(b(x), a(x)) = 1$

Πρόταση 5.4.1. *Έστω $a(x), b(x), c(x) \in \mathbb{F}[x]$ με μκδ $(a(x), b(x)) = 1$ και $a(x)|b(x)c(x)$. Τότε $a(x)|c(x)$.*

Απόδειξη. Επειδή μκδ $(a(x), b(x)) = 1$ υπάρχουν πολυώνυμα $\alpha(x)$ και $\beta(x)$ τέτοια ώστε

$$\text{μκδ } (a(x), b(x)) = \alpha(x)a(x) + \beta(x)b(x) = 1.$$

Πολλαπλασιάζοντας και τα δύο μέλη της τελευταίας σχέσης με το πολυώνυμο $c(x)$ έχουμε $\alpha(x)a(x)c(x) + \beta(x)b(x)c(x) = c(x)$. Το πολυώνυμο $a(x)$ διαιρεί το $\beta(x)b(x)c(x)$, από την υπόθεση, προφανώς διαιρεί και το $\alpha(x)a(x)c(x)$, άρα διαιρεί και το άθροισμα $\alpha(x)a(x)c(x) + \beta(x)b(x)c(x) = c(x)$. □

Πρόταση 5.4.2. *Έστω $a(x), b(x), c(x) \in \mathbb{F}[x]$ με μκδ $(a(x), b(x)) = 1$, $a(x)|c(x)$ και $b(x)|c(x)$. Τότε $a(x)b(x)|c(x)$*

Απόδειξη. Επειδή μκδ$(a(x), b(x)) = 1$, υπάρχουν $\alpha(x), \beta(x) \in \mathbb{F}[x]$ με

$$1 = \alpha(x)a(x) + \beta(x)b(x).$$

Άρα $c(x) = \alpha(x)a(x)c(x) + \beta(x)b(x)c(x)$. Επειδή $a(x)|c(x)$ έχουμε

$$a(x)b(x)|\beta(x)b(x)c(x)$$

και επειδή $b(x)|c(x)$ έχουμε

$$a(x)b(x)|\alpha(x)a(x)c(x).$$

Άρα $a(x)b(x)|\alpha(x)a(x)c(x) + \beta(x)b(x)c(x)$, δηλ. $a(x)b(x)|c(x)$.

□

Πρόταση 5.4.3. *Έστω $p(x), p_1(x), \ldots, p_n(x) \in \mathbb{F}[x]$ ανάγωγα πολυώνυμα επί του $\mathbb{F}$. Υποθέτουμε ότι το πολυώνυμο $p(x)$ διαιρεί το γινόμενο $p_1(x) \cdots p_n(x)$, τότε υπάρχει $c \in \mathbb{F}$ έτσι ώστε $p(x) = cp_i(x)$ για κάποιο δείκτη i.*

Απόδειξη. Επειδή το πολυώνυμο $p(x)$ είναι ανάγωγο θα έχουμε

$$p(x)|p_1(x) \text{ ή μκδ } (p(x), p_1(x)) = 1 \text{ (γιατί ;).}$$

Αν $p(x)|p_1(x)$ έχει καλώς, αν μκδ $(p(x), p_1(x)) = 1$, τότε από την υπόθεση και την Πρόταση 1.2.9 έχουμε ότι το πολυώνυμο $p(x)$ διαιρεί το γινόμενο $p_2(x) \cdots p_n(x)$. Οπότε πάλι είτε $p(x)|p_2(x)$ είτε μκδ $(p(x), p_2(x)) = 1$. Συνεχίζοντας αυτή τη διαδικασία σε πεπερασμένα βήματα θα καταλήξουμε ότι υπάρχει $1 \leq i \leq n$ έτσι ώστε $p(x)|p_i(x)$. Τα πολυώνυμα όμως $p(x)$ και $p_i(x)$ είναι ανάγωγα οπότε αναγκαστικά θα υπάρχει $c \in \mathbb{F}$ έτσι ώστε $p(x) = cp_i(x)$. □

Τώρα μπορούμε να αποδείξουμε το Θεώρημα 5.2.1.

Απόδειξη του 1.2.1 Θα εφαρμόσουμε επαγωγή στο βαθμό του πολυωνύμου $a(x)$. Αν $\deg(a(x)) = 1$, τότε το πολυώνυμο $a(x)$ είναι ανάγωγο και το θεώρημα ισχύει (εδώ θεωρούμε ότι έχουμε γινόμενο με ένα ανάγωγο όρο). Υποθέτουμε ότι το θεώρημα ισχύει για όλα τα πολυώνυμα με βαθμό μικρότερου του βαθμού του $a(x)$. Αν το $a(x)$ είναι ανάγωγο, τότε πάλι το θεώρημα ισχύει. Υποθέτουμε ότι το $a(x)$ δεν είναι ανάγωγο. Άρα υπάρχουν πολυώνυμα $a_1(x)$ και $a_2(x)$ τέτοια ώστε $a(x) = a_1(x)a_2(x)$. Ο βαθμός των $a_1(x)$ και $a_2(x)$ είναι μικρότερος του βαθμού του $a(x)$, άρα το θεώρημα ισχύει για αυτά τα πολυώνυμα, όποτε και το $a(x)$ μπορεί να γραφεί στη μορφή $a(x) = cp_1(x)p_2(x)\cdots p_n(x)$ με $c \in \mathbb{F}[x]$ και τα $p_i(x)$ μονικά και ανάγωγα.

Ας υποθέσουμε τώρα ότι

$$a(x) = c_1p_1(x)p_2(x)\cdots p_n(x) = c_2q_1(x)q_2(x)\cdots q_m(x),$$

όπου $c_1, c_2 \in \mathbb{F}$ και τα πολυώνυμα $p_1(x), p_2(x), \ldots, p_n(x), q_1(x), q_2(x), \ldots, q_m(x)$ είναι μονικά και ανάγωγα επί του $\mathbb{F}$. Το πολυώνυμο $q_m(x)$ διαιρεί το γινόμενο $c_1p_1(x)p_2(x)\cdots p_n(x)$, επομένως σύμφωνα με την προηγούμενη πρόταση υπάρχει $c \in \mathbb{F}$ έτσι ώστε $q_m(x) = cp_i(x)$ για κάποιο δείκτη i. Αλλά τα $q_m(x)$ και $p_i(x)$ είναι μονικά, οπότε $q_m(x) = p_i(x)$ και αλλάζοντας, εν ανάγκη, τη σειρά των παραγόντων μπορούμε να υποθέσουμε ότι $q_m(x) = p_n(x)$. Τώρα από τη σχέση

$$c_1p_1(x)p_2(x)\cdots p_n(x) = c_2q_1(x)q_2(x)\cdots q_m(x)$$

έχουμε ότι

$$c_1p_1(x)p_2(x)\cdots p_{n-1}(x) = c_2q_1(x)q_2(x)\cdots q_{m-1}(x).$$

Ο βαθμός όμως του πολυωνύμου $c_1p_1(x)p_2(x)\cdots p_{n-1}(x)$ είναι μικρότερος από τον βαθμό του $a(x)$, επομένως από την υπόθεση της επαγωγής έχουμε ότι $c_1 = c_2$, $n-1 = m-1$ και αλλάζοντας, εν ανάγκη, την σειρά των παραγόντων $p_i(x) = q_i(x)$. □

Παρατηρήσεις.

1. Στην παράσταση ενός πολυωνύμου ως γινόμενο αναγώγων μονικών πολυωνύμων οι παράγοντες $p_i(x)$ δεν είναι κατανάγκη διακεκριμένοι, οπότε θα μπορούσαμε να γράψουμε το πολυώνυμο στη μορφή $a(x) = c_1p_1^{\nu_1}(x)p_2^{\nu_2}(x)\cdots p_m^{\nu_m}(x)$, όπου τώρα τα πολυώνυμα $p_i(x)$ είναι διακεκριμένα και τα ν_i είναι θετικοί ακέραιοι αριθμοί. Η μοναδική αυτή γραφή ονομάζεται ***ανάλυση του*** $a(x)$ ***σε γινόμενο μονικών αναγώγων πολυωνύμων*** επί του $\mathbb{F}$.

2. Όπως έχουμε επισημάνει έχει σημασία επί ποίου συνόλου συντελεστών εξετάζουμε αν ένα πολυώνυμο είναι ανάγωγο. Επομένως θα έχουμε και την αντίστοιχη ανάλυση ενός πολυωνύμου σε γινόμενο μονικών αναγώγων πολυωνύμων. Για παράδειγμα, το πολυώνυμο $x^4-x^2-2 \in \mathbb{R}[x]$ έχει την ανάλυση $x^4-x^2-2 = (x-\sqrt{2})(x+\sqrt{2})(x^2+1)$, ενώ το ίδιο πολυώνυμο, αν θεωρηθεί ως στοιχείο του $\mathbb{C}[x]$, έχει την ανάλυση $x^4-x^2-2 = (x+\sqrt{2})(x-\sqrt{2})(x-i)(x+i)$.

3. Όπως βλέπουμε, η προηγούμενη απόδειξη δεν μας δίνει έναν τρόπο να υπολογίζουμε τους ανάγωγους παράγοντες στην ανάλυση ενός πολυωνύμου. Το πρόβλημα του προσδιορισμού των αναγώγων παραγόντων ενός πολυωνύμου είναι πολύ δύσκολο και είναι ανάλογο με το πρόβλημα του προσδιορισμού των πρώτων παραγόντων στους οποίους αναλύεται ένας ακέραιος αριθμός.

Χρησιμοποιώντας την ανάλυση ενός πολυωνύμου σε γινόμενο αναγώγων πολυωνύμων μπορούμε να δώσουμε έναν άλλο τρόπο υπολογισμού του μέγιστου κοινού διαιρέτη πολυωνύμων. Συγκεκριμένα έχουμε.

Πρόταση 5.4.4. *Έστω* $a(x), b(x) \in \mathbb{F}[x]$ *και έστω*
$a(x) = c_1 p_1^{\xi_1}(x) p_2^{\xi_2}(x) \cdots p_m^{\xi_m}(x)$ *και* $b(x) = c_2 p_1^{\nu_1}(x) p_2^{\nu_2}(x) \cdots p_m^{\nu_m}(x)$
οι αναλύσεις τους σε γινόμενο μονικών αναγώγων πολυωνύμων, όπου τα ξ_i *και* ν_i *ενδέχεται να είναι και μηδέν όταν ένας παράγοντας δεν εμφανίζεται στην αντίστοιχη ανάλυση του πολυωνύμου. Θέτουμε* $\mu_i = min(\xi_i, \nu_i)$. *Τότε ισχύει* $\mu\kappa\delta\left(a(x), b(x)\right) = p_1^{\mu_1}(x) p_2^{\mu_2}(x) \cdots p_m^{\mu_m}(x)$.

Απόδειξη. Η απόδειξη είναι απλή και αφήνεται ως άσκηση. □

5.5 Ρίζες πολυωνύμων

Έστω ένα πολυώνυμο $a(x) \in \mathbb{F}[x]$. Έχουμε ακούσει για *ρίζες* της (πολυωνυμικής) εξίσωσης $a(x) = 0$ και για το πρόβλημα κατά πόσο υπάρχουν ρίζες και πώς υπολογίζονται. Στην παράγραφο αυτή θα ασχοληθούμε με το πρόβλημα αυτό επικαλούμενοι το *Θεμελιώδες Θεώρημα της Άλγεβρας*.

Έστω ένα πολυώνυμο

$$a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$$

και $c \in \mathbb{F}$, το στοιχείο

$$a_n c^n + a_{n-1}c^{n-1} + \cdots + a_1 c + a_0$$

του συνόλου $\mathbb{F}$ θα το συμβολίζουμε με $a(c)$ και θα το ονομάζουμε ***τιμή*** του πολυωνύμου στη θέση c. Όπως βλέπουμε για να υπολογίσουμε την τιμή ένος πολυωνύμου στη θέση c δεν έχουμε παρά να " *αντικαταστήσουμε*" τη μεταβλητή x με το στοιχείο c και απλώς να κάνουμε τις πράξεις.

Για παράδειγμα η τιμή του πολυωνύμου $3x^3 - 2x^2 + 3x - 2$ στη θέση $1/2$ είναι ίση με $3(1/2)^3 - 2(1/2)^2 + 31/2 - 2 = 31/8 - 21/4 + 31/2 - 2 = -5/8$.

Έστω $a(x), b(x) \in \mathbb{F}[x]$ και $ac \in \mathbb{F}$. Τότε $a(c) + b(c) = (a + b)(c)$ και $a(c) \cdot b(c) = (a \cdot b)(c)$. Δηλαδή η αντικατάσταση της μεταβλητής για την εύρεση της τιμής ενός πολυωνύμου είναι *συμβιβαστή* με την πρόσθεση και τον πολλαπλασιασμό πολυωνύμων.

Ένα στοιχείο $\xi \in \mathbb{F}$ θα λέγεται ***ρίζα*** του πολυωνύμου $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$ αν $a(\xi) = 0$, δηλαδή η τιμή του πολυωνύμου στη θέση ξ είναι το μηδέν.

Για παράδειγμα το $2 \in \mathbb{R}$ είναι ρίζα του πολυωνύμου $x^2 - x - 2 \in \mathbb{R}[x]$, αφού $2^2 - 2 - 2 = 0$. Αλλά για το πολυώνυμο $a(x) = x^2 + 2 \in \mathbb{R}[x]$ δεν υπάρχει κανένα $\xi \in \mathbb{R}$ τέτοιο ώστε $a(\xi) = 0$. Γενικά αν δεν υπάρχει $\xi \in \mathbb{F}$ έτσι ώστε $a(\xi) = 0$, τότε λέμε ότι το $a(x)$ δεν έχει ρίζα στο $\mathbb{F}$.

Πρόταση 5.5.1. *Έστω $a(x) \in \mathbb{F}[x]$. Ένα στοιχείο $c \in \mathbb{F}$ είναι ρίζα του $a(x)$ αν και μόνο αν το $x - c$ διαιρεί το $a(x)$.*

Απόδειξη. Από την Ευκλείδεια διαίρεση υπάρχουν $\pi(x), \upsilon(x) \in \mathbb{F}[x]$ τέτοια ώστε

$$a(x) = \pi(x)(x - c) + \upsilon(x)$$

με το $\upsilon(x)$ σταθερό πολυώνυμο, αφού το $x - c$ είναι πρωτοβάθμιο. Υποθέτουμε ότι το c είναι ρίζα του $a(x)$. Αντικαθιστώντας στην προηγούμενη σχέση το x με το c έχουμε $a(c) = \pi(c)(c - c) + \upsilon(x)$. Δηλαδή $\upsilon(x) = 0$. Το αντίστροφο είναι προφανές. □

Στην προηγούμενη πρόταση αποδείξαμε ότι το $a \in \mathbb{F}$ είναι ρίζα του πολυωνύμου $a(x)$ αν και μόνο αν το $x - c$ διαιρεί το $a(x)$. Ισχύει κάτι ελαφρώς γενικότερο.

Πόρισμα 5.5.2. *Το υπόλοιπο της διαίρεσης του πολυωνύμου $a(x)$ με το $x - c$ ισούται με $a(c)$, την τιμή του πολυωνύμου στη θέση c.*

Έστω $a(x) \in \mathbb{F}[x]$ και $a(x) = cp_1^{\nu_1}(x)p_2^{\nu_2}(x)\cdots p_m^{\nu_m}(x)$ η ανάλυσή του σε γινόμενο αναγώγων μονικών πολυωνύμων. Αν $a \in \mathbb{F}$, τότε προφανώς το $x-a$ διαιρεί το $a(x)$ αν και μόνο αν το $x-a$ διαιρεί ακριβώς έναν από τους ανάγωγους παράγοντες $p_i(x)$ (γιατί ;). Δηλαδή αν και μόνο αν $p_i(x) = x-a$ για κάποιο i. Επομένως υπάρχουν τόσες διαφορετικές ρίζες $\xi_j \in \mathbb{F}$ του πολυωνύμου $a(x)$ όσοι και οι διαφορετικοί παράγοντες της μορφής $x-\xi_j$ στην ανάλυσή του σε γινόμενο αναγώγων μονικών πολυωνύμων.

Ο εκθέτης ν_j ενός παράγοντα της μορφής $x-\xi_j$ στην ανάλυση του πολυωνύμου ονομάζεται ***πολλαπλότητα*** της ρίζας ξ_j .

Από την προηγούμενη συζήτηση έπεται η επομένη πρόταση.

Πρόταση 5.5.3. *Έστω $a(x) \in \mathbb{F}[x]$ ένα μη μηδενικό πολυώνυμο. Το $a(x)$ έχει το πολύ $\deg(a(x))$ το πλήθος ρίζες στο $\mathbb{F}$ όπου κάθε ρίζα προσμετράται τόσες φορές όσες και η πολλαπλότητά της.*

Απόδειξη. 'μεση από τα προηγούμενα.

□

Εδώ θα θέλαμε να επισημάνουμε ότι ένα ανάγωγο πολυώνυμο $a(x) \in \mathbb{F}[x]$ με βαθμό μεγαλύτερο του 1, προφανώς, δεν έχει ρίζα στο $\mathbb{F}$. Δεν αληθεύει όμως ότι κάθε πολυώνυμο στο $\mathbb{F}[x]$, που δεν έχει ρίζα στο $\mathbb{F}$, είναι ανάγωγο. Για παράδειγμα, το πολυώνυμο

$$(x^2+1)(x^2+2) \in \mathbb{R}[x]$$

δεν είναι ανάγωγο επί του $\mathbb{R}$ και δεν έχει ρίζα στο $\mathbb{R}$. Στην περίπτωση όμως που το πολυώνυμο είναι βαθμού 2 ή 3 έχουμε την πρόταση.

Πρόταση 5.5.4. *Έστω $a(x) \in \mathbb{F}[x]$ με βαθμό 2 ή 3. Το $a(x)$ έχει ρίζα στο $\mathbb{F}$ αν και μόνο αν δεν είναι ανάγωγο επί του $\mathbb{F}$.*

Απόδειξη. Υποθέτουμε ότι το $a(x)$ δεν είναι ανάγωγο επί του $\mathbb{F}$. Επομένως υπάρχουν μη σταθερά πολυώνυμα $a_1(x), a_2(x) \in \mathbb{F}[x]$ τέτοια ώστε $a(x) = a_1(x)a_2(x)$ και με $\deg(a_1(x)), \deg(a_2(x)) \leq \deg(a(x))$. Επειδή όμως ο βαθμός του $a(x)$ είναι 2 ή 3, έπεται ότι ο βαθμός ένός από τα $a_1(x)$ και $a_2(x)$ αναγκαστικά θα είναι ίσος με 1. Δηλαδή ένα από τα $a_1(x), a_2(x)$ θα είναι της μορφής $ax+b$ με $a, b \in \mathbb{F}$ και $a \neq 0$, οπότε το στοιχείο $-a^{-1}b \in \mathbb{F}$ είναι ρίζα του $a(x)$. □

Έχουμε δει, για παράδειγμα, ότι το πολυώνυμο x^2+2 είναι ανάγωγο επί του $\mathbb{R}$ (και άρα δεν έχει ρίζες στο $\mathbb{R}$). Αν όμως θεωρήσουμε ότι το πολυώνυμο αυτό έχει συντελεστές από το $\mathbb{C}$, τότε βλέπουμε ότι το πολυώνυμο αυτό αναλύεται στο γινόμενο $x^2+2 = (x+\sqrt{2}i)(x-\sqrt{2}i)$. Δηλαδή έχει ως ρίζες τους μιγαδικούς αριθμούς $\xi_1 = \sqrt{2}i$ και $\xi_2 = -\sqrt{2}i$. Στα επόμενα θα ασχοληθούμε για το πότε ένα πολυώνυμο με πραγματικούς συντελεστές είναι ανάγωγο επί του $\mathbb{R}$ και επί του $\mathbb{C}$.

Καταρχάς υπενθυμίζουμε ότι αν $z = a+bi$ είναι ένας μιγαδικός αριθμός, τότε ο συζυγής του είναι ο μιγαδικός αριθμός $\bar{z} = a-bi$. Μάλιστα ισχύουν οι εξής σχέσεις για κάθε

$z, z_1, z_2 \in \mathbb{C}$

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2},$$

$$\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2},$$

$$z\bar{z} \in \mathbb{R}.$$

Για τα επόμενα είναι αναγκαίο να αναφέρουμε το Θεμελιώδες Θεώρημα της Άλγεβρας, το οποίο παραθέτουμε χωρίς απόδειξη [2]

Θεώρημα 5.5.5 (Θεμελιώδες Θεώρημα της Άλγεβρας)**.** *Κάθε μη σταθερό πολυώνυμο με μιγαδικούς συντελεστές έχει μιγαδική ρίζα.*

Ως πόρισμα προκύπτει ότι κάθε πολυώνυμο με μιγαδικοιύς συντελεστές παραγοντοποιείται σε γινόμενο πρωτοβάθμιων παραγόντων.

Πρόταση 5.5.6. *Για κάθε μη σταθερό πολυώνυμο $a(x)$ με μιγαδικούς συντελεστές βαθμού n υπάρχουν μιγαδικοί αριθμοι $c, z_1, z_2, \ldots, z_n$ (όχι κατάνάγκη διακεκριμένοι) έτσι ώστε*

$$a(x) = c(x - z_1)\cdots(x - z_n).$$

Απόδειξη. Με επαγωγή στο βαθμό του πολυωνύμου. □

Ισοδύναμα θα μπορούσαμε να διατυπώσουμε τον προηγούμενη Πρόταση ως εξής "*Τα μόνα ανάγωγα πολυώνυμα επί του $\mathbb{C}$ είναι τα πολυώνυμα βαθμού ένα* "

Πρόταση 5.5.7. *Έστω $a(x) \in \mathbb{R}[x]$ και z μία μιγαδική ρίζα του. Τότε ο $\bar{z}$ είναι ρίζα του $a(x)$*

Απόδειξη. Επειδή ο μιγαδικός αριθμός z είναι ρίζα του πολυωνύμου έχουμε $\overline{a(z)} = a_n z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 = 0$ επομένως και ο συζυγής μιγαδικός αριθμός $\overline{a(z)}$ θα ισούται με μηδέν. Δηλαδή

$$\overline{a_n z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0} = \overline{a_n z^n} + \overline{a_{n-1}z^{n-1}} + \cdots + \overline{a_1 z} + \overline{a_0} = 0.$$

Επομένως

$$a_n \bar{z}^n + a_{n-1}\bar{z}^{n-1} + \cdots + a_1\bar{z} + a_0 = a(\bar{z}) = 0.$$

□

[2] Το θεώρημα αυτό απεδείχθη για πρώτη φορά το 1799 από τον Gauss στη διδακτορική του διατριβή. Παρέμεινε δε στην Ιστορία με την ονομασία αυτή καθότι, για την εποχή εκείνη, ένα κύριο μέλημα των Μαθηματικών ήταν η επίλυση πολυωνυμικών εξισώσεων της μορφής $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$ με πραγματικούς (ή μιγαδικούς) συντελεστές. Από τότε έχουν δοθεί πολλές αποδείξεις. Εδώ δεν δίνουμε απόδειξη, διότι όλες οι γνωστές αποδείξεις χρησιμοποιούν μέσα που υπερβαίνουν τους σκοπούς αυτών των σημειώσεων. Αποδείξεις μπορείτε να δείτε στα μαθήματα Μιγαδική Ανάλυση και Θεωρία Galois.
Ένα βιβλίο στο οποίο, μαζί με χρήσιμες πληροφορίες, παρουσιάζονται έξι αποδείξεις αυτού του Θεωρήματος, είναι το βιβλίο των B. Fine και G. Rosenberger, "Το Θεμελιώδες Θεώρημα της Άλγεβρας", Springer-Verlag 1997.

Από την προηγούμενη Πρόταση έπεται το εξής αποτέλεσμα.

Θεώρημα 5.5.8. *1. Κάθε πολυώνυμο $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$ περιττού βαθμού έχει μία πραγματική ρίζα.*
2. Τα ανάγωγα πολυώνυμα επί του $\mathbb{R}$ είναι τα πρωτοβάθμια και τα πολυώνυμα της μορφής $ax^2 + bx + c$, όπου $b^2 - 4ac < 0$.

Απόδειξη. 1. Ένα πρωτοβάθμιο πολυώνυμο είναι της μορφής $ax + b$ με $a \neq 0$, οπότε ο πραγματικός αριθμός $-b/a$ είναι μια ρίζα του πολυωνύμου. Υποθέτουμε ότι το αποτέλεσμα ισχύει για όλα τα πολυώνυμα περιττού βαθμού μικροτέρου ή ίσου με $2k + 1$. Έστω ένα πολυώνυμο $a(x)$ με βαθμό $2(k + 1) + 1$. Από τα προηγούμενα έπεται ότι αν το πολυώνυμο έχει μια μιγαδική ρίζα, έστω z, τότε και ο συζυγής $\bar{z}$ είναι ρίζα του πολυωνύμου. Επομένως τα μονώνυμα $x - z$ και $x - \bar{z}$ διαιρούν το $a(x)$. Άρα και το γινόμενο $(x - z)(x - \bar{z})$ διαιρεί το $a(x)$ στο $\mathbb{C}$ (βλέπε Πρόταση 15.2.10). Αλλά το πολυώνυμο $(x-z)(x-\bar{z})$ έχει πραγματικούς συντελεστές (γιατί ;), επομένως και το πηλίκο της διαίρεσης, έστω $\pi(x)$, είναι ένα πολυώνυμο με πραγματικούς συντελεστές (βλέπε Άσκηση 12) και με βαθμό ίσο με $2k + 1$. Από την υπόθεση το $\pi(x)$ έχει τουλάχιστον μια πραγματική ρίζα, άρα και το $a(x)$ έχει τουλάχιστον μια πραγματική ρίζα.

2. Προφανώς τα πρωτοβάθμια πολυώνυμα και τα πολυώνυμα της μορφής $ax^2 + bx + c$, όπου $b^2 - 4ac < 0$ είναι ανάγωγα επί του $\mathbb{R}$. Κάθε άλλο πολυώνυμο δευτέρου βαθμού δεν είναι ανάγωγο. Έστω $a(x)$ ένα πολυώνυμο με $\deg(a(x)) \geq 3$. Όπως και στο 1. έχουμε ότι το $a(x)$, αν δεν έχει μια πραγματική ρίζα, θα περιέχει έναν παράγοντα της μορφής $(x - z)(x - \bar{z})$. Άρα δεν είναι ανάγωγο. □

5.6 Ασκήσεις

1. Έστω $a(x) \in \mathbb{F}[x]$. Δείξτε ότι υπάρχει $b(x) \in \mathbb{F}[x]$ τέτοιο ώστε $a(x)b(x) = 1$ αν και μόνο αν το $a(x)$ (οπότε και το $b(x)$) είναι σταθερό πολυώνυμο.

2. Έστω $a(x), b(x) \in \mathbb{F}[x]$. Δείξτε ότι $a(x)b(x) = 0$ αν και μόνο αν τουλάχιστον ένα από τα $a(x)$ και $b(x)$ είναι το μηδενικό πολυώνυμο.

3. Δειξτε ότι δεν υπάρχει πολυώνυμο $a(x) \in \mathbb{R}[x]$ τέτοιο ώστε $(a(x))^{11} = (x+1)^{22} + (x-1)^{2004}$.

4. Βρείτε όλα τα $f(x) \in \mathbb{C}[x]$ τέτοια ώστε $f(x+2) - 2f(x+1) = f(x)$.

5. Υποθέτουμε ότι το πολυώνυμο $a(x) \in \mathbb{F}[x]$ διαιρεί το πολυώνυμο $b(x) \in \mathbb{F}[x]$. Δείξτε ότι για κάθε $0 \neq c \in \mathbb{F}$ το πολυώνυμο $ca(x)$ διαιρεί το $b(x)$.

6. Βρείτε όλα τα $f(x) \in \mathbb{C}[x]$ με $f(x) = f(x-1)$.

7. Βρείτε όλα τα μονικά $f(x) \in \mathbb{C}[x]$ τέτοια ώστε $xf(x-1) = (x-2020)f(x)$.

8. Δείξτε ότι υπάρχουν άπειρα το πλήθος ανάγωγα πολυώνυμα στο $\mathbb{Q}[x]$.

9. Έστω $a(x), b(x) \in \mathbb{F}[x]$. Δείξτε ότι για κάθε πολυώνυμο $\mu(x) \in \mathbb{F}[x]$ ισχύει

$$\text{μκδ}(b(x), a(x)) = \text{μκδ } (b(x) + \mu(x)a(x), a(x)).$$

10. Έστω $a(x), p(x) \in \mathbb{F}[x]$ με το $p(x)$ ανάγωγο επί του $\mathbb{F}$. Δείξτε ότι είτε $p(x)|a(x)$ είτε μκδ $(a(x), p(x)) = 1$. Στην περίπτωση που $p(x)|a(x)$ ποίος είναι ο μκδ $(a(x), p(x))$;

11. Βρείτε το μκδ$(x^2+1, x^{2010}+1)$ και το μκδ$(x^2+1, x^{2010}-1)$.

12. Έστω $a(x), b(x) \in \mathbb{R}[x]$ με $a(x) \neq 0$. Από την ταυτότητα της διαίρεσης έχουμε ότι υπάρχουν μοναδικά $\pi_1(x), \upsilon_1(x) \in \mathbb{R}[x]$ τέτοια ώστε $b(x) = a(x) \cdot \pi_1(x) + \upsilon_1(x)$ και ή $\upsilon_1(x) = 0$ ή $\deg(\upsilon_1(x)) < \deg(a(x))$.

    Θεωρούμε τώρα ότι $a(x), b(x) \in \mathbb{C}[x]$ με $a(x) \neq 0$, τότε πάλι από την ταυτότητα της διαίρεσης έχουμε ότι υπάρχουν μοναδικά

    $\pi_2(x), \upsilon_2(x) \in \mathbb{C}[x]$ τέτοια ώστε $b(x) = a(x) \cdot \pi_2(x) + \upsilon_2(x)$ και ή $\upsilon_2(x) = 0$ ή $\deg(\upsilon_2(x)) < \deg(a(x))$.

    Δείξτε ότι $\pi_1(x) = \pi_2(x)$ και $\upsilon_1(x) = \upsilon_2(x)$.

13. Έστω $a(x) = x^5 - x^4 - x^2 + x, b(x) = x^2 + x - 6 \in \mathbb{R}[x]$. Να βρεθούν πολυώνυμα $\alpha(x)$ και $\beta(x)$ τέτοια ώστε μκδ $(a(x), b(x)) = \alpha(x)a(x) + \beta(x)b(x)$. Είναι τα πολυώνυμα αυτά μοναδικά;

14. Να προσδιορισθούν όλα τα μονικά πολυώνυμα $a(x) \in \mathbb{R}[x]$ βαθμού το πολύ 4 τέτοια ώστε μκδ $(a(x), x^2+1) \neq 1$ και μκδ $(a(x), x^2 - 3x + 2)$ να είναι πολυώνυμο βαθμού 1.

15. Έστω $a(x), b(x) \in \mathbb{F}[x]$ και $d(x) = \text{μκδ}(a(x), b(x))$. Δείξτε ότι τα πολυώνυμα $\frac{a(x)}{d(x)}$ και $\frac{b(x)}{d(x)}$ είναι σχετικά πρώτα.

16. Βρείτε όλα τα μονικά ανάγωγα $p(x), q(x) \in \mathbb{Q}[x]$ με $(x^2-1)p(x) + (x+2)q(x) = p(x)q(x)$.

17. Έστω $a(x), b(x), \alpha(x) \in \mathbb{F}[x]$ με το $\alpha(x)$ μονικό πολυώνυμο.

    Δείξτε ότι μκδ $(\alpha(x)a(x), \alpha(x)b(x)) = \alpha(x)$ μκδ $(a(x), b(x))$.

    μκδ($a(x)$,μκδ($b(x)\sigma(x)$)).

18. Έστω δύο πολυώνυμα $a(x)$ και $b(x)$ και έστω

    $a(x) = c_1 p_1^{\xi_1}(x) p_2^{\xi_2}(x) \cdots p_m^{\xi_m}(x)$ και $b(x) = c_2 p_1^{\nu_1}(x) p_2^{\nu_2}(x) \cdots p_m^{\nu_m}(x)$

    οι αναλύσεις τους σε γινόμενο μονικών αναγώγων πολυωνύμων, όπου τα ξ_i και ν_i ενδέχεται να είναι και μηδέν όταν ένας παράγοντας δεν εμφανίζεται στην αντίστοιχη ανάλυση του πολυωνύμου. Θέτουμε $\mu_i = min(\xi_i, \nu_i)$. Δείξτε ότι μκδ $(a(x), b(x)) = p_1^{\mu_1}(x) p_2^{\mu_2}(x) \cdots p_m^{\mu_m}(x)$.

19. Έστω $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$.

    i) Δείξτε ότι η τιμή του $a(x)$ στη θέση 0 ισούται με a_0. Οπότε ένα πολυώνυμο έχει ρίζα το μηδέν αν και μόνο αν έχει μηδενικό σταθερό όρο.

    ii) Δείξτε ότι η τιμή του $a(x)$ στη θέση 1 ισούται με $\sum_{i=0}^{n} a_i$. Οπότε ένα πολυώνυμο έχει ρίζα το ένα αν και μόνο αν το άθροισμα των συντελεστών του ισούται με μηδέν.

20. Να βρεθούν οι ρίζες του πολυωνύμου $2x^3 - 3x^2 + 6x - 5$.

21. Δίνεται ότι μια ρίζα του $f(x) = x^4 - x^3 + 4x^2 + 3x + 5 \in \mathbb{C}[x]$ είναι το $1 + 2i$. Βρείτε όλες τις ρίζες του $f(x)$ στο $\mathbb{C}$.

    Έστω $f_{4,r}$ ο περιορισμός της προηγούμενης απεικόνισης στο διανυσματικό χώρο $\mathbb{F}_4[x]$ των πολυωνύμων με βαθμό το πολύ τέσσερα. Να βρείτε μια βάση του πυρήνα της $f_{4,r}$.

22. Εφαρμόζοντας επαγωγή στο βαθμό ενός πολυωνύμου $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$, δώστε μια άλλη απόδειξη της Πρότασης 1.3.3.

23. Έστω $a(x), b(x) \in \mathbb{F}[x]$ με βαθμούς n και k αντίστοιχα και $m = \max(n, k)$. Δείξτε ότι $a(x) = b(x)$ αν και μόνο αν υπάρχουν $m+1$ το πλήθος στοιχεία $a \in \mathbb{F}[x]$ τέτοια ώστε $a(a) = b(a)$

24. Έστω $a(x) = x^3 + x^2 - 2x - 1 \in \mathbb{R}[x]$ και ξ μια ρίζα του. Δείξτε ότι και το $\xi^2 - 2$ είναι ρίζα του $a(x)$. Τι συμπεραίνετε για το είδος των ριζών του $a(x)$;

25. Έστω $a(x) \in \mathbb{F}[x]$.

    i) Αν $a \neq b$ να δείξετε ότι το υπόλοιπο της διαίρεσης του $a(x)$ με το πολυώνυμο $(x-a)\cdot(x-b)$ είναι το $\frac{a(a)-a(b)}{a-b}x + \frac{aa(b)-ba(a)}{a-b}$.

ii) Να βρείτε αντίστοιχο τύπο για το υπόλοιπο της διαίρεσης του $a(x)$ με το $(x-a)^2$.

26. Έστω $a_1, a_2, \ldots, a_n \in \mathbb{R}$. Θέτουμε $e_k = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} a_{i_1} a_{i_2} \ldots a_{i_k}$, $k = 1, 2, \ldots, n$. Για παράδειγμα, αν $n = 3$, τότε $e_1 = a_1 + a_1 + a_3$, $e_2 = a_1 a_2 + a_1 a_3 + a_2 a_3$ και $e_3 = a_1 a_2 a_3$. Δείξτε ότι αν $e_k > 0$ για κάθε $k = 1, 2, \ldots, n$, τότε $a_i > 0$ για κάθε $i = 1, 2, \ldots, n$.