ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ
ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΪΚΑ ΜΑΘΗΜΑΤΑ

Τίτλος Μαθήματος: Αλγεβρικές Δομές ΙΙ

Ενότητα: Ιδεώδη και Περιοχές κυρίων Ιδεωδών

Διδάσκων: Καθηγητής Μαρμαρίδης Νικόλαος - Θεοδόσιος

Τμήμα: Μαθηματικών

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Για το σύμβολο «$-\infty$» δεχόμαστε ότι $\forall n \in \mathbb{N} \cup \{0\}, -\infty < n$ καθώς και ότι:

$$\forall n \in \mathbb{N} \cup \{0\}, (-\infty) + n = -\infty = n + (-\infty) \text{ και } (-\infty) + (-\infty) = -\infty. \qquad (**)$$

Ονομάζουμε *επικεφαλής συντελεστή* ενός μη μηδενικού πολυωνύμου f, τον συντελεστή $f(i) = a_i$ με το μεγαλύτερο $i \in \mathbb{N} \cup \{0\}$, όπου $f(i) \neq 0_R$.
Ονομάζουμε ένα μη μηδενικό πολυώνυμο *μονοστό*, αν ο επικεφαλής του συντελεστής ισούται με 1_R.

Παραδείγματα 1.2.1. Έστω ο δακτύλιος των ακεραίων αριθμών $(\mathbb{Z}, +, \cdot)$ και $\mathbb{Z}[x]$ ο αντίστοιχος δακτύλιος των πολυωνύμων μιας μεταβλητής υπεράνω τού $\mathbb{Z}$.
Το πολυώνυμο $f_1(x) = 2 \in \mathbb{Z}[x]$ έχει $\deg f_1(x) = 0$, το $f_2(x) = 2+x^{3n} \in \mathbb{Z}[x], n \in \mathbb{N}$ έχει $\deg f_2(x) = 3n$ και το πολυώνυμο $f_3(x) = 1 + x + x^2 + \cdots + x^n, n \in \mathbb{N}$ έχει $\deg f_3(x) = n$. Ο επικεφαλής συντελεστής τού $f_1(x)$ είναι 2. Τα $f_2(x)$ και $f_3(x)$ είναι μονοστά πολυώνυμα.

Πρόταση 1.2.2. *Αν ο δακτύλιος $(R, +, \cdot)$ είναι ακέραια περιοχή, τότε και ο δακτύλιος $R[x]$ είναι ακέραια περιοχή και μάλιστα $\forall f(x), g(x) \in R[x]$ είναι* $\deg f(x)g(x) = \deg f(x) + \deg g(x)$.

Απόδειξη. Αν ένα από τα δύο πολυώνυμα είναι το μηδενικό, τότε το γινόμενό τους είναι επίσης το μηδενικό πολυώνυμο και από την παραδοχή που κάναμε, βλ. (**), σχετικά με τον βαθμό τού μηδενικού πολυνωύμου έπεται η ισότητα $\deg f(x)g(x) = \deg f(x) + \deg g(x)$.

Αν ούτε το $f(x) = a_0 + a_1x + \cdots + a_nx^n$ είναι το μηδενικό πολυώνυμο, ας πούμε ότι $\deg f(x) = n$, ούτε το $g(x) = b_0 + b_1x + \cdots + b_mx^m$ είναι το μηδενικό πολυώνυμο, ας πούμε ότι $\deg g(x) = m$, τότε ο επικεφαλής συντελεστής τού γινομένου $f(x)g(x)$ είναι ο $a_nb_m \neq 0_R$, επειδή $a_n \neq 0_R, b_m \neq 0_R$ και επειδή ο R είναι ακεραια περιοχή. Συνεπώς, $\deg f(x)g(x) = n + m = \deg f(x) + \deg g(x)$. □

Παρατηρήσεις 1.2.1. Επιπλέον αν, $(R, +, \cdot)$ είναι οποιοσδήποτε μοναδιαίος δακτύλιος,

$$\forall f(x), g(x) \in R[x], \deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}.$$

1.3 Ιδεώδη και Περιοχές κυρίων Ιδεωδών

Έστω $(R, +, \cdot)$ ένας μοναδιαίος μεταθετικός δακτύλιος και $I \subseteq R$ ένα υποσύνολό του. Υπενθυμίζουμε ότι

Ορισμός 1.3.1. Το $I \subseteq R$ είναι ένα *ιδεώδες* τού $(R, +, \cdot)$ αν, το ζεύγος $(I, +)$ είναι μια υποομάδα τού $(R, +)$ και το I είναι κλειστό ως προς τον πολλαπλασιασμό με τα στοιχεία τού R, δηλαδή $\forall a \in I$ και $r \in R$, το στοιχείο ra ανήκει στο I.

Επιπλέον υπενθυμίζουμε ότι ένα ιδεώδες I τού R ονομάζεται *πεπερασμένως παραγόμενο* αν, υπάρχει ένα πεπερασμένο υποσύνολο $A = \{a_1, a_2, \ldots, a_t\}$ τού R, ώστε κάθε στοιχείο $a \in I$ να είναι ένας R–γραμμικός συνδυασμός στοιχείων τού A, δηλαδή για κάθε $a \in I$ να υπάρχουν $r_1, r_2, \ldots, r_t \in R$ (όχι απαραιτήτως μοναδικά) με $a = \sum_{i=1}^{t} r_i a_i$. Στην περίπτωση αυτή γράφουμε $I = \langle a_1, a_2, \ldots, a_t \rangle$.

Υπενθυμίζουμε ακόμη ότι το ιδεώδες

$$\langle a_1, a_2, \ldots, a_t \rangle = \{\sum_{i=1}^{t} r_i a_i \mid a_i \in A, r_i \in R, i = 1, 2, \ldots, t\}$$

είναι το μικρότερο (ως προς τη σχέση «$\subseteq$») ιδεώδες τού R που περιέχει το A.

Ορισμός 1.3.2. Ένα ιδεώδες I τού R ονομάζεται *κύριο*, αν παράγεται από ένα μονοσύνολο τού R, δηλαδή αν υπάρχει $a \in R$ με $I = \langle a \rangle$.

Ένας δακτύλιος, τού οποίου κάθε ιδεώδες είναι κύριο ονομάζεται δακτύλιος κυρίων ιδεωδών. Ιδιαιτέρως,

Ορισμός 1.3.3. Ένας μοναδιαίος μεταθετικός δακτύλιος $(R, +, \cdot)$ ονομάζεται *περιοχή κυρίων ιδεωδών* αν, είναι ακέραια περιοχή και κάθε ιδεώδες του είναι κύριο.

Συνήθως δηλώνουμε μια περιοχή κυρίων ιδεωδών, γράφοντας τη συντόμευση Π.Κ.Ι. Ήδη γνωρίζουμε ότι

Πρόταση 1.3.1. *Ο δακτύλιος των ακεραίων αριθμών είναι Π.Κ.Ι..*

Απόδειξη. (*Περιγραφή*) Τα ιδεώδη τού $\mathbb{Z}$ συμπίπτουν ακριβώς με τις υποομάδες τού $\mathbb{Z}$. Κάθε υποομάδα τού $\mathbb{Z}$ είναι κυκλική και επομένως κάθε ιδεώδες τού $\mathbb{Z}$ είναι κύριο. □

Στη παρούσα ενότητα θα αποδείξουμε ότι ο δακτύλιος πολυωνύμων μιας μεταβλητής υπεράνω ενός σώματος είναι Π.Κ.Ι. και γι' αυτό χρειαζόμαστε τη λεγόμενη *Ευκλείδεια Διαίρεση Πολυωνύμων*, την οποία διατυπώνουμε λίγο γενικότερα στο ακολουθο:

Λήμμα 1.3.1 (Ευκλείδεια Διαίρεση Πολυωνύμων). *Έστω $(R, +, \cdot)$ ένας μοναδιαίος μεταθετικός δακτύλιος και $f(x), g(x)$ δύο πολυώνυμα τού $R[x]$, όπου ο επικεφαλής συντελεστής τού $g(x)$ είναι αντιστρέψιμο στοιχείο τού R.*
Υπάρχουν πολυώνυμα $q(x)$ (το λεγόμενο πηλίκο) και $r(x)$ (το λεγόμενο υπόλοιπο) τού $R[x]$ με

$$f(x) = q(x)g(x) + r(x), \text{ όπου } \deg r(x) < \deg g(x). \tag{*}$$

Επιπλέον αν, ο R είναι ακέραια περιοχή, τότε $q(x)$ και $r(x)$ είναι τα μοναδικά πολυώνυμα που ικανοποιούν την (*).

Στην περίπτωση που ο R δεν είναι ακέραια περιοχή τα $q(x), r(x)$ δεν είναι απαραιτήτως μοναδικά.

Παράδειγμα 1.3.1. Στον δακτύλιο $\mathbb{Z}_6[x]$ θεωρούμε τα πολυώνυμα

$$f(x) = [2]x^3 + [2]x + [2], \text{ και } g(x) = [2]x^2 + [2].$$

Παρατηρούμε ότι

$$[2]x^3 + [2]x + [2] = q_1(x)g(x) + r_1(x), q_1(x) = [3]x^2 + x, r_1(x) = 2, \deg r_1 = 0 < 2 = \deg g(x)$$

και

$$[2]x^3 + [2]x + [2] = q_1(x)g(x) + r_1(x), q_2(x) = x + [3], r_2(x) = 2, \deg r_2 = 0 < 2 = \deg g(x).$$

Θεώρημα 1.3.1. *Ο δακτύλιος πολυωνύμων $F[x]$ μιας μεταβλητής υπεράνω ενός σώματος F είναι Π.Κ.Ι..*

Απόδειξη. Σύμφωνα με την Πρόταση 1.2.2 ο δακτύλιος $F[x]$ είναι ακέραια περιοχή.

Έστω I ένα ιδεώδες τού $F[x]$. Αν $I = \{0_{F[x]}\}$, τότε $I = \langle 0_{F[x]} \rangle$. Αν $I \neq \{0_{F[x]}\}$, τότε το I περιέχει και μη μηδενικά πολυώνυμα . Μεταξύ αυτών των μη μηδενικών πολυωνύμων τού I θεωρούμε ένα $g(x) \in I$ ελαχίστου βαθμού. Θα δείξουμε ότι κάθε $f(x) \in I$ είναι πολλαπλάσιο τού $g(x)$. Πράγματι, εκτελώντας την Ευκλείδεια Διαίρεση τού $f(x)$ δια τού $g(x)$ έχουμε:

$$f(x) = q(x)g(x) + r(x), \deg r(x) < \deg g(x).$$

Παρατηρώντας ότι το πολυώνυμο $r(x) = f(x) - q(x)g(x)$ ανήκει στο I, (αφού τα $f(x)$ και $q(x)g(x)$ ανήκουν στο ιδεώδες I), συμπεραίνουμε ότι το $r(x)$ οφείλει να ισούται με το μηδενικό πολυώνυμο, επειδή στην αντίθετη περίπτωση το πολυώνυμο $g(x) \in I$ δεν είναι ένα ελαχίστου βαθμού μη μηδενικό πολυώνυμο τού I. Ώστε,

$$f(x) = q(x)g(x)$$

και συνεπώς $I = \langle g(x) \rangle$. □

Προσέξτε ότι αν ένας δακτύλιος R είναι Π.Κ.Ι., τότε δεν έπεται απαραιτήτως ότι και ο R[x] είναι Π.Κ.Ι..

Παράδειγμα 1.3.2. Ο δακτύλιος $\mathbb{Z}$ είναι Π.Κ.Ι., αλλά ο $\mathbb{Z}[x]$ δεν είναι Π.Κ.Ι..

Πράγματι, ας θεωρήσουμε το ιδεώδες που παράγεται από τα $2, x \in \mathbb{Z}[x]$.

$$\langle 2, x\rangle = \{f(x)2 + g(x)x \mid f(x), g(x) \in \mathbb{Z}[x]\} \subset \mathbb{Z}[x]. \qquad (*)$$

Μια άλλη περιγραφή τού $\langle 2, x\rangle$ είναι ότι αποτελείται από τα πολυώνυμα τού $\mathbb{Z}[x]$ που έχουν τον σταθερό τους όρο άρτιο. Ιδιαιτέρως το $\langle 2, x\rangle$ περιέχεται γνήσια εντός τού $\mathbb{Z}[x]$, αφού $1 \notin \langle 2, x\rangle$.

Υποθέτοντας ότι το ιδεώδες $\langle 2, x\rangle$ είναι κύριο, δηλαδή ότι υπάρχει $\ell(x) \in \mathbb{Z}[x]$ με $\langle \ell(x)\rangle = \langle 2, x\rangle$, θα καταλήξουμε σε άτοπο. Πράγματι, αν ήταν έτσι θα είχαμε $2 \in \langle \ell(x)\rangle$ και $x \in \langle \ell(x)\rangle$. Επομένως,

$$2 = \alpha(x)\ell(x), x = \beta(x)\ell(x), \alpha(x), \beta(x) \in \mathbb{Z}[x].$$

Στον $\mathbb{Z}[x]$ ο βαθμός τού γινομένου δύο πολυωνύμων ισούται με το άθροισμα των βαθμών τους και έτσι

$$\deg 2 = \deg(\alpha(x)\ell(x)) = \deg \alpha(x) + \deg \ell(x) \Rightarrow 0 = \deg \alpha(x) + \deg \ell(x).$$

Επομένως, τα $a(x)$ και $\ell(x)$ είναι ακέραιοι αριθμοί. Αλλά τότε το $\ell(x) = \pm 1, \pm 2$. Επειδή $\langle 2, x\rangle \subsetneq \mathbb{Z}[x]$ έπεται ότι $\ell(x) \neq \pm 1$ και συνεπώς $\ell(x) = \pm 2$. Τώρα όμως, λόγω τής (*), έπεται ότι $x = \pm 2\beta(x)$. Αυτό όμως είναι άτοπο, αφού ο συντελεστής τού x ισούται με 1, ενώ ο συντελεστής τού $\pm 2\beta(x)$ είναι σε κάθε περίπτωση άρτιος.

Τίθεται λοιπόν το ερώτημα, πώς βρίσκουμε τον γεννήτορα κάποιου ιδεώδους πολυωνυμικού δακτυλίου υπεράνω ενός σώματος; Η απάντηση βρίσκεται στην έννοια τού μέγιστου κοινού διαιρέτη.

Έστω $(R, +, \cdot)$ ένας μεταθετικός μοναδιαίος δακτύλιος και $a, b \in R$. Το στοιχείο a *διαιρεί* το στοιχείο b αν, υπάρχει $c \in R$ με $b = ac$. (Σύμβολο: $a \mid b$.)

Τα στοιχεία a, c ονομάζονται *διαιρέτες* τού b.

Τα επόμενα είναι προφανή:

(α΄) $a \mid b \Leftrightarrow b \in \langle a\rangle$.

(β΄) $\forall a \in R, a \mid 0_R$.

(γ΄) $0_R \mid a \Leftrightarrow a = 0_R$.

(δ΄) $\forall a \in R, a \mid a$.

(ε΄) $a \mid 1_R \Leftrightarrow a$ αντιστρέψιμο στοιχείο τού R.

Ορισμός 1.3.4. Έστω R μια ακέραια περιοχή και $f(x), g(x)$ δύο πολυώνυμα τού $R[x]$. Ονομάζουμε *μέγιστο κοινό διαιρέτη* των $f(x), g(x)$ ένα πολυώνυμο $d(x) \in R[x]$ με τις ακόλουθες ιδιότητες:

(α') $d(x) \mid f(x)$ και $d(x) \mid g(x)$,

(β') αν $d'(x) \in R[x]$ με $d'(x) \mid f(x)$ και $d'(x) \mid g(x)$, τότε $d'(x) \mid d(x)$,

(γ') τέλος απαιτούμε το $d(x)$ να είναι μονοστό πολυώνυμο.

Συμβολίζουμε τον μέγιστο κοινό διαιρέτη των $f(x), g(x)$ με Μ.Κ.Δ.$(f(x), g(x))$.

Παρατηρήσεις 1.3.1. Αν υπάρχει ο Μ.Κ.Δ. δύο πολυωνύμων $f(x), g(x) \in R[x]$, όπου τουλάχιστον ένα από τα δύο είναι $\neq 0_R$, τότε είναι μοναδικός. Πράγματι, ας είναι $d_1(x)$ $d_2(x)$ δύο μέγιστοι κοινοί διαιρέτες των $f(x), g(x)$. Προφανώς, $d_1(x) \neq 0_R$ και $d_2(x) \neq 0_R$. Τότε $d_1(x) \mid d_2(x)$ και $d_2(x) \mid d_1(x)$ και συνεπώς $d_2(x) = \ell(x)d_1(x)$, $d_1(x) = \lambda(x)d_2(x)$ (*), όπου $\ell(x), \lambda(x) \in R[x]$. Επομένως, $d_1(x) = \lambda(x)d_2(x)\ell(x)d_1(x)$ και αφού ο R είναι ακέραια περιοχή έπεται

$$\deg d_1 = \deg \lambda + \deg \ell + \deg d_1 \Rightarrow \deg \lambda + \deg \ell = 0 \Rightarrow \deg \lambda = \deg \ell = 0.$$

Ώστε τα $\lambda(x), \ell(x)$ είναι σταθερά μη μηδενικά πολυώνυμα τού $R[x]$, δηλαδή μη μηδενικά στοιχεία τού R. Ας πούμε $\lambda(x) = \lambda \in R, \ell(x) = \ell \in R$. Τώρα, από την (*) έπεται ότι ο επικεφαλής συντελεστής τού $d_1(x)$ (επειδή το $d_2(x)$ είναι μονοστό) ισούται με λ. Αλλά και το $d_1(x)$ είναι επίσης μονοστό και γι' αυτό $\lambda = 1$ και συνεπώς $d_1(x) = d_2(x)$.

Πρόταση 1.3.2. *Έστω ότι το F είναι ένα σώμα και $f(x), g(x)$ είναι δύο πολυώνυμα τού $F[x]$ με $g(x) \neq 0_R$. Τότε υπάρχει ο Μ.Κ.Δ.$(f(x), g(x)) = d(x)$ και μάλιστα $\langle f(x), g(x)\rangle = \langle d(x)\rangle$ από όπου έπεται ότι ο Μ.Κ.Δ.$(f(x), g(x)) = d(x)$ είναι τής μορφής $d(x) = \alpha(x)f(x) + \beta(x)g(x), \alpha(x), \beta(x) \in F[x]$.*

Απόδειξη. Το ιδεώδες $\langle f(x), g(x)\rangle$ που παράγεται από τα $f(x), g(x)$ είναι μη μηδενικό και επειδή ο $F[x]$ είναι Π.Κ.Ι., βλ. Θεώρημα 1.3.1, υπάρχει κάποιο μη μηδενικό πολυώνυμο $d(x) \in F[x]$ με $\langle d(x)\rangle = \langle f(x), g(x)\rangle$ (*). Επιπλέον, μπορούμε να δεχθούμε χωρίς περιορισμό τής γενικότητας ότι το $d(x)$ είναι μονοστό πολυώνυμο, αφού το ιδεώδες $d(x)$ ισούται με το ιδεώδες $\langle a^{-1}d(x)\rangle$, όπου a^{-1} είναι ο επικεφαλής συντελεστής τού $d(x)$. Παρατηρούμε ότι $d(x) = \alpha(x)f(x) + \beta(x)g(x)$(**), αφού λόγω τής (*), $d(x) \in \langle f(x), g(x)\rangle$.
Έχουμε $f(x) \in \langle d(x)\rangle$ και $g(x) \in \langle d(x)\rangle$ και συνεπώς $d(x) \mid f(x)$ και $d(x) \mid g(x)$. Αν $d'(x) \in F[x]$ με $d'(x) \mid f(x)$ και $d'(x) \mid g(x)$, τότε λόγω τής (**) έπεται ότι $d'(x) \mid d(x)$. Επομένως, το πολυώνυμο $d(x)$ είναι ο Μ.Κ.Δ. των $f(x), g(x)$. □

Προσδιορισμός Μ.Κ.Δ. δύο πολυωνύμων, όπου τουλάχιστον ένα δεν είναι το μηδενικό

Έστω $f(x), g(x) \in F[x]$ με $g(x) \neq 0$. Εκτελούμε τη διαίρεση τού $f(x)$ δια τού $g(x)$.

Αν το υπόλοιπο $r_1(x)$ τής διαίρεσης ισούται με μηδέν, τότε θα δείξουμε ότι ο Μ.Κ.Δ.$(f(x), g(x))= a^{-1}g(x)$, όπου a είναι ο επικεφαλής συντελεστής τού $g(x)$.

Αν το $r_1(x) \neq 0$, τότε διαιρούμε το $g(x)$ δια τού $r_1(x)$. Αν το υπόλοιπο $r_2(x)$ τής διαίρεσης ισούται με μηδέν, τότε θα δείξουμε ότι ο Μ.Κ.Δ.$(f(x), g(x))= a_1^{-1}r_1(x)$, όπου a_1 είναι ο επικεφαλής συντελεστής τού $r_1(x)$.

Αν το $r_2(x) \neq 0$, τότε διαιρούμε το $r_1(x)$ δια τού $r_2(x)$. Αν το υπόλοιπο $r_3(x)$ τής διαίρεσης ισούται με μηδέν, τότε θα δείξουμε ότι ο Μ.Κ.Δ.$(f(x), g(x))= a_2^{-1}r_2(x)$, όπου a_2 είναι ο επικεφαλής συντελεστής τού $r_2(x)$. Συνεχίζουμε αυτήν τη διαδικασία διαιρώντας κάθε μη μηδενικό υπόλοιπο με το αμέσως προηγούμενο μη μηδενικό υπόλοιπο, μέχρις ότου να προκύψει μηδενικό υπόλοιπο. Αυτό είναι βέβαιο ότι θα συμβεί, αφού $\deg g(x) > \deg r_1(x) > \deg r_2(x) > \dots$ και ούτω καθεξής. Στην αμέσως επόμενη σειρά ισοτήτων, βλ. (*), παρουσιάζουμε ακριβώς αυτήν τη διαδικασία.

$$\begin{array}{rcllcl}
f & = & q_1 g + r_1 & \deg(r_1) & < & \deg(g) \\
g & = & q_2 r_1 + r_2 & \deg(r_2) & < & \deg(r_1) \\
r_1 & = & q_3 r_2 + r_3 & \deg(r_3) & < & \deg(r_2) \\
 & \vdots & & & \vdots & \\
r_{n-2} & = & q_n r_{n-1} + r_n & \deg(r_n) & < & \deg(r_{n-1}) \\
r_{n-1} & = & q_{n+1} r_n + r_{n+1} & \deg(r_{n+1}) & < & \deg(r_n) \\
r_n & = & q_{n+2} r_{n+1} & & &
\end{array} \qquad (*)$$

Θα δείξουμε ότι το $a_{n+1}^{-1}r_{n+1}(x)$, όπου a_{n+1} είναι ο επικεφαλής συντελεστής τού $r_{n+1}(x)$ είναι ο Μ.Κ.Δ.$(f(x), g(x))$.

Αρχίζοντας από την τελευταία ισότητα, παρατηρούμε ότι $r_{n+1} \mid r_n$ και τώρα χρησιμοποιώντας την προτελευταία ισότητα έχουμε ότι $r_{n+1} \mid r_{n-1}$. Ανεβαίνοντας βήμα βήμα προς την πρώτη ισότητα, έχουμε διαδοχικά ότι

$$\begin{array}{llll}
r_{n+1} \mid r_{n-2}, & r_{n+1} \mid r_{n-3}, & \dots\dots\dots & r_{n+1} \mid r_3, \\
r_{n+1} \mid r_2, & r_{n+1} \mid r_1, & r_{n+1} \mid g, & r_{n+1} \mid f.
\end{array}$$

Συνεπώς το πολυώνυμο $a_{n+1}^{-1}r_{n+1}(x)$ διαιρεί και αυτό τα $f(x)$ και $g(x)$. Αν τώρα ένα πολυώνυμο $s(x)$ διαιρεί τα $f(x)$ και $g(x)$, τότε από την πρώτη ισότητα των σχέσεων (*), έπεται ότι $s \mid r_1$. Κατόπιν από τη δεύτερη ισότητα των (*) έπεται ότι $s \mid r_2$ και συνεχίζοντας κατ' αυτόν τον τρόπο καταλήγουμε ότι $s \mid r_{n+1}$. Συνεπώς, το $s(x)$ διαιρεί και το $a_{n+1}^{-1}r_{n+1}(x)$. Ώστε $a_{n+1}^{-1}r_{n+1}(x)$ =Μ.Κ.Δ.$(f(x), g(x))$.

Παρατήρηση 1.3.1. Προσέξτε ότι η προηγούμενη κατασκευή τού μέγιστου κοινού διαιρέτη δύο πολυωνύμων $F[x]$ εκτελείται εντός τού $F[x]$. Συνεπώς ο Μ.Κ.Δ.$(f(x), g(x))$ των $f(x), g(x) \in F[x]$ παραμένει ο ίδιος αν θεωρήσουμε τα $f(x), g(x)$ ως στοιχεία ενός «ευρύτερου» πολυωνυμικού δακτυλίου $K[x]$, όπου K σώμα με $F \subseteq K$.

Ιδιαιτέρως, αν τα $f(x), g(x)$ είναι σχετικώς πρώτα ως πολυώνυμα τού $F[x]$, δηλαδή Μ.Κ.Δ.$(f(x), g(x))= 1$, τότε Μ.Κ.Δ.$(f(x), g(x))= 1$ και ως πολυώνυμα τού $K[x]$, όπου K υπέρσωμα τού F.

1.4 Ομομορφισμοί και Πηλικοδάκτυλιοι

Ομομορφισμοί

Έστω R και S δύο μοναδιαίοι μεταθετικοί δακτύλιοι. Υπενθυμίζουμε ότι

Ορισμός 1.4.1. Ένας *ομομορφισμός δακτυλίων* από τον δακτύλιο R στον δακτύλιο S είναι μια απεικόνιση $\phi : R \to S$ που ικανοποιεί τα

(α΄) $\forall a, b \in R, \phi(a + b) = \phi(a) + \phi(b)$,

(β΄) $\forall a, b \in R, \phi(ab) = \phi(a)\phi(b)$,

(γ΄) $\phi(1_R) = 1_S$.

Ονομάζουμε *πυρήνα* τού ομομορφισμού $\phi : R \to S$, το σύνολο

$$\mathrm{Ker}\phi = \{r \in R \mid \phi(r) = 0_S\}.$$

Γνωρίζουμε ότι

Λήμμα 1.4.1. *Ο πυρήνας* $\mathrm{Ker}\phi$ *οποιουδήποτε ομομορφισμού* $\phi : R \to S$ *είναι ένα ιδεώδες τού* R.

Υπενθυμίζουμε ότι ένας ομομορφισμός $\phi : R \to S$ ονομάζεται

(α΄) *μονομορφισμός* αν, ο ομομορφισμός ϕ είναι μια «1-1» απεικόνιση,

(β΄) *επιμορφισμός* αν, ο ομομορφισμός ϕ είναι μια «επί» απεικόνιση,

(γ΄) *ισομορφισμός* αν, ο ομομορφισμός ϕ είναι μια «1-1» και «επί» απεικόνιση,

Είναι γνωστά τα εξής:

Λήμμα 1.4.2. (α΄) *Ένας ομομορφισμός δακτυλίων* $\phi : R \to S$ *είναι μονομορφισμός, αν και μόνο αν,* $\mathrm{Ker}\phi = \{0_R\}$.

(β΄) *Αν* $\phi : R \to S$ *είναι ένας ισομορφισμός,τότε και η αντίστροφη απεικόνιση* $\phi^{-1} : S \to R, s \mapsto \phi^{-1}(s) = r$ *όταν* $\phi(r) = s$, *είναι επίσης ένας ισομορφισμός δακτυλίων.*

Ανοικτά Ακαδημαϊκά Μαθήματα

Πανεπιστήμιο Ιωαννίνων

Τέλος Ενότητας

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Ιωαννίνων**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Σημειώματα

Σημείωμα Αναφοράς

Σημείωμα Αδειοδότησης