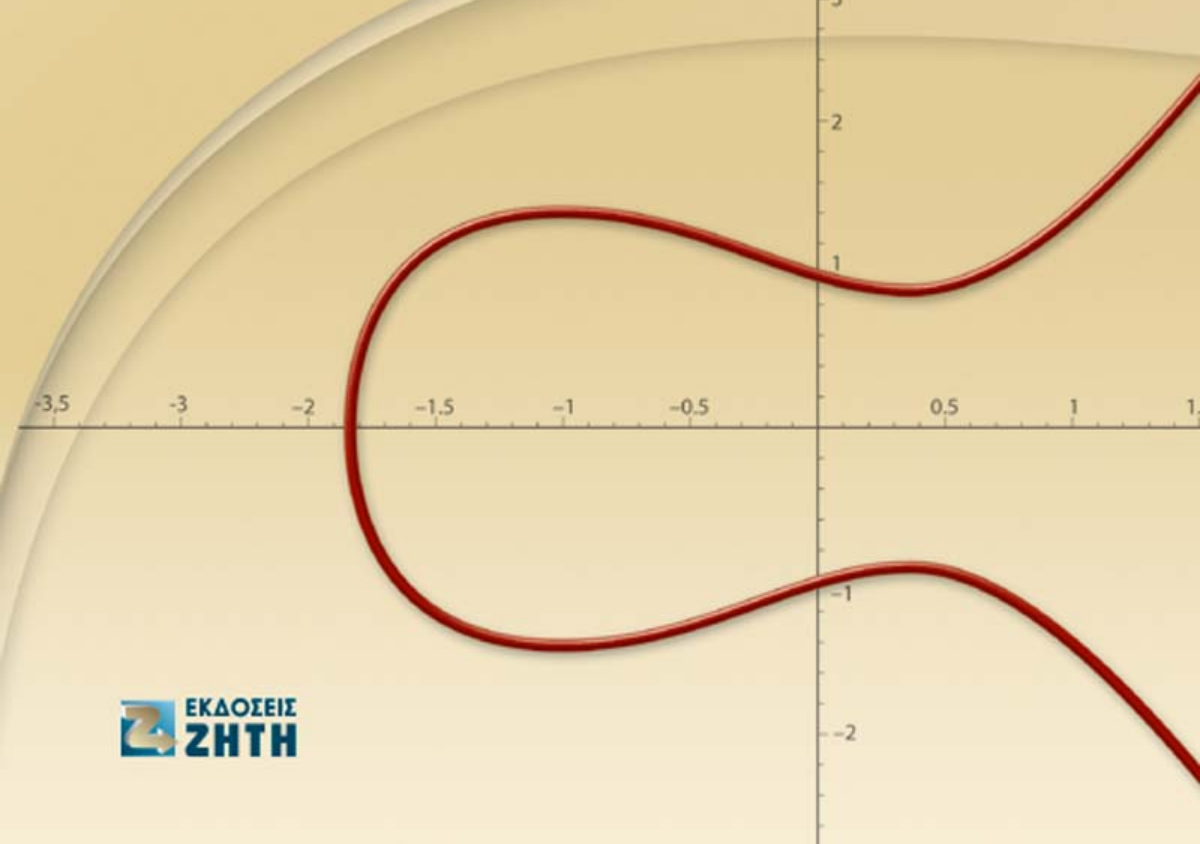
Δημήτριος Μ. Πουλάκης

ΕΙΣΑΓΩΓΗ ΣΤΗ

ΓΕΩΜΕΤΡΙΑ ΤΩΝ ΑΛΓΕΒΡΙΚΩΝ ΚΑΜΠΥΛΩΝ



ΕΚΔΟΣΕΙΣ ΖΗΤΗ

Περιεχόμενα

Πρόλογος

Η θεωρία των Αλγεβρικών Καμπυλών είναι ένας από τους παλαιότερους κλάδους των μαθηματικών. Στην αρχαιότητα απλές καμπύλες, όπως ευθείες, κύκλοι κ.τ.λ. χρησιμοποιούνται για επίλυση πρακτικών προβλημάτων, όπως κατασκευές οικοδομημάτων, μέτρηση γης κ.τ.λ.. Αργότερα, οι κωνικές τομές, ο κισσοειδής του Διοκλέους, ο κονγχοειδής του Νικομήδους και άλλες καμπύλες χρησιμοποιήθηκαν για την επίλυση κλασσικών προβλημάτων της αρχαιότητας. Από τότε μέχρι σήμερα η θεωρία των Αλγεβρικών Καμπυλών αναπτύχθηκε σε μεγάλο βαθμό, όχι μόνο για την ποικιλία των μεθόδων της και τα ανοικτά προβλήματα που περιέχει, αλλά και για τις πολλές εφαρμογές της σε κλάδους, όπως η Αστρονομία, Οπτική, Αρχιτεκτονική, Κινηματική, Μηχανική, κ.α.. Ας σημειωθεί ότι την τελευταία εικοσαετία οι Αλγεβρικές Καμπύλες έχουν σημαντική συνεισφορά στην Κρυπτογραφία, στους Κώδικες Διορθωτές Λαθών και την Ρομποτική.

Σκοπός του παρόντος βιβλίου είναι να δώσει μία απλή εισαγωγή στη Γεωμετρία των Αλγεβρικών Καμπυλών. Απαραίτητες γνώσεις για την κατανόησή του είναι η βασική Γραμμική Άλγεβρα και η βασική θεωρία των Άλγεβρικών Δομών. Μέρος του καλύπτει την ύλη του μαθήματος *Αλγεβρικές Καμπύλες* το οποίο διδάσκεται στο τέταρτο έτος του Τμήματος Μαθηματικών του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης.

Το πρώτο κεφάλαιο είναι αφιερωμένο στο πολυωνυμικό δακτύλιο $A[X_1, \ldots, X_n]$ υπεράνω ενός αντιμεταθετικού δακτυλίου A. Περιγράφεται η κατασκευή του και αποδεικνύεται ότι είναι δακτύλιος με μοναδική παραγοντοποίηση, στη περίπτωση όπου ο A έχει αυτή την ιδιότητα. Επίσης μελετάται η ευκλείδεια διαίρεση, η παραγώγιση και η απαλείφουσα δύο πολυωνύμων. Τέλος δίνονται μερικά αποτελέσματα επί των μιγαδικών πολυωνύμων μία απροσδιόριστης, μεταξύ των οποίων και μία αρκετά απλή απόδειξη του Θεμελιώδους Θεωρήματος της Άλγεβρας.

Στο δεύτερο κεφάλαιο εισάγονται οι αλγεβρικές καμπύλες του $\mathbb{C}^2$

και εξετάζονται βασικές τους ιδιότητες. Ειδικότερα, μελετάται η σχέση ισοδυναμίας τους, ο αριθμός τομής καμπύλης και ευθείας σ΄ ένα σημείο, τα ανώμαλα σημεία τους, οι εφαπτόμενες ευθείες και τέλος οι ρητές καμπύλες.

Στο τρίτο κεφάλαιο εισάγεται η έννοια του προβολικού χώρου και των προβολικών αλγεβρικών καμπυλών. Εξετάζεται η σχέση μεταξύ των καμπυλών του $\mathbb{C}^2$ και των προβολικών καμπυλών, και μελετώνται αντίστοιχα θέματα μ΄ αυτά που διαπραγματεύθηκε το δεύτερο κεφαλαιο.

Το τέταρτο κεφάλαιο είναι αφιερωμένο στη τομή δύο προβολικών καμπυλών. Ορίζεται ο αριθμός τομής δύο προβολικών καμπυλών σ΄ ένα σημείο και αποδεικνύεται το κλασσικό θεώρημα του Bézout. Τέλος εξετάζεται η σχέση του αριθμού τομής με την πολλαπλότητα της κάθε μίας από τις δύο καμπύλες σ΄ αυτό το σημείο.

Τα γραμμικά συστήματα προβολικών καμπυλών και οι βασικές τους ιδιότητές μελετώνται στο πέμπτο κεφάλαιο. Επίσης, χρησιμοποιούνται για την μελέτη των ανωμάλων σημείων των προβολικών καμπυλών και την απόδειξη του κλασσικού θεωρήματος του Pascal.

Τέλος, το αντικείμενο του πέμπτου κεφαλαίου είναι οι κυβικές. Δίνεται μία ταξινόμησή τους με την βοήθεια της σχέσης ισοδυναμίας των προβολικών καμπυλών και δομείται το σύνολο των ομαλών σημείων τους σε αντιμεταθετική ομάδα.

Θεσσαλονίκη 2006 Δημήτριος Πουλάκης

Συμβολισμοί - Ορολογία

Θα χρησιμοποιούμε τα συνήθη σύμβολα της Θεωρίας Συνολων: $\in$, $\subseteq$, $\subset$, $\cap$ και $\cup$. Αν X και Y είναι υποσύνολα του ίδιου συνόλου, τότε συμβολίζουμε με $X - Y$ το σύνολο των στοιχείων του X που δεν ανήκουν στο Y.

Ας είναι $f : A \to B$ μία απεικόνιση. Η f καλείται ένεση, αν για κάθε $x, y \in A$ με $x \neq y$ έχουμε $f(x) \neq f(y)$ και έφεση αν για κάθε $z \in B$ υπάρχει $x \in A$ με $f(x) = z$. Επίσης, η f καλείται αμφίεση, αν είναι ένεση και έφεση.

Θα συμβολίζουμε με $\mathbb{N}$ το σύνολο των φυσικών αριθμών $\{0, 1, 2, \ldots\}$ και με $\mathbb{Z}$ το σύνολο των ακεραίων αριθμών. Επίσης, με $\mathbb{Q}$, $\mathbb{R}$ και $\mathbb{C}$ θα συμβολίζουμε τα σύνολα των ρητών, πραγματικών και μιγαδικών αριθμών, αντίστοιχα.

Υποθέτουμε ότι όλοι οι δακτύλιοι που χρησιμοποιούμε έχουν μοναδιαίο στοιχείο. Ένα μη μηδενικό στοιχείο a ενός δακτυλίου A καλείται διαιρέτης του μηδενός, αν υπάρχει μη μηδενικό στοιχείο $b \in A$ έτσι, ώστε $ab = 0$. Ένας αντιμεταθετικός δακτύλιος (μη τετριμμένος) ο οποίος δεν έχει διαιρέτες του μηδενός καλείται πεδίο ακεραιότητας.

Κεφάλαιο 1

Πολυώνυμα

1.1 Ο Δακτύλιος των Πολυωνύμων

Ας είναι A ένας αντιμεταθετικός δακτύλιος. Αν n είναι ένας θετικός ακέραιος, τότε συμβολίζουμε με $F_n(A)$ το σύνολο των συναρτήσεων $f : \mathbb{N}^n \to A$ οι οποίες μηδενίζονται σε όλα τα σημεία του $\mathbb{N}^n$ εκτός ενός πεπερασμένου συνόλου. Για $f, g \in F_n(A)$ ορίζουμε τις συναρτήσεις

$$f + g : \mathbb{N}^n \longrightarrow A,\ \mathbf{x} \longmapsto f(\mathbf{x}) + g(\mathbf{x})$$

και

$$fg : \mathbb{N}^n \longrightarrow A,\ \mathbf{x} \longmapsto \sum_{\mathbf{y}+\mathbf{z}=\mathbf{x}} f(\mathbf{y})g(\mathbf{z}).$$

Οι συναρτήσεις $f + g$ και fg καλούνται *άθροισμα* και *γινόμενο* των f και g, αντίστοιχα. Έτσι, έχουμε ορίσει μία πρόσθεση και ένα πολλαπλασιασμό για τα στοιχεία του $F_n(A)$.

Πρόταση 1.1 *Το σύνολο $F_n(A)$ εφοδιασμένο με τις πράξεις της πρόσθεσης και πολλαπλασιασμού δομείται σε αντιμεταθετικό δακτύλιο.*

Απόδειξη. Ας είναι $f, g, h \in F_n(A)$. Τότε για κάθε $\mathbf{x} \in \mathbb{N}^n$ έχουμε

$$\begin{aligned}((f + g) + h)(\mathbf{x}) &= (f + g)(\mathbf{x}) + h(\mathbf{x}) = \\ &(f(\mathbf{x}) + g(\mathbf{x})) + h(\mathbf{x}) = f(\mathbf{x}) + (g(\mathbf{x}) + h(\mathbf{x})) = (f + (g + h))(\mathbf{x})\end{aligned}$$

και

$$(f + g)(\mathbf{x}) = f(\mathbf{x}) + g(\mathbf{x}) = g(\mathbf{x}) + f(\mathbf{x}) = (g + f)(\mathbf{x}).$$

Επομένως, ισχύει

$$(f+g)+h=f+(g+h) \quad \text{και} \quad f+g=g+f.$$

Συνεπώς, η πρόσθεση είναι προσεταιριστική και αντιμεταθετική πράξη. Αν f_0 είναι η συνάρτηση του $F_n(A)$ η οποία απεικονίζει κάθε στοιχείο του $\mathbb{N}^n$ στο 0, τότε για κάθε $f \in F_n(A)$ και $\mathbf{x} \in \mathbb{N}^n$ έχουμε

$$(f+f_0)(\mathbf{x}) = f(\mathbf{x}) + f_0(\mathbf{x}) = f(\mathbf{x}) + 0 = f(\mathbf{x})$$

και επομένως $f + f_0 = f$. Καθώς η πρόσθεση είναι αντιμεταθετική πράξη, ισχύει επίσης $f_0 + f = f$. Άρα η συνάρτηση f_0 είναι το ουδέτερο στοιχείο για την πρόσθεση. Για κάθε $f \in F_n(A)$ ορίζουμε την συνάρτηση

$$-f : \mathbb{N}^n \longrightarrow A,\ \mathbf{x} \longmapsto -f(\mathbf{x}).$$

Εύκολα προκύπτει ότι

$$f+(-f) = f_0 = (-f)+f.$$

Επομένως, η συνάρτηση $-f$ είναι το αντίθετο στοιχείο της f. Για κάθε $\mathbf{x} \in \mathbb{N}^n$ ισχύει

$$(fg)(\mathbf{x}) = \sum_{\mathbf{y}+\mathbf{z}=\mathbf{x}} f(\mathbf{y})g(\mathbf{z}) = \sum_{\mathbf{y}+\mathbf{z}=\mathbf{x}} g(\mathbf{y})f(\mathbf{z}) = (gf)(\mathbf{x})$$

και επομένως έχουμε $fg = gf$. Άρα, ο πολλαπλασιασμός είναι αντιμεταθετική πράξη. Θέτουμε $\mathbf{0} = (0, \ldots, 0)$. Ας είναι f_1 η συνάρτηση του $F_n(A)$ με $f_1(\mathbf{0}) = 1$ και $f(\mathbf{x}) = 0$ για κάθε $\mathbf{x} \neq \mathbf{0}$. Τότε για κάθε $\mathbf{x} \in \mathbb{N}^n$ έχουμε

$$(ff_1)(\mathbf{x}) = \sum_{\mathbf{y}+\mathbf{z}=\mathbf{x}} f(\mathbf{y})f_1(\mathbf{z}) = f(\mathbf{x})f_1(\mathbf{0}) = f(\mathbf{x}).$$

Επομένως $ff_1 = f$. Καθως ο πολλαπλασιασμός είναι αντιμεταθετικός, έχουμε και $f_1 f = f$. Συνεπώς, η συνάρτηση f_1 είναι το ουδέτερο στοιχείο για τον πολλαπλασιασμό. Για κάθε $\mathbf{x} \in \mathbb{N}^n$ έχουμε

$$(f(g+h))(\mathbf{x}) = \sum_{\mathbf{y}+\mathbf{z}=\mathbf{x}} f(\mathbf{y})(g+h)(\mathbf{z}) = \sum_{\mathbf{y}+\mathbf{z}=\mathbf{x}} f(\mathbf{y})(g(\mathbf{z})+h(\mathbf{z}))$$

$$= \sum_{\mathbf{y}+\mathbf{z}=\mathbf{x}} f(\mathbf{y})g(\mathbf{z}) + \sum_{\mathbf{y}+\mathbf{z}=\mathbf{x}} f(\mathbf{y})h(\mathbf{z}) = (fg)(\mathbf{x}) + (fh)(\mathbf{x})$$

και επομένως $f(g+h) = fg + fh$. Επίσης, η αντιμεταθετικότητα του πολλαπλασιασμού δίνει $(g+h)f = gf + hf$. Συνεπώς, ο πολλαπλασιασμός είναι επιμεριστικός ως προς την πρόσθεση. Τέλος, θα δείξουμε ότι ο πολλαπλασιασμός είναι προσεταιριστικός. Αν $\mathbf{x} \in \mathbb{N}^n$, τότε

$$((fg)h)(\mathbf{x}) = \sum_{\mathbf{y}+\mathbf{z}=\mathbf{x}} (fg)(\mathbf{y})h(\mathbf{z}) =$$
$$\sum_{\mathbf{y}+\mathbf{z}=\mathbf{x}} \Big(\sum_{\mathbf{u}+\mathbf{v}=\mathbf{y}} f(\mathbf{u})g(\mathbf{v})\Big)h(\mathbf{z}) = \sum_{\mathbf{u}+\mathbf{v}+\mathbf{z}=\mathbf{x}} f(\mathbf{u})g(\mathbf{v})h(\mathbf{z}).$$

Με τον ίδιο τρόπο παίρνουμε

$$(f(gh))(\mathbf{x}) = \sum_{\mathbf{u}+\mathbf{v}+\mathbf{z}=\mathbf{x}} f(\mathbf{u})g(\mathbf{v})h(\mathbf{z}).$$

Άρα $(fg)h = f(gh)$. Επομένως, το σύνολο $F_n(A)$ εφοδιασμένο με την πρόσθεση και τον πολλαπλασιασμό που ορίσαμε παραπάνω είναι ένας αντιμεταθετικός δακτύλιος.

Ας είναι $a \in A$. Συμβολίζουμε με f_a την συνάρτηση του $F_n(A)$ με $f_a(\mathbf{x}) = 0$ για κάθε $\mathbf{x} \neq \mathbf{0}$ και $f_a(\mathbf{0}) = a$. Αν $a, b \in A$ τότε

$$f_{a+b}(\mathbf{x}) = 0 = f_a(\mathbf{x}) + f_b(\mathbf{x}), \quad f_{ab}(\mathbf{x}) = 0 = f_a(\mathbf{x})f_b(\mathbf{x})$$

για κάθε $\mathbf{x} \in \mathbb{N}^n$ με $\mathbf{x} \neq \mathbf{0}$ και

$$f_{a+b}(\mathbf{0}) = a + b = f_a(\mathbf{0}) + f_b(\mathbf{0}), \quad f_{ab}(\mathbf{0}) = ab = f_a(\mathbf{0})f_b(\mathbf{0}).$$

Έτσι, έχουμε

$$f_{a+b} = f_a + f_b \quad \text{και} \quad f_{ab} = f_a f_b.$$

Επίσης, αν $f_a = f_b$, τότε

$$a = f_a(\mathbf{0}) = f_b(\mathbf{0}) = b.$$

Άρα η απεικόνιση

$$\phi : A \longrightarrow F_n(A), \ a \longmapsto f_a$$

είναι ένας μονομορφισμός δακτυλίων. Έτσι, θα ταυτίζουμε τον δακτύλιο A με την εικόνα του διά μέσου του ϕ μέσα στον $F_n(A)$.

Ας είναι m ένας θετικός ακέραιος με $m < n$. Αν $f \in F_m(A)$, τότε υπάρχει ένα πεπερασμένο σύνολο S έτσι, ώστε $f(\mathbf{x}) = 0$, για κάθε $\mathbf{x} \in \mathbb{N}^n - S$. Ορίζουμε την συνάρτηση $\tilde{f} \in F_n(A)$ ως εξής: Θέτουμε $\tilde{f}(a_1, \ldots, a_m, 0, \ldots, 0) = f(a_1, \ldots, a_m)$ για κάθε $(a_1, \ldots, a_m) \in S$ και $\tilde{f}(\mathbf{x}) = 0$ για οποιοδήποτε άλλο στοιχείο $\mathbf{x} \in \mathbb{N}^n$. Εύκολα διαπιστώνουμε ότι η απεικόνιση

$$\psi : F_m(A) \longrightarrow F_n(A), \ f \longmapsto \tilde{f}$$

είναι ένας μονομορφισμός δακτυλίων. Οπότε, θα ταυτίζουμε τον δακτύλιο $F_m(A)$ με την εικόνα του διά μέσου του ψ μέσα στον $F_n(A)$.

Ας θεωρήσουμε στη συνέχεια τις παρακάτω n-άδες:

$$\mathbf{e}_1 = (1, 0, \ldots, 0), \ \mathbf{e}_2 = (0, 1, \ldots, 0), \ldots, \ \mathbf{e}_n = (0, \ldots, 0, 1).$$

Συμβολίζουμε με X_i την συνάρτηση του $F_n(A)$ με $X_i(\mathbf{e}_i) = 1$ και $X_i(\mathbf{x}) = 0$ για κάθε $\mathbf{x} \in \mathbb{N}^n - \{\mathbf{e}_i\}$. Ορίζουμε $X_i^0 = f_1$ $(i = 1, \ldots, n)$. Θα δείξουμε ότι αν $a \in A$ και $(i_1, \ldots, i_n) \in \mathbb{N}^n$, τότε η συνάρτηση $aX_1^{i_1} \cdots X_n^{i_n}$ απεικονίζει την n-άδα $(i_1, \ldots, i_n)$ στο a και οποιοδήποτε άλλο στοιχείο του $\mathbb{N}^n$ στο μηδέν. Για κάθε στοιχείο $\mathbf{i} = (i_1, \ldots, i_n)$ του $\mathbb{N}^n$ θέτουμε $|\mathbf{i}| = i_1 + \cdots + i_n$. Θα εφαρμόσουμε την μέθοδο της επαγωγής επί του $|\mathbf{i}|$. Αν $|\mathbf{i}| = 0$, τότε $i_l = 0$ $(l = 1, \ldots, n)$. Άρα $aX_1^{i_1} \cdots X_n^{i_n} = af_1$ και κατά συνέπεια η προς απόδειξη πρόταση αληθεύει. Ας υποθέσουμε ότι για την n-άδα $\mathbf{i} = (i_1, \ldots, i_n)$ η πρόταση ισχύει και ας πάρουμε $\mathbf{j} = (j_1, \ldots, j_n)$ με $|\mathbf{j}| = |\mathbf{i}| + 1$. Τότε υπάρχει δείκτης l με $j_l = i_l + 1$ και $j_k = i_k$ για κάθε δείκτη k με $k \neq l$. Για $\mathbf{a} \in \mathbb{N}^n$ έχουμε

$$(aX_1^{j_1} \cdots X_n^{j_n})(\mathbf{a}) = \sum_{\mathbf{b}+\mathbf{c}=\mathbf{a}} (aX_1^{i_1} \cdots X_n^{i_n})(\mathbf{b}) X_l(\mathbf{c}).$$

Αν $\mathbf{a} = \mathbf{j}$, τότε

$$(aX_1^{j_1} \cdots X_n^{j_n})(\mathbf{j}) = (aX_1^{i_1} \cdots X_n^{i_n})(\mathbf{i}) = a.$$

Αν $\mathbf{a} \neq \mathbf{j}$, τότε έχουμε είτε $\mathbf{b} \neq \mathbf{i}$ είτε $\mathbf{c} \neq \mathbf{e}_l$ και επομένως

$$(aX_1^{j_1} \cdots X_n^{j_n})(\mathbf{a}) = 0.$$

Άρα, η συνάρτηση $aX_1^{i_1} \cdots X_n^{i_n}$ απεικονίζει την n-άδα $(i_1, \ldots, i_n)$ στο a και κάθε άλλο στοιχείο του $\mathbb{N}^n$ στο μηδέν.

Η συνάρτηση $aX_1^{i_1}\cdots X_n^{i_n}$, όπου $a\neq 0$, καλείται *μονώνυμο*. Παρατηρούμε ότι κάθε συνάρτηση $f\in F_n(A)$ γράφεται με μοναδικό τρόπο ως ένα πεπερασμένο άθροισμα διαφορετικών μονωνύμων:

$$f=\sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n}X_1^{i_1}\cdots X_n^{i_n}.$$

Θα καλούμε την f *πολυώνυμο* ως προς τις απροσδιόριστες (ή μεταβλητές) $X_1,\ldots, X_n$ και τα $a_{i_1,\ldots,i_n}$ *συντελεστές* του. Αν

$$g=\sum_{i_1,\ldots,i_n} b_{i_1,\ldots,i_n}X_1^{i_1}\cdots X_n^{i_n},$$

είναι ένα άλλο πολυώνυμο, τότε το άθροισμα και το γινόμενο των f και g είναι

$$f+g=\sum_{i_1,\ldots,i_n}(a_{i_1,\ldots,i_n}+b_{i_1,\ldots,i_n})X_1^{i_1}\cdots X_n^{i_n}$$

και

$$fg=\sum_{i_1,\ldots,i_n}\Big(\sum_{k_1+l_1=i_1}\cdots\sum_{k_n+l_n=i_n} a_{k_1,\ldots,k_n}b_{l_1,\ldots,l_n}\Big)X_1^{i_1}\cdots X_n^{i_n},$$

αντίστοιχα. Στη συνέχεια, θα συμβολίζουμε με $A[X_1,\ldots,X_n]$, αντί με $F_n(A)$, τον δακτύλιο των πολυωνύμων με απροσδιόριστες $X_1,\ldots,X_n$ επί του A. Αν m είναι ακέραιος με $1\leq m<n$, τότε, καθώς είδαμε παραπάνω, ο δακτύλιος $A[X_1,\ldots,X_m]$ μπορεί να θεωρηθεί ως υποδακτύλιος του $A[X_1,\ldots,X_n]$. Επομένως, έχουμε $A[X_1,\ldots,X_n]=A[X_1,\ldots,X_m][X_{m+1},\ldots,X_n]$.

Καλούμε *βαθμό* ενός μη μηδενικού πολυωνύμου

$$f=\sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n}X_1^{i_1}\cdots X_n^{i_n}$$

του $A[X_1,\ldots,X_n]$ το μεγαλύτερο από τα αθροισματα $i_1+\cdots+i_n$ με $a_{i_1,\ldots,i_n}\neq 0$. Ο βαθμός του f συμβολίζεται με $\deg f$. Αν όλα τα παραπάνω αθροίσματα έχουν την ίδια τιμή, τότε το πολυώνυμο f καλειται *ομογενες*. Παρατηρούμε ότι

$$f=f_{d_1}+f_{d_2}+\cdots+f_{d_k},$$

όπου f_{d_j} είναι ομογενές πολυώνυμο βαθμού d_j με $d_1<\ldots<d_k$. Επίσης, θέτουμε $\deg(0)=-\infty$. Για κάθε $f,g\in A[X_1,\ldots,X_n]$, εύκολα παίρνουμε

$$\deg fg\leq \deg f+\deg g,\quad \deg(f+g)\leq\max\{\deg f,\deg g\}.$$

Παράδειγμα 1.1 Ας είναι $f = \bar{2}X^3 + \bar{1}$, $g = \bar{3}X^4 + X$ και $h = X^2 + \bar{1}$ τρία πολυώνυμα του $\mathbb{Z}_6[X]$. Έχουμε $fg = \bar{5}X^4 + X$ και $fh = \bar{2}X^5 + \bar{2}X^3 + X^2 + \bar{1}$. Παρατηρούμε ότι $\deg fg = 4 < 7 = \deg f + \deg g$ και $\deg fh = 5 = \deg f + \deg h$.

Πρόταση 1.2 *Ας είναι f ένα πολυώνυμο του $A[X_1, \ldots, X_n]$ βαθμού $d \geq 0$. Τότε, το f είναι ομογενές, αν και μόνον αν η ισότητα*

$$f(TX_1, \ldots, TX_n) = T^d f(X_1, \ldots, X_n)$$

ισχύει μέσα στο $A[X_1, \ldots, X_n, T]$.

Απόδειξη. Ας είναι

$$f = \sum_{i_1, \ldots, i_n} a_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n} = f_{d_1} + f_{d_2} + \cdots + f_{d_k},$$

όπου f_{d_j} είναι ομογενές πολυώνυμο βαθμού d_j και $d_1 < \ldots < d_k = d$. Αν το f είναι ομογενές, τότε για κάθε n-άδα $(i_1, \ldots, i_n)$ με $a_{i_1, \ldots, i_n} \neq 0$ ισχύει $i_1 + \cdots + i_n = d$. Έτσι, έχουμε

$$f(TX_1, \ldots, TX_n) = T^d f(X_1, \ldots, X_n).$$

Αντιστρόφως, ας υποθέσουμε ότι το f έχει την παραπάνω ιδιότητα. Τότε

$$T^{d_1} f_{d_1} + T^{d_2} f_{d_2} + \cdots + T^{d_k} f_{d_k} = T^d (f_{d_1} + f_{d_2} + \cdots + f_{d_k}),$$

απ' όπου έπεται $f_{d_1} = \cdots = f_{d_{k-1}} = 0$ και επομένως το f είναι ομογενές πολυώνυμο.

Στη συνέχεια, ας γράψουμε $f = F_0 + F_1 X_i + \cdots + F_r X^r$, όπου F_j είναι πολυώνυμο του $A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$ $(j = 1, \ldots, r)$. και $F_r \neq 0$. Ο ακέραιος r καλείται *βαθμός* του f ως προς X_i και συμβολίζεται με $\deg_{X_i} f$. Δηλαδή, έχουμε $\deg_{X_i} f = r$. Για κάθε $f, g \in A[X_1, \ldots, X_n]$ ισχύουν τα εξής:

$$\deg_{X_i} fg \leq \deg_{X_i} f + \deg_{X_i} g, \quad \deg_{X_i}(f+g) \leq \max\{\deg_{X_i} f, \deg_{X_i} g\}.$$

Πρόταση 1.3 *Ας είναι A ένα πεδίο ακεραιότητας. Τότε ο δακτύλιος $A[X_1, \ldots, X_n]$ είναι ένα πεδίο ακεραιότητας. Αν $f, g \in A[X_1, \ldots, X_n]$, τότε $\deg fg = \deg f + \deg g$ και $\deg_{X_i} fg = \deg_{X_i} f + \deg_{X_i} g$. Επίσης, η ομάδα των αντιστρεψίμων στοιχείων του $A[X_1, \ldots, X_n]$ είναι η ομάδα των αντιστρεψίμων στοιχείων του A.*

Απόδειξη. Θα εφαρμόσουμε επαγωγή επί του n. Ας υποθέσουμε ότι $n = 1$ και ας είναι

$$f = a_0 + a_1X + \cdots + a_rX^r, \quad g = b_0 + b_1X + \cdots + b_sX^s$$

δύο πολυώνυμα του $A[X]$ με $a_r \neq 0$ και $b_s \neq 0$. Τότε

$$fg = a_0b_0 + (a_0b_1 + a_1b_0)X + \cdots + a_rb_sX^{r+s}.$$

Καθώς ο A είναι πεδίο ακεραιότητας, έχουμε $a_rb_s \neq 0$ και επομένως $fg \neq 0$. Συνεπώς, ο δακτύλιος $A[X]$ είναι ένα πεδίο ακεραιότητας. Ας υποθέσουμε τώρα ότι ο δακτύλιος $A[X_1, \ldots, X_{n-1}]$ είναι ένα πεδίο ακεραιότητας. Τότε ο δακτύλιος $A[X_1, \ldots, X_{n-1}][X_n]$ είναι επίσης ένα πεδίο ακεραιότητας. Καθώς $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$ παίρνουμε το ζητούμενο.

Ας είναι τώρα f, g δύο μη μηδενικά πολυώνυμα του $A[X_1, \ldots, X_n]$ και

$$f = f_{d_1} + \cdots + f_{d_k}, \quad g = g_{e_1} + \cdots + g_{e_l},$$

όπου f_{d_j}, g_{e_l} είναι ομογενή πολυώνυμα βαθμού d_j και e_l αντίστοιχα με $d_1 < \ldots < d_k$ και $e_1 < \ldots < e_l$. Καθώς το $A[X_1, \ldots, X_n]$ είναι ένα πεδίο ακεραιότητας, έχουμε $f_{d_k}g_{e_l} \neq 0$ και επομένως το άθροισμα των ομογενών όρων μεγαλυτέρου βαθμού του fg είναι το πολυώνυμο $f_{d_k}g_{e_l}$. Άρα $\deg fg = \deg f + \deg g$. Επίσης, αν

$$f = F_0 + F_1X_i + \cdots + F_{n_i}X^{n_i}, \quad g = G_0 + G_1X_i + \cdots + G_{m_i}X^{m_i},$$

όπου $F_j, G_l \in A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$ και $F_{n_i} \neq 0$, $G_{m_i} \neq 0$, τότε έχουμε

$$fg = F_0G_0 + (F_1G_0 + F_0G_1)X_i + \cdots + F_{n_i}G_{m_i}X_i^{n_i+m_i}$$

και $F_{n_i}G_{m_i} \neq 0$. Άρα $\deg_{X_i} fg = \deg_{X_i} f + \deg_{X_i} g$.

Ας είναι f ένα αντιστρέψιμο στοιχείο του $A[X_1, \ldots, X_n]$. Τότε υπάρχει $g \in A[X_1, \ldots, X_n]$ με $fg = 1$. Επομένως $\deg f + \deg g = 0$. Άρα $\deg f = 0$ και κατά συνέπεια $f \in A$.

Παράδειγμα 1.2 Σύμφωνα με την Πρόταση 1.3, οι ομάδες των αντιστρεψίμων στοιχείων των δακτυλίων $\mathbb{Z}[X_1, \ldots, X_n]$ και $\mathbb{Q}[X_1, \ldots, X_n]$ είναι οι $\{1, -1\}$ και $\mathbb{Q} - \{0\}$, αντίστοιχα.

Αν A είναι ένα πεδίο ακεραιότητας και K το σώμα κλασμάτων του, τότε θα συμβολίζουμε με $K(X_1, \ldots, X_n)$ το σώμα κλασμάτων του πεδίου ακεραιότητας $A[X_1, \ldots, X_n]$.

Ας είναι $f \in A[X_1, \ldots, X_n]$ και $P = (p_1, \ldots, p_n) \in A^n$. Αν

$$f = \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n},$$

τότε το στοιχείο

$$\sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} p_1^{i_1} \ldots p_n^{i_n}$$

καλείται *τιμή* του f στο P και συμβολίζεται με $f(P)$. Για κάθε ζεύγος πολυωνύμων f, g και $P \in A^n$ ισχύει

$$(f+g)(P) = f(P) + g(P), \quad (fg)(P) = f(P)g(P).$$

Η συνάρτηση

$$\Sigma_f : A^n \longrightarrow A, \ P \longmapsto f(P)$$

καλείται *πολυωνυμική συνάρτηση* που αντιστοιχεί στο f.

1.2 Δακτύλιοι με Μοναδική Παραγοντοποίηση

Ας είναι A ένα πεδίο ακεραιότητας και U η ομάδα των αντιστρεψίμων στοιχείων του. Αν $a, b \in A$, τότε λέμε ότι το b *διαιρεί* το a (ή ότι το a είναι *διαιρετό* από το b) και γράφουμε $b|a$, αν υπάρχει $c \in A$ τέτοιο, ώστε $a = bc$. Αποδεικνύονται εύκολα οι εξής ιδιότητες:
(α) Αν $a|b$ και $b|c$, τότε $a|c$.
(β) Αν $a|b$ και $a|c$, τότε $a|xb + yc$ για κάθε $x, y \in A$.
(γ) Για κάθε $a \in A$ ισχύει $a|0$.
Επίσης, αν το b δεν διαιρεί το a, τότε γράφουμε $b \nmid a$.

Δύο στοιχεία $a, b \in A$ καλούνται *προσαρτημένα*, αν υπάρχει $u \in U$ έτσι, ώστε $a = bu$. Ας είναι $ab \neq 0$. Τότε τα a και b είναι προσαρτημένα, αν και μόνον αν $a|b$ και $b|a$. Πράγματι, αν $a|b$ και $b|a$, τότε υπάρχουν $u, v \in A$ με $a = ub$ και $b = va$. Έτσι, $b = uvb$ και επομένως $uv = 1$. Άρα $u, v \in U$ και κατά συνέπεια τα a, b είναι προσαρτημένα. Αντιστρόφως, αν τα a, b είναι προσαρτημένα, τότε υπάρχει $u \in U$ έτσι, ώστε $a = bu$ και επομένως $b|a$. Επίσης, έχουμε $au^{-1} = b$ και κατά συνέπεια $a|b$.

Ας είναι $a_1, \ldots, a_n \in A$. Ένα στοιχείο d καλείται *μέγιστος κοινός διαιρέτης* (μ.κ.δ.) των $a_1, \ldots, a_n$, αν ισχύουν τα εξής:
(α) $d|a_1, \ldots, d|a_n$.
(β) αν $\delta \in A$ και $\delta|a_1, \ldots, \delta|a_n$, τότε $\delta|d$.
Αν d και d' είναι δύο μέγιστοι κοινοί διαιρέτες για τα $a_1, \ldots, a_n$, τότε $d|d'$ και $d'|d$. Επομένως, τα στοιχεία d και d' είναι προσαρτημένα. Αν ένας μ.κ.δ. των $a_1, \ldots, a_n$ είναι το 1, τότε λέμε ότι τα $a_1, \ldots, a_n$ είναι *πρώτα μεταξύ τους*. Τότε ένα στοιχείο $d \in A$ είναι μ.κ.δ. των $a_1, \ldots, a_n$, αν και μόνον αν είναι αντιστρέψιμο.

Ένα στοιχείο $m \in A$ καλείται *ελάχιστο κοινό πολλαπλάσιο* (ε.κ.π.) των $a_1, \ldots, a_n$, αν ισχύουν τα εξής:
(α) $a_1|m, \ldots, a_n|m$.
(β) αν $\mu \in A$ και $a_1|\mu, \ldots, a_n|\mu$, τότε $m|\mu$.
Όπως και στη περίπτωση του μέγιστου κοινού διαιρέτη, αν m και m' είναι δύο ελάχιστα κοινά πολλαπλάσια για τα $a_1, \ldots, a_n$, τότε αυτά είναι προσαρτημένα.

Ένα μη αντιστρέψιμο στοιχείο $a \in A$, με $a \neq 0$, καλείται *ανάγωγο* αν δεν υπάρχουν $b, c \in A - U$ έτσι, ώστε $a = bc$. Δηλαδή, οι μόνοι διαιρέτες του a είναι τα αντιστρέψιμα και τα προσαρτημένα σ' αυτό στοιχεία. Για παράδειγμα, στο δακτύλιο $\mathbb{Z}$ τα ανάγωγα στοιχεία είναι οι ακέραιοι της μορφής $\pm p$, όπου p είναι πρώτος αριθμός.

Το πεδίο ακεραιότητας A καλείται *δακτύλιος με μοναδική παραγοντοποίηση* αν ισχύουν τα εξής:
(α) Για κάθε στοιχείο $a \in A$ με $a \neq 0$ έχουμε είτε $a \in U$ είτε

$$a = p_1 \cdots p_k,$$

όπου $p_1, \ldots p_k$ είναι ανάγωγα στοιχεία του A.
(β) Η παραπάνω γραφή είναι μοναδική. Δηλαδή, αν

$$a = p_1 \cdots p_k = q_1 \cdots q_l$$

είναι δύο αναλύσεις του a σε γινόμενο αναγώγων στοιχείων, τότε $k = l$ και υπάρχει μία μετάθεση σ του $\{1, \ldots, k\}$ έτσι, ώστε τα στοιχεία $p_i, q_{\sigma(i)}$ είναι προσαρτημένα για κάθε $i = 1, \ldots, k$.

Ένα κλασσικό παράδειγμα ενός τέτοιου δακτυλίου είναι ο δακτύλιος των ακεραίων αριθμών. Επίσης, κάθε σώμα είναι ένας δακτυλιος με μοναδική παραγοντοποίηση.

Ας υποθέσουμε ότι ο A είναι δακτύλιος με μοναδική παραγοντοποίηση. Ας είναι $a \in A - \{0\}$ και $a \notin U$. Τότε $a = up_1^{a_1} \cdots p_k^{a_k}$, όπου

u είναι αντιστρέψιμο στοιχείο, $p_1, \ldots, p_k$ διακεκριμμένα ανάγωγα στοιχεία και $a_1, \ldots, a_k$ θετικοί ακέραιοι. Αν $b \in A$ είναι διαιρέτης του a, τότε υπάρχει $c \in A$ με $bc = a$. Από την μοναδικότητα της γραφής των στοιχείων του A ως γινόμενο αναγώγων στοιχείων, έπεται ότι $b = vp_1^{b_1} \cdots p_k^{b_k}$, όπου v είναι αντιστρέψιμο στοιχείο και $0 \leq b_i \leq a_i$ $(i = 1, \ldots, k)$. Αντιστρόφως, αν το b έχει την παραπάνω μορφή, τότε θέτουμε $c = uv^{-1}p_1^{a_1-b_1} \cdots p_k^{a_k-b_k}$ και έχουμε $bc = a$. Άρα $b|a$, αν και μόνον αν $b = vp_1^{b_1} \cdots p_k^{b_k}$, όπου v είναι αντιστρέψιμο στοιχείο και $0 \leq b_i \leq a_i$ $(i = 1, \ldots, k)$.

Κάθε ζεύγος στοιχείων $a, b \in A$ έχει ένα μέγιστο κοινό διαιρέτη. Πράγματι, ας είναι

$$a = up_1^{a_1} \cdots p_k^{a_k}, \quad b = vp_1^{b_1} \cdots p_k^{b_k},$$

όπου u, v είναι αντιστρέψιμα στοιχεία, $p_1, \ldots, p_k$ διακεκριμμένα ανάγωγα στοιχεία και $a_1, \ldots a_k, b_1, \ldots, b_k$ ακέραιοι ≥ 0. Θέτουμε

$$d = p_1^{\min\{a_1,b_1\}} \cdots p_k^{\min\{a_k,b_k\}}.$$

Τότε $d|a$ και $d|a$. Αν $\delta \in A$ και $\delta|a$, $\delta|b$, τότε

$$\delta = wp_1^{c_1} \cdots p_k^{c_k},$$

όπου w είναι αντιστρέψιμο στοιχείο του A και $c_1, \ldots, c_k$ ακέραιοι με $0 \leq c_i \leq \min\{a_i, b_i\}$ $(i = 1, \ldots, n)$ και επομένως $\delta|d$. Συνεπώς το d είναι ένας μέγιστος κοινός διαιρέτης των a και b.

Με ανάλογο τρόπο αποδεικνύεται ότι ένα ελάχιστο κοινό πολλαπλάσιο των a, b είναι το στοιχείο

$$p_1^{\max\{a_1,b_1\}} \cdots p_k^{\max\{a_k,b_k\}}.$$

Πρόταση 1.4 *Το πεδίο ακεραιότητας A είναι δακτύλιος με μοναδική παραγοντοποίηση, αν και μόνον αν ισχύουν τα εξής:*
(α) Κάθε μη μηδενικό και μη αντιστρέψιμο στοιχείο του A αναλύεται σε γινόμενο αναγώγων στοιχείων.
(β′) Κάθε ανάγωγο στοιχείο που διαιρεί το γινόμενο δύο στοιχείων διαιρεί τουλάχιστον ένα από αυτά.

Απόδειξη. Κατ′ αρχάς ας υποθέσουμε οτι ο A είναι δακτύλιος με μοναδική παραγοντοποίηση. Τότε η (α) ισχύει. Θα δείξουμε την (β′).

Ας είναι p ένα ανάγωγο στοιχείο του A και $a, b \in A$ με $p|ab$. Τότε υπάρχει $c \in A$ με $ab = pc$. Καθώς το p είναι ανάγωγο, τουλάχιστον ένα από τα a, b είναι μη αντιστρέψιμο. Αν το a (αντίστοιχα το b) είναι αντιστρέψιμο, τότε το p διαιρεί το b (αντίστοιχα το a). Ας υποθέσουμε λοιπόν ότι τα a, b είναι μη αντιστρέψιμα και ας είναι

$$a = a_1 \cdots a_k, \quad b = b_1 \cdots b_l, \quad c = c_1 \cdots c_m$$

οι αναλύσεις των a, b, c σε γινόμενο αναγώγων στοιχείων. Επομένως

$$a_1 \cdots a_k b_1 \cdots b_l = pc_1 \cdots c_m.$$

Καθώς ο A είναι δακτύλιος με μοναδική παραγοντοποίηση, το p είναι προσαρτημένο σε κάποιο a_i ή σε κάποιο b_i και κατά συνέπεια διαιρεί το a ή το b. Συνεπώς, ισχύει η (β′).

Αντιστρόφως, ας υποθέσουμε ότι ισχύουν οι (α) και (β′). Πρώτα θα δείξουμε ότι αν $p, p_1, \ldots, p_k$ είναι ανάγωγα στοιχεία του A με $p|p_1 \cdots p_k$, τότε υπάρχει i έτσι, ώστε $p|p_i$. Για $i = 1$ αυτό είναι προφανές. Ας υποθέσουμε ότι αυτό ισχύει για $k = m$ και ας είναι $k = m + 1$. Από την (β′) έχουμε ότι $p|p_1 \cdots p_m$ ή $p|p_{m+1}$. Αν το p δεν διαιρεί το p_{m+1}, τότε διαιρεί το $p_1 \cdots p_m$ και, σύμφωνα με την υπόθεση της επαγωγής, έχουμε $p|p_i$ με $1 \leq i \leq m$.

Ας είναι τώρα $p_1, \ldots, p_k, q_1, \ldots, q_l$ ανάγωγα στοιχεία του A με

$$p_1 \cdots p_k = q_1 \cdots q_l.$$

Μπορούμε να υποθέσουμε ότι $k \leq l$. Τότε $p_1|q_1 \cdots q_l$ και από τα παραπάνω έπεται ότι υπάρχει i με $p_1|q_i$. Έτσι, καθώς το q_i είναι ανάγωγο, έχουμε $q_i = p_1 u_i$, όπου το u_i είναι αντιστρέψιμο στοιχείο του A. Επομένως

$$p_2 \cdots p_k = q_1 \cdots q_{i-1} u_i q_{i+1} \cdots q_l.$$

Με τον ίδιο τρόπο βρίσκουμε ότι το p_2 διαιρεί κάποιο από τα $q_1, \ldots, q_{i-1}$, $q_{i+1}, \ldots, q_l$. Επαναλαμβάνοντας αυτή την διαδικασία συμπεραίνουμε ότι τα $p_3, \ldots, p_{k-1}$ διαιρούν επίσης κάποια από τα $q_1, \ldots, q_l$ και έτσι παίρνουμε

$$p_k = u r_1 \cdots r_{l-k+1},$$

όπου u είναι αντιστρέψιμο στοιχείο και $r_1, \ldots, r_{l-k+1}$ είναι κάποια από τα στοιχεία $q_1, \ldots, q_l$. Επειδή το p_k είναι ανάγωγο, έπεται ότι $l = k$ και $p_k = u r_1$.

Πόρισμα 1.1 *Ας είναι A ένας δακτύλιος με μοναδική παραγοντοποίηση. Αν $a, b, c \in A$ με $a|bc$ και τα a, b είναι πρώτα μεταξύ τους, τότε $a|c$.*

Απόδειξη. Αν $a \in U$, τότε $a|c$. Ας υποθέσουμε λοιπόν ότι $a \notin U$. Τότε $a = up_1^{a_1} \cdots p_k^{a_k}$, όπου u είναι αντιστρέψιμο στοιχείο, $p_1, \ldots, p_k$ διακεκριμμένα ανάγωγα στοιχεία και $a_1, \ldots, a_k$ θετικοί ακέραιοι. Καθώς τα a και b είναι πρώτα μεταξύ τους, η Πρόταση 1.4(β′) έπεται ότι $p_i|c$ $(i = 1, \ldots, k)$. Αν c_i είναι ο μεγαλύτερος θετικός ακέραιος τέτοιος, ώστε $p_i^{c_i}|c$, τότε από την μοναδικότητα της γραφής των στοιχείων του A ως γινόμενο αναγώγων στοιχείων, προκύπτει ότι $a_i \leq c_i$. Άρα $a|c$.

Στη συνέχεια θ′ ασχοληθούμε με πολυώνυμα των οποίων οι συντελεστές ανήκουν στο πεδίο ακεραιότητας A. Ένα στοιχείο $a \in A$ είναι ανάγωγο, αν και μόνον αν είναι ανάγωγο ως στοιχείο του $A[X]$. Πράγματι, αν το a είναι ανάγωγο μέσα στο $A[X]$, τότε αυτό είναι προφανώς ανάγωγο και μέσα στο A. Αντιστρόφως, αν το a είναι ανάγωγο μέσα στο A και $a = f_1 f_2$, όπου f_1, f_2 είναι μη αντιστρέψιμα στοιχεία του $A[X]$, τότε $0 = \deg f_1 f_2 = \deg f_1 + \deg f_2$ και επομένως $\deg f_1 = \deg f_2 = 0$. Άρα $f_1, f_2 \in A$ και κατά συνέπεια ένα από τα f_1, f_2 είναι αντιστρέψιμο που είναι άτοπο. Επομένως, το a είναι ανάγωγο μέσα στο $A[X]$.

Θεώρημα 1.1 *Ας είναι A ένας δακτύλιος με μοναδική παραγοντοποίηση. Τότε ο δακτύλιος πολυωνύμων $A[X]$ είναι επίσης δακτύλιος με μοναδική παραγοντοποίηση.*

Για την απόδειξη αυτού του θεωρήματος θα χρειαστούμε το παρακάτω λήμμα.

Λήμμα 1.1 *Ας είναι A ένας δακτύλιος με μοναδική παραγοντοποίηση. Αν $f, g \in A[X]$ και a είναι ένα ανάγωγο στοιχείο του A με $a|fg$, τότε $a|f$ ή $a|g$.*

Απόδειξη. Ας είναι

$$f = b_0 + b_1 X + \cdots + b_n X^n, \quad g = c_0 + c_1 X + \cdots + c_m X^m.$$

Ας υποθέσουμε ότι το a δεν διαιρεί κανένα από τα f και g. Τότε υπάρχουν δείκτες k και h, ώστε $b_k \neq 0$, $c_h \neq 0$ και $a \not| b_k$, $a \not| c_h$. Υποθέτουμε ότι οι k και h είναι οι μικρότεροι δείκτες μ′ αυτή την ιδιότητα. Ο συντελεστής του X^{h+k} στο πολυώνυμο fg είναι:

$$d_{h+k} = b_0 c_{h+k} + b_1 c_{h+k-1} + \cdots + b_k c_h + \cdots + b_{h+k} c_0$$

(όπου θέσαμε $b_i = c_j = 0$ για $i > n$ και $j > m$). Από την επιλογή των k, h και την Πρόταση 1.4 έχουμε ότι το a δεν διαιρεί το $b_k c_h$. Καθώς το a διαιρεί καθένα από τους άλλους όρους του d_{h+k}, έπεται ότι το a δεν διαιρεί το d_{h+k}. Αν το a διαιρεί το γινόμενο fg, τότε διαιρεί όλους τους συντελεστές του fg και επομένως τον d_{k+h} που είναι άτοπο. Άρα το fg δεν διαιρείται από το a.

Απόδειξη του Θεωρήματος 1.1. Ας είναι $f \in A[X]$, $f \neq 0$ και f μη αντιστρέψιμο στοιχείο. Θα εφαρμόσουμε επαγωγή επί του βαθμού του f. Αν $\deg f = 0$, τότε $f \in A$ και επομένως το f αναλύεται σε γινόμενο αναγώγων στοιχείων με μοναδικό τρόπο. Ας υποθέσουμε ότι κάθε πολυώνυμο του $A[X]$ βαθμού $< k$ γράφεται ως γινόμενο αναγώγων στοιχείων με μοναδικό τρόπο. Ας είναι $\deg f = k$. Συμβολίζουμε με d ένα μ.κ.δ. των συντελεστών του f. Άρα $f = df_1$, όπου f_1 είναι ένα πολυώνυμο του $A[X]$ του οποίου οι συντελεστές είναι πρώτοι μεταξύ τους. Επίσης, υπάρχουν ανάγωγα στοιχεία $c_1, \ldots, c_m$ του A έτσι, ώστε $d = c_1 \cdots c_m$. Αν το f_1 είναι ανάγωγο, τότε τελειώσαμε. Αν το f_1 δεν είναι ανάγωγο, τότε υπάρχουν μη αντιστρέψιμα στοιχεία $g, h \in A[X]$ έτσι, ώστε $f_1 = gh$. Καθώς κάθε μ.κ.δ. των συντελεστών του f_1 είναι αντιστρέψιμο στοιχείο του A, έχουμε $0 < \deg g < \deg f_1$ και $0 < \deg h < \deg f_1$. Επομένως, σύμφωνα με την υπόθεση της επαγωγής, υπάρχουν ανάγωγα στοιχεία $p_1, \ldots, p_r, q_1, \ldots, q_s$ του $A[X]$ τέτοια, ώστε

$$g = p_1 \cdots p_r, \quad h = q_1 \cdots q_s.$$

Επομένως

$$f = c_1 \cdots c_m p_1 \cdots p_r q_1 \cdots q_s.$$

Ας υποθέσουμε τώρα ότι υπάρχει πολυώνυμο του $A[X] - A$ το οποίο γράφεται με δύο τρόπους ως γινόμενο αναγώγων στοιχείων του $A[X]$. Ας είναι f ένα τέτοιο πολυώνυμο με τον μικρότερο δυνατό βαθμό του οποίου οι συντελεστές είναι πρώτοι μεταξύ τους. Έτσι, υπάρχουν ανάγωγα στοιχεία $p_1, \ldots, p_r, q_1, \ldots, q_s$ του $A[X]$ με

$$p_1 \cdots p_r = f = q_1 \cdots q_s.$$

Επίσης, για κάθε ζεύγος δεικτών $i \in \{1, \ldots, r\}$ και $j \in \{1, \ldots, s\}$ τα στοιχεία p_i και q_j δεν είναι προσαρτημένα. Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι

$$m = \deg p_1 \geq \ldots \geq \deg p_r, \quad n = \deg q_1 \geq \ldots \geq \deg q_s$$

και $n \geq m > 0$. Συμβολίζουμε με a και b τους συντελεστές των μεγιστοβαθμίων όρων των p_1 και q_1, αντίστοιχα. Θέτουμε

$$g = af - bp_1X^{n-m}q_2 \cdots q_s.$$

Έτσι, από την μία πλευρά έχουμε

$$g = ap_1 \cdots p_r - bp_1X^{n-m}q_2 \cdots q_s = p_1(ap_2 \cdots p_r - bX^{n-m}q_2 \cdots q_s)$$

και από την άλλη

$$g = aq_1 \cdots q_r - bp_1X^{n-m}q_2 \cdots q_s = (aq_1 - bp_1X^{n-m})q_2 \cdots q_s.$$

Αν $g \neq 0$, τότε $\deg(aq_1 - bp_1X^{n-m}) < \deg q_1$ και επομένως $\deg g < \deg f$. Έτσι, η γραφή του g σε γινόμενο αναγώγων παραγόντων του $A[X]$ είναι μοναδική. Έτσι, καθώς ο p_1 διαιρεί τον g και δεν είναι προσαρτημένος με κανένα από τους $q_2, \ldots, q_s$, από την Πρόταση 1.4(β′) έπεται ότι ο p_1 διαιρεί το $aq_1 - bp_1X^{n-m}$ και κατά συνέπεια διαιρεί το aq_1. Επίσης, αν $g = 0$, τότε $aq_1 - bp_1X^{n-m}$. Επομένως, και στις δύο περιπτώσεις υπάρχει $h \in A[X]$ τέτοιο, ώστε $aq_1 = p_1h$. Εφαρμόζοντας το Λήμμα 1.1 για κάθε ανάγωγο παράγοντα του a, καθώς κάθε μ.κ.δ. των συντελεστών του p_1 είναι αντιστρέψιμο στοιχείο του A, έπεται ότι το a διαιρεί το h. Άρα $h = ah_1$, όπου $h_1 \in A[X]$. Έτσι, έχουμε $q_1 = p_1h_1$ που είναι άτοπο γιατί τα p_1 και q_1 είναι ανάγωγα στοιχεία μη προσαρτημένα.

Πόρισμα 1.2 *Ας είναι A ένας δακτύλιος με μοναδική παραγοντοποίηση. Τότε ο δακτύλιος πολυωνύμων $A[X_1, \ldots, X_n]$ είναι επίσης δακτύλιος με μοναδική παραγοντοποίηση.*

Απόδειξη. Για $n = 1$ το Θεώρημα 1.1 δίνει το αποτέλεσμα. Ας υποθέσουμε ότι η προς απόδειξη πρόταση ισχύει για κάθε θετικό ακέραιο $< n$. Έχουμε $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$ και σύμφωνα με την υπόθεση της επαγωγής ο δακτύλιος $A[X_1, \ldots, X_{n-1}]$ είναι δακτύλιος με μοναδική παραγοντοποίηση. Επομένως, το Θεώρημα 1.1 συνεπάγεται ότι δακτύλιος πολυωνύμων $A[X_1, \ldots, X_n]$ είναι δακτύλιος με μοναδική παραγοντοποίηση.

Στη συνέχεια δίνουμε το παρακάτω θεώρημα που είναι γνωστό ως *κριτήριο αναγωγιμότητας του Eisenstein.*

Θεώρημα 1.2 *Ας είναι A ένας δακτύλιος με μοναδική παραγοντοποίηση, K το σώμα κλασμάτων του A και $f = a_nX^n + \cdots + a_0$ ένα πολυώνυμο του $A[X]$ βαθμού $n \geq 1$. Ας υποθέσουμε ότι υπάρχει ένα ανάγωγο στοιχείο p του A με $p|a_i$ $(i = 0, \ldots, n-1)$, $p \nmid a_n$ και $p^2 \nmid a_0$. Τότε το f είναι ανάγωγο μέσα στο $K[X]$.*

Για την απόδειξη του Θεωρήματος 1.2 θα χρησιμοποιήσουμε το παρακάτω λήμμα:

Λήμμα 1.2 *Ας είναι A ένας δακτύλιος με μοναδική παραγοντοποίηση, K το σώμα κλασμάτων του A και $f \in A[X] - A$. Αν $f = GH$ με $G, H \in K[X] - K$, τότε υπάρχουν $g, h \in A[X] - A$ έτσι, ώστε $f = gh$.*

Απόδειξη. Ας υποθέσουμε ότι υπάρχουν $G, H \in K[X] - K$ έτσι, ώστε $f = GH$. Τότε υπάρχουν $a, b \in A$ τέτοια, ώστε τα πολυώνυμα $g_1 = aG$ και $h_1 = bH$ ανήκουν στο $A[X]$. Έτσι, έχουμε $abf = g_1h_1$. Χρησιμοποιώντας το Λήμμα 1.1, για κάθε ανάγωγο διαιρέτη του ab, παίρνουμε ότι το ab διαιρεί το g_1h_1 και επομένως υπάρχουν $g, h \in A[X]$ έτσι, ώστε $f = gh$.

Απόδειξη του Θεωρήματος 1.2. Ας υποθέσουμε ότι το f δεν είναι ανάγωγο μέσα στο $K[X]$. Οπότε, σύμφωνα με το Λήμμα 1.2 υπάρχουν $g, h \in A[X] - A$ έτσι, ώστε $f = gh$. Θέτουμε

$$g = b_qX^q + \cdots + b_0, \quad h = c_mX^m + \cdots + c_0$$

με $q, m > 0$ και $b_q \neq 0$, $c_m \neq 0$. Καθώς το $a_0 = b_0c_0$ διαιρείται από το p, η Πρόταση 1.4(β′) μας δίνει ότι $p|b_0$ ή $p|c_0$. Από την άλλη πλευρά όμως η σχέση $p^2 \nmid a_0$, συνεπάγεται ότι κάποιο από τα στοιχεία b_0 και c_0 δεν διαιρείται από το p. Ας είναι $p \nmid b_0$ και $p|c_0$. Το p δεν διαιρεί το $a_n = b_qc_m$ και επομένως δεν διαιρεί κανένα από τα b_q και c_m. Ας είναι r ο πιο μικρός δείκτης τέτοιος, ώστε $p \nmid c_r$. Έχουμε

$$a_r = b_0c_r + b_1c_{r-1} + \cdots + b_rc_0$$

και $p|c_i$ $(i = 0, \ldots, r-1)$, $p \nmid c_r$, $p \nmid b_0$. Συνεπώς, το p δεν διαιρεί το a_r. Καθώς $r \leq m < n$, καταλήγουμε σε άτοπο. Συνεπώς, το f είναι ανάγωγο μέσα στο $K[X]$.

Παράδειγμα 1.3 Το πολυώνυμο $f = X^5 + 5X^3 + 125X^2 + 35$ είναι ανάγωγο μέσα στο $\mathbb{Q}[X]$. Πράγματι, όλοι οι συντελεστές του f, εκτός

του πρώτου, διαιρούνται με τον 5 και ο σταθερός δεν διαιρείται από τον 25. Έτσι, σύμφωνα με το κριτήριο του Eisenstein το f είναι ανάγωγο μέσα στο $\mathbb{Q}[X]$.

Τελειώνοντας την ενότητα, δίνουμε την παρακάτω πρόταση, σύμφωνα με την οποία οι διαιρέτες των ομογενών πολυωνύμων είναι επίσης ομογενή πολυώνυμα.

Πρόταση 1.5 *Ας είναι $F \in A[X_1, \ldots, X_n]$ ένα ομογενές πολυώνυμο και G ένας διαιρέτης του F. Τότε το πολυώνυμο G είναι επίσης ομογενές.*

Απόδειξη. Καθώς $G|F$, υπάρχει $E \in A[X_1, \ldots, X_n]$ με $F = GE$. Ας υποθέσουμε ότι το πολυώνυμο G δεν είναι ομογενές. Τότε

$$G = G_a + G_{a+k_1} + \cdots + G_{a+k_r}, \quad E = E_b + E_{b+l_1} + \cdots + E_{b+l_s},$$

όπου G_i και E_i είναι ομογενή πολυώνυμα βαθμού i, $0 < k_1 < \ldots < k_r$ και $0 \leq l_1 < \ldots < l_s$. Επομένως,

$$F = G_a E_b + G_{a+k_1} E_b + G_a E_{b+l_1} + \cdots + G_{a+k_r} E_{b+l_s}.$$

Καθώς ο δακτύλιος A είναι πεδίο ακεραιότητας, έχουμε $G_a E_b \neq 0$ και $G_{a+k_r} E_{b+l_s} \neq 0$. Επομένως

$$\deg(G_a E_b) = a + b < a + b + k_r + l_s = \deg(G_{a+k_r} E_{b+l_s}).$$

Άρα, το πολυώνυμο F δεν είναι ομογενές που είναι άτοπο. Συνεπώς, το G είναι ομογενές πολυώνυμο.

1.3 Ευκλείδεια Διαίρεση

Ας είναι A ένας αντιμεταθετικός δακτύλιος και f ένα πολυώνυμο του $A[X] - A$. Ένα στοιχείο $a \in A$ με $f(a) = 0$ καλείται *ρίζα* του f.

Θεώρημα 1.3 *Ας είναι f, g μη μηδενικά πολυώνυμα του $A[X]$. Αν ο συντελεστής του μεγιστοβαθμίου όρου του g είναι αντιστρέψιμο στοιχείο του A, τότε υπάρχουν $q, r \in A[X]$ έτσι, ώστε*

$$f = gq + r \quad \text{και} \quad \deg r < \deg g.$$

Απόδειξη. Αν $\deg f < \deg g$, τότε θέτουμε $q = 0$ και $r = f$. Ας υποθέσουμε λοιπόν ότι $m = \deg f \geq \deg g = n$. Θα εφαρμόσουμε την μέθοδο της επαγωγής επί του m. Συμβολίζουμε με a και b, αντίστοιχα, τους συντελεστές των μεγιστοβαθμίων όρων των g και f. Αν $m = 0$, τότε $f = b$ και $g = a$. Επομένως, για $q = a^{-1}b$ και $r = 0$ έχουμε $f = gq + r$.

Ας υποθέσουμε τώρα ότι $m > 0$ και ότι η προς απόδειξη πρόταση ισχύει για κάθε μη μηδενικό πολυώνυμο βαθμού $\leq m - 1$. Ο βαθμός του πολυωνύμου $af - bX^{m-n}g$ είναι $\leq m - 1$. Έτσι, σύμφωνα με την υπόθεση επαγωγής, υπάρχουν $q_1, r_1 \in A[X]$ έτσι, ώστε

$$af - bX^{m-n}g = gq_1 + r_1 \quad \text{και} \quad \deg r_1 < \deg g.$$

Επομένως

$$f = a^{-1}(bX^{m-n} + q_1)g + a^{-1}r_1.$$

Ας είναι (q_1, r_1), (q_2, r_2) δύο ζεύγη πολυωνύμων του $A[X]$ με

$$f = gq_i + r_i \quad \text{και} \quad \deg r_i < \deg g \quad (i = 1, 2).$$

Τότε $g(q_1 - q_2) = r_2 - r_1$ και επομένως

$$\deg g + \deg(q_1 - q_2) = \deg(r_2 - r_1) < \deg g.$$

Άρα $\deg(q_1 - q_2) < 0$ και κατά συνέπεια έχουμε $q_1 = q_2$. Έτσι, παίρνουμε $r_1 = f - gq_1 = f - qg_2 = r_2$.

Τα πολυώνυμα q και r του παραπάνω θεωρήματος καλούνται, αντίστοιχα, *πηλίκο* και *υπόλοιπο* της διαίρεσης του f διά g.

Παράδειγμα 1.4 Ας είναι $f = 2X^4 + X^2 + 1$ και $g = X^3 + X$ δύο πολυώνυμα του $\mathbb{Z}[X]$. Η διαίρεση του f διά g δίνει πηλίκο $q = 2X$ και υπόλοιπο $r = -X^2 + 1$.

Πόρισμα 1.3 *Ας είναι $f \in A[X]$ και $a \in A$. Τότε το a είναι ρίζα του f, αν και μόνον αν υπάρχει $q \in A[X]$ έτσι, ώστε $f = (X - a)q$.*

Απόδειξη. Σύμφωνα με το Θεώρημα 1.3, υπάρχει $q \in A[X]$ έτσι, ώστε $f = (X - a)q + r$ και $r \in A$. Οπότε, $r = 0$, αν και μόνον αν $f(a) = 0$.

Πόρισμα 1.4 *Ας υποθέσουμε ότι ο δακτύλιος A είναι ένα πεδίο ακεραιότητας και $f \in A[X] - A$. Τότε το πλήθος των διαφορετικών ριζών του f μέσα στο A είναι $\leq \deg f$.*

Απόδειξη. Ας είναι $\rho_1, \ldots, \rho_m$ όλες οι διαφορετικές ρίζες του f μέσα στο A. Θα δείξουμε, χρησιμοποιώντας επαγωγή επί του m, ότι υπάρχει $q \in A[X]$ έτσι, ώστε

$$f = (X - a_1) \cdots (X - a_m)q.$$

Για $m = 1$, αυτό προκύπτει από το Πόρισμα 1.1. Ας υποθέσουμε ότι υπάρχει $g \in A[X]$ έτσι, ώστε

$$f = (X - a_1) \cdots (X - a_{m-1})g.$$

Καθώς το A δεν έχει διαιρέτες του μηδενός, οι σχέσεις $f(a_m) = 0$ και $a_m - a_j \neq 0$ $(j = 1, \ldots, m-1)$ δίνουν $g(a_m) = 0$. Έτσι, από το Πόρισμα 1.1 έπεται ότι υπάρχει $p \in A[X]$ έτσι, ώστε $g = (X - a)p$. Αντικαθιστώντας στη παραπάνω ισότητα το g με το ίσο του παίρνουμε την ζητούμενη σχέση. Άρα ισχύει $m \leq \deg f$.

Ας είναι $f \in A[X] - A$ και $a \in A$ μία ρίζα του f. Τότε, σύμφωνα με το Πόρισμα 1.3, έχουμε $X - a | f$. Υπάρχει, λοιπόν, θετικός ακέραιος $h \leq \deg f$ τέτοιος, ώστε $(X - a)^h | f$ και $(X - a)^{h+1} \nmid f$. Ο ακέραιος h καλείται *πολλαπλότητα* της ρίζας a. Επομένως, το a είναι μία ρίζα πολλαπλότητας h του f, αν και μόνον αν υπάρχει $q \in A[X]$ τέτοιο, ώστε $f = (X - a)^h q$ και $X - a \nmid q$. Από το Πόρισμα 1.1 έπεται ότι η σχέση $X - a \nmid q$ ισοδυναμεί με $q(a) \neq 0$. Συνεπώς, το a είναι ρίζα πολλαπλότητας h του f, αν και μόνον αν υπάρχει $q \in A[X]$ τέτοιο, ώστε $f = (X - a)^h q$ και $q(a) \neq 0$.

Ας υποθέσουμε ότι ο δακτύλιος A είναι σώμα. Σύμφωνα με την Πρόταση 1.3, η ομάδα των αντιστρεψίμων στοιχείων του $A[X]$ είναι η $A - \{0\}$. Επομένως, δύο πολυώνυμα f και g είναι προσαρτημένα, αν και μόνον αν υπάρχει $u \in A - \{0\}$ με $f = ug$. Το Θεώρημα 1.3 μας δίνει μία συστηματική διαδικασία για την εύρεση ενός μ.κ.δ. δύο πολυωνύμων $f, g \in A[X]$, αντίστοιχη μ΄ αυτή του ευκλείδειου αλγόριθμου για την εύρεση του μ.κ.δ. δύο ακεραίων. Σύμφωνα, λοιπόν, με το Θεώρημα 1.3, υπάρχουν $q_j \in A[X]$ $(j = 1, \ldots, n)$ και $r_j \in A[X]$ $(j = 0, \ldots, n+1)$ τέτοια, ώστε $r_0 = f$, $r_1 = g$ και

$$r_{k-1} = q_k r_k + r_{k+1}, \quad \deg r_{k+1} < \deg r_k.$$

Έχουμε

$$\deg r_{n+1} < \deg r_n < \deg r_{n-1} < \ldots < \deg g$$

και επομένως για κάποιο δείκτη n ισχύει $r_j \neq 0$ $(j = 2, \ldots, n)$ και $r_{n+1} = 0$. Από την άλλη πλευρά, παρατηρούμε ότι τα σύνολα των κοινών διαιρετών των ζευγών r_{k-1}, r_k και r_k, r_{k+1} συμπίπτουν. Επομένως, τα δύο αυτά ζεύγη έχουν τους ίδιους μ.κ.δ.. Έτσι, καθώς το r_n διαιρεί το r_{n-1}, προκύπτει ότι κάθε μ.κ.δ. των f και g είναι προσαρτημένος στο r_n. Η παραπάνω διαδικασία είναι γνωστή ως *ευκλείδειος αλγόριθμος* για πολυώνυμα.

Εργαζόμενοι αντίστροφα, από τις σχέσεις

$$r_{k-1} = q_k r_k + r_{k+1} \quad (k = n-1, n-2),$$

έχουμε

$$r_n = A_{n-2} r_{n-2} + B_{n-3} r_{n-3},$$

όπου $A_{n-2} = 1 + q_{n-1} q_{n-2}$ και $B_{n-3} = -q_{n-1}$. Από την παραπάνω ισότητα και την σχέση $r_{n-4} = q_{n-3} r_{n-3} + r_{n-2}$ παίρνουμε

$$r_n = A_{n-3} r_{n-3} + B_{n-4} r_{n-4},$$

όπου $A_{n-3} = -A_{n-2} q_{n-3} + B_{n-3}$ και $B_{n-4} = A_{n-2}$. Συνεχίζοντας μ' αυτόν τον τρόπο βλέπουμε ότι υπάρχουν $a, b \in A[X]$ έτσι, ώστε

$$r_n = Af + Bg.$$

Καθώς κάθε μ.κ.δ. των f και g είναι προσαρτημένος στο r_n, προκύπτει η παρακάτω πρόταση.

Πρόταση 1.6 *Ας υποθέσουμε ότι ο δακτύλιος A είναι ένα σώμα. Αν d είναι ένας μ.κ.δ. των πολυωνύμων $f, g \in A[X]$, τότε υπάρχουν πολυώνυμα $u, v \in A[X]$ τέτοια, ώστε*

$$d = uf + vg.$$

Παράδειγμα 1.5 Θα βρούμε ένα μ.κ.δ. των πολυωνύμων $f = X^3 - \bar{1}$ και $g = X^2 + \bar{3}X + \bar{1}$ του $\mathbb{Z}_5[X]$ και θα τον εκφράσουμε ως γραμμικό συνδυασμό αυτών. Χρησιμοποιώντας τον ευκλείδειο αλγόριθμο έχουμε

$$X^3 - \bar{1} = (X^2 + \bar{3}X + \bar{1})(X + \bar{2}) + \bar{3}X + \bar{2},$$

$$X^2 + \bar{3}X + \bar{1} = (\bar{3}X + \bar{2})(\bar{2}X + \bar{3}).$$

Άρα, ένας μ.κ.δ των f και g είναι το πολυώνυμο $\bar{3}X + \bar{2}$. Επίσης, ισχύει

$$\bar{3}X + \bar{2} = X^3 - \bar{1} + (X^2 + \bar{3}X + \bar{1})(-X + \bar{3}).$$

Πρόταση 1.7 *Ας υποθέσουμε ότι ο δακτύλιος A είναι ένα άπειρο πεδίο ακεραιότητας και $S_1, \ldots, S_n$ άπειρα υποσύνολα του A. Αν f είναι πολυώνυμο του $A[X_1, \ldots, X_n]$ τέτοιο, ώστε $f(a_1, \ldots, a_n) = 0$ για κάθε $(a_1, \ldots, a_n) \in S_1 \times \cdots \times S_n$, τότε $f = 0$.*

Απόδειξη. Θα εφαρμόσουμε επαγωγή επί του n. Για $n = 1$, από το Πόρισμα 1.4 έχουμε $f = 0$. Ας υποθέσουμε ότι η πρόταση αληθεύει για $n = k$ και ότι το f είναι ένα μη μηδενικό πολυώνυμο του $A[X_1, \ldots, X_{k+1}] - A[X_1, \ldots, X_k]$. Τότε

$$f = f_0 + f_1 X_{k+1} + \cdots + f_s X_{k+1}^s,$$

με $s > 0$, $f_0, \ldots, f_s \in A[X_1, \ldots, X_k]$ και $f_s \neq 0$. Έτσι, σύμφωνα με την υπόθεση της επαγωγής, υπάρχει $(a_1, \ldots, a_k) \in S_1 \times \cdots \times S_k$ με $f_s(a_1, \ldots, a_k) \neq 0$. Από το Πορισμα 1.4 προκύπτει ότι το πολυώνυμο $f(a_1, \ldots, a_k, X_{k+1})$ μηδενίζεται για πεπερασμένο το πολύ πλήθος τιμών του X_{k+1}. Από την άλλη πλευρά, σύμφωνα με την υπόθεσή μας το $f(a_1, \ldots, a_k, X_{k+1})$ μηδενίζεται επί του απείρου συνόλου S_{k+1} που είναι άτοπο. Συνεπώς, $f = 0$ και έτσι η πρόταση αληθεύει και για $n = k+1$.

Παρατήρηση 1.1 Στη περίπτωση όπου το πεδίο ακεραιότητας A είναι πεπερασμένο η παραπάνω πρόταση δεν ισχύει. Για παράδειγμα, αν $A = \mathbb{Z}_p$ και $f = X^p - X$, τότε $f(a) = 0$ για κάθε $a \in A$ και $f \neq 0$.

1.4 Παραγώγιση Πολυωνύμων

Ας είναι A ένας αντιμεταθετικός δακτύλιος και

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n$$

ένα πολυώνυμο του $A[X]$. Καλούμε *τυπική παράγωγο* ή απλώς *παράγωγο* του $f(X)$ το πολυώνυμο

$$f'(X) = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}.$$

Πρόταση 1.8 *Ας είναι $f, g \in A[X]$. Τότε ισχύουν οι εξής ιδιότητες:*
(α) $(f+g)' = f' + g'$,
(β) $(fg)' = fg' + f'g$,
(γ) $(f^m)' = m f^{m-1} f'$, *για κάθε θετικό ακέραιο m.*

Απόδειξη. Ας είναι

$$f = a_0 + a_1X + \cdots + a_kX^k, \quad g = b_0 + b_1X + \cdots + b_lX^l$$

με $k \geq l$. Τότε

$$f' = a_1 + 2a_2X + \cdots + ka_kX^{k-1}, \quad g' = b_1 + 2b_1X + \cdots + lb_lX^{l-1}$$

και επομένως

$$f' + g' = \sum_{i=1}^{k} ia_iX^{i-1} + \sum_{i=1}^{l} ib_iX^{i-1} = \sum_{i=1}^{k} i(a_i + b_i)X^{i-1} = (f+g)'.$$

Άρα ισχύει η (α).

Για την απόδειξη της (β) έχουμε

$$\begin{aligned} fg' + f'g &= (\sum_{i=0}^{k} a_iX^i)(\sum_{j=1}^{l} jb_jX^{j-1}) + (\sum_{i=1}^{k} ia_iX^{i-1})(\sum_{j=0}^{l} b_jX^j) \\ &= \sum_{m=1}^{k+l} (\sum_{i+j=m} ja_ib_j)X^{m-1} + \sum_{m=1}^{k+l} (\sum_{i+j=m} ia_ib_j)X^{m-1} \\ &= \sum_{m=1}^{k+l} m(\sum_{i+j=m} a_ib_j)X^{m-1} = (fg)'. \end{aligned}$$

Για ν΄ αποδείξουμε την (γ) θα εφαρμόσουμε την μέθοδο της μαθηματικής επαγωγής επί του m. Η περίπτωση $m = 1$ είναι προφανής. Ας υποθέσουμε ότι ισχύει για $m = k \geq 1$. Τότε ισχύει $(f^k)' = kf^{k-1}f'$. Από αυτή την ισότητα και την (β) παίρνουμε

$$(f^{k+1})' = (f^kf)' = f^kf' + (f^k)'f = f^kf' + kf^kf' = (k+1)f^kf'.$$

Συνεπώς, ισχύει και η (γ).

Ορίζουμε την δεύτερη παράγωγο του $f(X)$ ως την παράγωγο του $f'(X)$. Γενικότερα, ορίζουμε επαγωγικά την n-οστή παράγωγο $f^{(n)}(X)$ του $f(X)$ ως την παράγωγο του $f^{(n-1)}(X)$.

Ας είναι $f(X_1, \ldots, X_n)$ ένα πολυώνυμο με συντελεστές στο A. Τότε

$$f(X_1, \ldots, X_n) = f_{i,0} + f_{i,1}X_i + \cdots + f_{i,d(i)}X_i^{d(i)},$$

όπου $f_{i,0}, \ldots, f_{i,d(i)} \in A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$. Καλούμε *τυπική παράγωγο* ή απλώς *παράγωγο* του $f(X_1, \ldots, X_n)$ ως προς την μεταβλητή X_i το πολυώνυμο

$$f_{X_i}(X_1, \ldots, X_n) = f_{i,1} + 2f_{i,2}X_i + \cdots + d(i)f_{i,d(i)}X_i^{d(i)-1}.$$

Ανάλογα ορίζουμε τις δεύτερες παραγώγους του $f(X_1, \ldots, X_n)$ τις οποίες συμβολίζουμε με $f_{X_iX_j}(X_1, \ldots, X_n)$, κ.ο.κ.

Πρόταση 1.9 *Ας είναι $f(X_1, \ldots, X_n)$ και $g_1(X), \ldots, g_n(X)$ πολυώνυμα με συντελεστές στο A. Τότε*

$$f(g_1(X), \ldots, g_n(X))' = \sum_{i=1}^{n} f_{X_i}(g_1(X), \ldots, g_n(X))g_i'(X).$$

Απόδειξη. Κατ' αρχάς ας υποθέσουμε ότι

$$f(X_1, \ldots, X_n) = X_1^{i_1} \cdots X_n^{i_n}.$$

Σύμφωνα με την Πρόταση 1.8(γ), η προς απόδειξη σχέση ισχύει για $n = 1$. Ας υποθέσουμε ότι ισχύει για $n = k \geq 1$. Αν $n = k + 1$, τότε θέτουμε

$$h(X_1, \ldots, X_k) = X_1^{i_1} \cdots X_k^{i_k}$$

και επομένως

$$f(g_1(X), \ldots, g_{k+1}(X))' = h(g_1(X), \ldots, g_k(X))'g_{k+1}(X)^{i_{k+1}} +$$
$$h(g_1(X), \ldots, g_k(X))i_{k+1}g_{k+1}(X)^{i_{k+1}-1}g_{k+1}'(X).$$

Από την υπόθεση επαγωγής, παίρνουμε

$$h(g_1(X), \ldots, g_k(X))' = \sum_{i=1}^{k} h_{X_i}(g_1(X), \ldots, g_k(X))g_i'(X).$$

Οπότε, καθώς για $i = 1, \ldots, k$ έχουμε

$$h_{X_i}(g_1(X), \ldots, g_k(X))g_{k+1}(X)^{i_{k+1}} = f_{X_i}(g_1(X), \ldots, g_{k+1}(X)),$$

έπεται

$$f(g_1(X), \ldots, g_{k+1}(X))' = \sum_{i=1}^{k+1} f_{X_i}(g_1(X), \ldots, g_{k+1}(X))g_i'(X).$$

Ας είναι τώρα

$$f(X_1,\dots,X_n)=\sum_{j=1}^{k} f_j(X_1,\dots,X_n),$$

όπου τα $f_j(X_1,\dots,X_n)$ είναι μονώνυμα. Συμφωνα με τα παραπάνω, έχουμε

$$\begin{aligned} f(g_1(X),\dots,g_n(X))' &= \sum_{j=1}^{k} f_j(g_1(X),\dots,g_n(X)),\\ &= \sum_{j=1}^{k}\sum_{i=1}^{n}(f_j)_{X_i}(g_1(X),\dots,g_n(X))g_i'(X),\\ &= \sum_{i=1}^{n} f_{X_i}(g_1(X),\dots,g_n(X))g_i'(X). \end{aligned}$$

Πρόταση 1.10 *Ας υποθέσουμε ότι A είναι ένα σώμα χαρακτηριστικής 0, $g(T)$ ένα πολυώνυμο του $A[T]$ βαθμού d και $a\in A$. Τότε*

$$g(T+a)=g(a)+Tg'(a)+\frac{1}{2!}T^2g^{(2)}(a)+\cdots+\frac{1}{d!}T^dg^{(d)}(a).$$

Απόδειξη. Ας είναι

$$g(T+a)=a_0+a_1T+\cdots+a_dT^d.$$

Τότε

$$\begin{aligned} g'(T+a) &= a_1+2a_2T+\cdots+da_dT^{d-1},\\ g^{(2)}(T+a) &= 2a_2+6a_3T+\cdots+d(d-1)a_dT^{d-2},\\ \dots &\quad \dots\\ g^{(d)}(T+a) &= d!a_d. \end{aligned}$$

Θέτοντας $T=0$, παίρνουμε

$$a_0=g(a),\quad a_1=g'(a),\quad a_2=\frac{1}{2!}g^{(2)}(a),\quad \dots,\quad a_d=\frac{1}{d!}g^{(d)}(a).$$

Πρόταση 1.11 *Ας υποθέσουμε ότι A είναι ένα σώμα χαρακτηριστικής 0, $f(X_1,\dots,X_n)\in A[X_1,\dots,X_n]$ και $a=(a_1,\dots,a_n)\in A^n$. Τότε*

$$\begin{aligned} &f(X_1+a_1,\dots,X_n+a_n)=\\ &\qquad f(a)+\sum_{i=1}^{n} f_{X_i}(a)X_i+\frac{1}{2!}\sum_{i,j} f_{X_iX_j}(a)X_iX_j+\cdots \end{aligned}$$

Απόδειξη. Ας είναι $(x_1, \ldots, x_n) \in A^n$. Θέτουμε

$$g(T) = f(Tx_1 + a_1, \ldots, Tx_n + a_n)$$

και $\deg g = d$. Από την Πρόταση 1.10 έχουμε

$$g(T) = g(0) + Tg'(0) + \frac{1}{2!}T^2 g^{(2)}(0) + \cdots + \frac{1}{d!}T^d g^{(d)}(0).$$

Έχουμε $g(0) = f(a_1, \ldots, a_n)$. Η Πρόταση 1.9 δίνει

$$\begin{aligned} g'(0) &= f(Tx_1 + a_1, \ldots, Tx_n + a_n)'(0) \\ &= (\sum_{i=1}^{n} f_{X_i}(Tx_1 + a_1, \ldots, Tx_n + a_n)x_i)(0) \\ &= \sum_{i=1}^{n} f_{X_i}(a_1, \ldots, a_n)x_i. \end{aligned}$$

Ομοίως υπολογίζουμε και τις ποσότητες $g^{(2)}(0), \ldots, g^{(d)}(0)$. Οπότε, για $T = 1$ παίρνουμε

$$\begin{aligned} &f(x_1 + a_1, \ldots, x_n + a_n) = \\ &\quad f(a) + \sum_{i=1}^{n} f_{X_i}(a)x_i + \frac{1}{2!}\sum_{i,j} f_{X_i X_j}(a)x_i x_j + \cdots, \end{aligned}$$

απ' όπου, χρησιμοποιώντας την Πρόταση 1.7, προκύπτει το ζητούμενο.

Η παρακάτω πρόταση είναι γνωστή ως λήμμα του Euler.

Πρόταση 1.12 *Ας υποθέσουμε ότι ο δακτύλιος A είναι ένα πεδίο ακεραιότητας χαρακτηριστικής 0 και $F \in A[X_1, \ldots, X_n]$ ένα ομογενές πολυώνυμο βαθμού $d \geq 1$. Τότε*

$$dF(X_1, \ldots, X_n) = \sum_{k=1}^{n} X_k F_{X_k}(X_1, \ldots, X_n).$$

Απόδειξη. Καθώς το πολυώνυμο F είναι ομογενές, από την Πρόταση 1.2 έχουμε την ισότητα

$$F(TX_1, \ldots, TX_n) = T^d F(X_1, \ldots, X_n)$$

στο $A[X_1, \ldots, X_n, T]$. Οπότε για κάθε $(x_1, \ldots, x_n) \in A^n$ ισχύει

$$F(Tx_1, \ldots, Tx_n) = T^d F(x_1, \ldots, x_n).$$