1 Δακτύλιος Πολυωνύμων

Ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο λέγεται **ακέραια περιοχή** αν δεν έχει διαιρέτες του μηδενός, δηλαδή αν $ab = 0$ τότε $a = 0$ ή $b = 0$. Έστω D ακέραια περιοχή, ένα **πολυώνυμο** $f(x) = a_0 + a_1x + ... + a_nx^n$ είναι ένα πεπερασμένο τυπικό άθροισμα με $a_i \in D$. Το σύμβολο x λέγεται απροσδιόριστη ή μεταβλητή και τα a_i λέγονται συντελεστές του $f(x)$. Το σύνολο όλων των πολυωνύμων με συντελεστές από το D συμβολίζεται με $D[x]$. Αν για κάποιο $i > 0$ ισχύει $a_i \neq 0$, η μεγαλύτερη τέτοια τιμή του i λέγεται **βαθμός** του $f(x)$ και συμβολίζεται με $degf$. Αν δεν υπάρχει τέτοιο $i > 0$, τότε λέμε ότι το $f(x)$ είναι βαθμού μηδέν (ή σταθερό πολυώνυμο)[1] Δύο πολυώνυμα $f(x) = a_0 + a_1x + ... + a_nx^n$ και $g(x) = b_0 + b_1x + ...b_nx^n$ θεωρούνται ίσα αν ισχύει $a_i = b_i$ για κάθε i.
Άθροισμα δύο πολυωνύμων $f(x) = a_0+a_1x+...+a_nx^n$ και $g(x) = b_0+b_1x+...b_mx^m$ με $n \geq m$ λέγεται το πολυώνυμο

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_n + b_n)x^n$$

όπου $b_j = 0$ για $j > m$.
Γινόμενο δύο πολυωνύμων $f(x) = a_0 + a_1x + ... + a_nx^n$ και $g(x) = b_0 + b_1x + ...b_mx^m$ λέγεται το πολυώνυμο

$$f(x)g(x) = (a_0b_0) + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + ... + (a_nb_m)x^{n+m}.$$

Επειδή το D είναι ακέραια περιοχή για $f \neq 0, g \neq 0$ ισχύει ότι $degf + degg = degfg$.
Με τις προηγούμενες πράξεις το σύνολο των πολυωνύμων $D[x]$ είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο το μοναδιαίο στοιχείο του D.

Θεώρημα 2.1 *Αν D ακέραια περιοχή τότε και $D[x]$ είναι ακέραια περιοχή.*

Απόδειξη Υποθέτουμε ότι $D[x]$ δεν είναι ακέραια περιοχή, τότε $D[x]$ έχει διαιρέτες του μηδενός. Αν για $f, g \in D[x]$ με $f \neq 0$, $g \neq 0$ ισχύει $fg = 0$ τότε $degf + degg = degfg = 0$. Άρα $degf = 0$ και $degg = 0$. Δηλαδή $0 \neq f \in D$ και $0 \neq g \in D$ και $fg = 0$ άρα η D έχει μηδενοδιαιρέτες, που είναι άτοπο αφού D είναι ακέραια περιοχή. Καταλήξαμε σε άτοπο άρα η $D[x]$ είναι ακέραια περιοχή.

[1] Με τον τρόπο αυτό θεωρούμε το μηδενικό πολυώνυμο ως πολυώνυμο βαθμού μηδέν. Στην βιβλιογραφία εμφανίζονται τρείς διαφορετικές θεωρήσεις για τον βαθμό του μηδενικού πολυωνύμου: 1. έχει βαθμό μηδέν 2. δεν έχει βαθμό 3. έχει βαθμό $-\infty$. Οποιαδήποτε απ' αυτές θεωρείται σωστή αρκεί να προσέξει κανείς τη συμβατότητα στην διατύπωση των Θεωρημάτων και των αποδείξεων.

2 Διαίρεση Πολυωνύμων και Περιοχές Μονοσήμαντης Ανάλυσης

Έστω D ακέραια περιοχή και $f(x) = a_0 + a_1x + ... + a_nx^n \in D[x]$ πολυώνυμο βαθμού n, δηλαδή $a_n \neq 0$.

Θεώρημα 2.2 Αν f και g είναι πολυώνυμα του $D[x]$ με $g \neq 0$ τότε υπάρχει $0 \neq a \in D$ και πολυώνυμα q και r με $degr < degg$ ή $r = 0$ αν $degg = 0$, τέτοια ώστε $af = qg + r$.
Το q λέγεται πηλίκο και το r υπόλοιπο.

Απόδειξη Αν $degg = 0$, δηλαδή g σταθερά διάφορη του μηδενός τότε $a = g, q = f, r = 0$. Άρα μπορούμε να υποθέσουμε ότι $degg > 0$. Θα αποδείξουμε το θεώρημα με επαγωγή στο βαθμό του f. Αν $degf < degg$ τότε $q = 0$ και $f = r, a = 1$. Άρα ισχύει για $degf < degg$ (άρα και για $degf = 0$). Υποθέτουμε ότι το θεώρημα ισχύει για όλους τους βαθμούς μικρότερους του n και θα δείξουμε ότι ισχύει για n. Έστω $f(x) = a_0 + a_1x + ... + a_nx^n$ και $g(x) = b_0 + b_1x + ... + b_mx^m$ με $n \geq m$ και $a_n \neq 0 \neq b_m$. Τότε το πολυώνυμο $b_mf - a_ngx^{n-m}$ έχει $deg(b_mf - a_ngx^{n-m}) < degf$. Άρα από την υπόθεση της μαθηματικής επαγωγής υπάρχουν a', q', r με $degr < degg$ τέτοια ώστε $a'(b_mf - a_ngx^{n-m}) = q'g + r$ και άρα $a'b_mf = (a'a_nx^{n-m} + q')g + r$, που αποδεικνύει το θεώρημα.

Έστω D ακέραια περιοχή και $a, b \in D$. Αν υπάρχει $c \in D$ τέτοιο ώστε $b = ac$ τότε λέμε ότι το a είναι παράγοντας του b ή ότι το a διαιρεί το b ή ότι το b διαιρείται από το a και γράφουμε $a|b$. Για την διαίρεση ισχύουν οι παρακάτω ιδιότητες:

1. Αν $a|b$ και $b|c$ τότε $a|c$.
2. Αν $a|b$ και $a|c$ τότε $a|(rb + sc)$, για κάθε $r, s \in D$.
3. $a|0$ για κάθε $a \in D$.
4. Αν $b = ac$ και $b \neq 0$ τότε το c είναι μοναδικό.

Ορισμός 2.3 Ένα στοιχείο λέγεται **μονάδα** του D αν έχει πολλαπλασιαστικό αντίστροφο.

Παράδειγμα Στο $\mathbb{Q}$, όπως και σε κάθε σώμα, κάθε στοιχείο διαφορετικό του μηδενός είναι μονάδα. Στο $\mathbb{Z}$, τον δακτύλιο των ακεραίων, μονάδες είναι μόνο το 1 και το -1. Στον δακτύλιο πολυωνύμων $D[x]$ μονάδες είναι μόνο οι μονάδες του D.

Ορισμός 2.4 Δύο στοιχεία a, b λέγονται **ισοδύναμα** αν $a = bu$, όπου u είναι μονάδα.

Ορισμός 2.5 Ένα μη μηδενικό στοιχείο p που δεν είναι μονάδα της ακεραίας περιοχής D λέγεται **ανάγωγο** στοιχείο του D, αν σε κάθε ανάλυση $p = ab$ του p στον D, το a ή το b είναι μονάδα.

Παράδειγμα 2.6 Στο $\mathbb{Z}$ τα ανάγωγα στοιχεία είναι της μορφής $p, -p$ όπου p είναι πρώτος αριθμός. Το πολυώνυμο $x^2 + 1$ είναι ανάγωγο στον $\mathbb{R}[x]$, αλλά δεν είναι ανάγωγο στον $\mathbb{C}[x]$. Το πολυώνυμο $y^2 - x^3$ είναι ανάγωγο στον $\mathbb{R}[x, y]$.

Ορισμός 2.7 Μια ακέραια περιοχή D λέγεται **Περιοχή Μονοσήμαντης Ανάλυσης ΠΜΑ)** αν:

α) Κάθε στοιχείο της D που δεν είναι μηδέν ή μονάδα, αναλύεται σε γινόμενο πεπερασμένου πλήθους αναγώγων στοιχείων και

β) Αν $p_1p_2...p_r = q_1q_2...q_s$ είναι δύο αναλύσεις του ίδιου στοιχείου σε γινόμενο αναγώγων τότε $r = s$ και μπορούμε να τα αριθμήσουμε ξανά ώστε τα p_i και q_i να είναι ισοδύναμα, για κάθε $1 \leq i \leq r = s$.

Παράδειγμα 2.8 Κάθε σώμα είναι ΠΜΑ επειδή κάθε στοιχείο του είναι μηδέν ή μονάδα. Το $\mathbb{Z}$ είναι ΠΜΑ. Το Θεώρημα 2.2.16 δίνει πολλά σημαντικά παραδείγματα ΠΜΑ, όπως το $K[x], K[x, y], K[x_1, x_2, ..., x_n]$ όπου K είναι τυχαίο σώμα ή το $\mathbb{Z}[x], \mathbb{Z}[x, y], \mathbb{Z}[x_1, x_2, ..., x_n]$.
Στην συνέχεια του κεφαλαίου αυτού το D θα σημαίνει πάντα Περιοχή Μονοσήμαντης Ανάλυσης.

Θεώρημα 2.9 Αν $a \in D$ διαιρεί το πολυώνυμο $f(x) = a_0 + a_1x + ... + a_nx^n$, τότε το a διαιρεί κάθε συντελεστη a_i του f.

Απόδειξη Αφού $a|f$ υπάρχει πολυώνυμο $g(x) = b_0 + b_1x + ... + b_nx^n$ τέτοιο ώστε $f = ag$. Άρα $a_0 + a_1x + ... + a_nx^n = a(b_0 + b_1x + ... + b_nx^n)$. Δηλαδή $a_i = ab_i$, που σημαίνει ότι το a διαιρεί κάθε συντελεστή a_i του f.

Θεώρημα 2.10 Αν $a, b, c \in D$ με a ανάγωγο και $a|bc$, τότε $a|b$ ή $a|c$.

Απόδειξη Αφού $a|bc$ υπάρχει $d \in D$ τέτοιο ώστε $ad = bc$. Η περιοχή D είναι ΠΜΑ και αν αναλύσουμε τα b, c, d σε γινόμενο αναγώγων στοιχείων (όσα δεν είναι μη-

δέν ή μονάδες) έχουμε $ad_1...d_s = b_1...b_nc_1...c_m$. Το a είναι ανάγωγο άρα θα πρέπει να υπάρχει κάποιο b_i ή c_j που να είναι ισοδύναμο με το a. Αλλά τότε το $a|b$ ή $a|c$ αντίστοιχα.

Θεώρημα 2.11 Έστω $a \in D$ είναι ανάγωγο και $f, g \in D[x]$. Αν $a|fg$ τότε $a|f$ ή $a|g$.

Απόδειξη Έστω $f(x) = a_0 + a_1x + ... + a_nx^n$, $g(x) = b_0 + b_1x + ... + b + mx^m$ και υποθέτουμε ότι το a δεν διαιρεί ούτε το f και ούτε το g. Θα καταλήξουμε σε άτοπο. Αφού το a δεν διαιρεί το f υπάρχει τουλάχιστον ένα i τέτοιο ώστε το a δεν διαιρεί το a_i. Έστω p το μικρότερο τέτοιο i, δηλαδή το a δεν διαιρεί το a_p αλλά $a|a_i$ για κάθε $i < p$. Όμοια υπάρχει q τέτοιο ώστε το a δεν διαιρεί το b_q αλλά $a|b_i$ για κάθε $i < q$. Ο συντελεστής του x^{p+q} στο fg είναι
$a_0b_{p+q} + a_1b_{p+q-1} + ... + a_{p-1}b_{q+1} + a_pb_q + a_{p+1}b_{q-1} + ... + a_{p+q}b_0$, όπου $a_i = 0$ για $i > n$ και $b_j = 0$ για $j > m$. Το a διαιρεί το συντελεστή, αφού διαιρεί το fg. Επίσης το a διαιρεί το $a_0b_{p+q} + a_1b_{p+q-1} + ... + a_{p-1}b_{q+1}$, αφού $a|a_i$ για κάθε $i < p$, και το a διαιρεί το $a_{p+1}b_{q-1} + ... + a_{p+q}b_0$, αφού $a|b_i$ για κάθε $i < q$. Τότε όμως $a|a_pb_q$ και επειδή a ανάγωγο θα ισχύει $a|a_p$ ή $a|b_q$ που είναι άτοπο. Άρα το $a|f$ ή $a|g$.

Θεώρημα 2.12 Έστω K το σώμα πηλίκων του D. Αν $f \notin D$ και είναι ανάγωγο στο $D[x]$ τότε είναι ανάγωγο στο $K[x]$.

Απόδειξη Ας υποθέσουμε ότι το f δεν είναι ανάγωγο στο $K[x]$. Τότε $f = g_1h_1$ όπου $g_1, h_1 \in K[x]$ και κανένα από τα g_1, h_1 δεν είναι μονάδες. Ισχύει $g_1 \notin K$, $h_1 \notin K$, αφού οι μονάδες του $K[x]$ είναι ακριβώς τα στοιχεία του K που είναι διαφορετικά του μηδενός. Έστω $g_1(x) = b_{10} + b_{11}x + ... + b_{1m}x^m$ και $h_1(x) = c_{10} + c_{11}x + ... + c_{1n}x^n \in D$. Τα b_{1i} και c_{1j} είναι πηλίκα στοιχείων του D, άρα υπάρχουν b, c του D (κάποιοι κοινοί παρανομαστές των b_{1i} και c_{1j} αντίστοιχα) τέτοιοι ώστε $bg_1, ch_1 \in D[x]$. Έχουμε $bcf = (bg_1)(ch_1) = gh$ στον $D[x]$, όπου $g = bg_1$ και $h = ch_1$. Έστω e ανάγωγος παράγοντας του bc, τότε $e|bcf = gh$ άρα $e|g$ ή $e|h$. Αν $e|g$ τότε $g = eg'$ με $g' \in D[x]$. Άρα $\frac{bc}{e}f = g'h$ στον $D[x]$. Συνεχίζοντας με τον ίδιο τρόπο απαλείφουμε όλους τους ανάγωγους παράγοντες του bc, και έχουμε $f = GH$ στον $D[x]$ για κάποια G, H. Όμως f είναι ανάγωγο στον $D[x]$, άρα κάποιο από τα G, H είναι μονάδα του $D[x]$. Ώστε ο βαθμός του G ή του H πρέπει να είναι μηδέν. Όμως στην παραπάνω διαδικασία βγάζαμε μόνο παράγοντες από το D, άρα ο βαθμός των πολυωνύμων δεν άλλαζε. Καταλήγουμε ότι ο βαθμός του $g_1(x)$ ή του $h_1(x)$ είναι μηδέν, που είναι άτοπο γιατί τότε $g_1(x) \in K$ ή $h_1(x) \in K$.

Θεώρημα 2.13 Αν $f, g \in K[x]$ τότε υπάρχει $h \in K[x]$ τέτοιο ώστε:

(ι) $h|f$ και $h|g$,

(ιι) αν $q|f$ και $q|g$ τότε $q|h$,

(iii) υπάρχουν $A, B \in K[x]$ τέτοια ώστε $h = Af + Bg$.

Απόδειξη Διαιρούμε το f με το g και παίρνουμε υπόλοιπο r. Συνεχίζουμε διαιρώντας σε κάθε νέα διαίρεση τον προηγούμενο διαιρέτη με το υπόλοιπο και παίρνουμε

$$f = q_1 g + r_1$$

$$g = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

$$...$$

$$r_{p-2} = q_p r_{p-1} + r_p$$

$$r_{p-1} = q_{p+1} r_p + 0.$$

Στην παραπάνω διαδικασία ο βαθμός του υπολοίπου συνεχώς φθίνει άρα μετά από κάποια βήματα θα γίνει μηδέν. Το h του θεωρήματος είναι το r_p. Πράγματι το $r_p | r_{p-1}$ από την τελευταία εξίσωση. Αφού $r_p | r_{p-1}$ η προτελευταία εξίσωση μας δίνει ότι $r_p | r_{p-2}$. Συνεχίζοντας προς τα πάνω η δεύτερη εξίσωση μας δίνει ότι $r_p | g$ και η πρώτη $r_p | f$.
Αν $q | f$ και $q | g$ τότε από την πρώτη εξίσωση προκύπτει ότι $q | r_1$. Αφου $q | g$ και $q | r_1$ από την δεύτερη εξίσωση προκύπτει ότι $q | r_2$. Συνεχίζοντας από την προτελευταία εξίσωση προκύπτει ότι $q | r_p$.
Λύνοντας την πρώτη εξίσωση ως προς το r_1, προκύπτει το r_1 σαν γραμμικός συνδυασμός των f, g με συντελεστές πολυώνυμα. Αντικαθιστώντας το r_1 στην δεύτερη και λύνοντας την δεύτερη εξίσωση ως προς το r_2, προκύπτει το r_2 σαν γραμμικός συνδυασμός των f, g με συντελεστές πολυώνυμα. Συνεχίζοντας με τον ίδιο τρόπο γράφουμε το r_p σαν γραμμικό συνδυασμό των f, g, δηλαδή $Af + Bg$, όπου $A, B \in K[x]$.
Παρατηρούμε ότι το h είναι ένας μέγιστος κοινός διαιρέτης των f, g και δεν είναι μοναδικός. Όταν όμως έχουμε δύο μέγιστους κοινούς διαιρέτες αυτοί είναι ισοδύναμοι, από την (i) και (ii).

Θεώρημα 2.14 Έστω $f, g, q \in K[x]$ με f ανάγωγο, τότε αν $f | gq$ συνεπάγεται $f | g$ ή $f | q$.

Απόδειξη Έστω $f | gq$ και το f δεν διαιρεί το g. Από το προηγούμενο θεώρημα, για τα f, g υπάρχει $h \in K[x]$ τέτοιο ώστε να ισχύουν τα $(i), (ii), (iii)$. Επειδή το f είναι ανάγωγο, είναι διάφορο του μηδενός, άρα από το (i) το h είναι διάφορο του μηδενός. Από την (i) έχουμε το $h | f$ και f ανάγωγο, άρα το h είναι μονάδα ή ισοδύναμο με το f. Αν όμως h είναι ισοδύναμο με το f τότε επειδή $h | g$ έχουμε $f | g$ που δεν ισχύει. Ώστε το h είναι μονάδα και άρα υπάρχουν $A, B \in K[x]$ τέτοια ώστε $1 = Af + Bg$, αφού $1, h$ είναι ισοδύναμα. Πολλαπλασιάζοντας την ισότητα $1 = Af + Bg$ με q έχουμε $q = Afq + Bgq$. Αλλά $f | gq$ και $f | Afq$, άρα $f | Afq + Bgq = q$.

Θεώρημα 2.15 Έστω $f, g, q \in D[x]$ με f ανάγωγο, τότε αν $f|gq$ συνεπάγεται $f|g$ ή $f|q$.

Απόδειξη Αν το $f \in D$, τότε το θεώρημα έχει ήδη αποδειχθεί. Αν $f \notin D$, τότε το f είναι ανάγωγο στο $D[x]$ άρα είναι ανάγωγο και στο $K[x]$. Από το προηγούμενο θεώρημα έχουμε ότι $f|g$ ή $f|q$ στο $K[x]$. Έστω ότι $f|g$ τότε υπάρχει $l \in K[x]$ τέτοιο ώστε $g = lf$. Όμως $l \in K[x]$ άρα υπάρχει $a \in D$, ένας κοινός παρονομαστής όλων των συντελεστών του l, έτσι ώστε $al \in D[x]$. Ώστε $ag = (al)f$ στο $D[x]$. Έστω e ανάγωγος παράγοντας του a και $a = ea_1$. Τότε $e|ag = (al)f$, αλλά το e δεν διαιρεί το f αφού f ανάγωγο και $f \notin D$. Άρα $e|al$, δηλαδή $\frac{al}{e} = a_1 l \in D[x]$. Άρα $a_1 g = (a_1 l)f$ στο $D[x]$. Συνεχίζοντας με τον ίδιο τρόπο ώσπου να μη μείνει ανάγωγος παράγοντας καταλήγουμε $g = lf$ στο $D[x]$.

Θεώρημα 2.16 Αν D είναι περιοχή μονοσήμαντης ανάλυσης τότε και $D[x]$ είναι περιοχή μονοσήμαντης ανάλυσης.

Απόδειξη Έστω $f \in D[x]$. Αν το $f \in D$ τότε δεν έχουμε τίποτα να αποδείξουμε αφού D είναι ΠΜΑ. Άρα μπορούμε να υποθέσουμε ότι το f είναι πολυώνυμο βαθμού $n > 0$. Το f μπορεί να έχει διαιρέτες που είναι στοιχεία του D, είτε πολυώνυμα βαθμού > 0. Αν το f δεν είναι ανάγωγο τότε υπάρχουν f_1, f_2 έτσι ώστε $f = f_1 f_2$ με $f_1, f_2 \in D[x]$ και κανένα δεν είναι μονάδα. Για τους βαθμούς έχουμε $degf = degf_1 + degf_2$. Άρα ή ένα από τα δύο έχει βαθμό μηδέν ή ο βαθμός και των δύο πολυωνύμων είναι μικρότερος του βαθμού του f. Συνεχίζουμε έτσι στην περίπτωση που ένα τουλάχιστον από τα f_1, f_2 δεν είναι ανάγωγο. Σε κάθε βήμα είτε χαμηλώνει ο βαθμός των παραγόντων είτε βγαίνει ένας παράγοντας από τον συντελεστή του μεγιστοβάθμιου του f. Και επειδή κανένα από τα παραπάνω δεν μπορεί να συνεχίζεται επ άπειρο η διαδικασία καταλήγει σε πεπερασμένους ανάγωγους παράγοντες.
Αν $p_1 p_2 ... p_r = q_1 q_2 ... q_s$ είναι δύο αναλύσεις του ίδιου στοιχείου του $D[x]$ σε γινόμενο αναγώγων τότε το p_1 διαιρεί το $q_1 q_2 ... q_s$ άρα διαιρεί κάποιο από τα $q_1, q_2, ..., q_s$. Αν χρειαστεί τα ξανα-αριθμούμε και μπορούμε να υποθέσουμε ότι διαιρεί το q_1. Όμως τα p_1, q_1 είναι ανάγωγα και το πρώτο διαιρεί το δεύτερο, άρα p_1, q_1 ισοδύναμα. Ώστε $p_2 ... p_r = u_1 q_2 ... q_s$, όπου u_1 μονάδα. Εργαζόμαστε όπως και πριν: Το p_2 διαιρεί το $q_2 ... q_s$ άρα διαιρεί κάποιο από τα $q_2, ..., q_s$ ξανα-αριθμώντας τα αν χρειαστεί μπορούμε να υποθέσουμε ότι διαιρεί το q_2. Όμως τα p_2, q_2 είναι ανάγωγα και το πρώτο διαιρεί το δέυτερο, άρα p_2, q_2 ισοδύναμα. Συνεχίζουμε έτσι μέχρι το p_r και έχουμε $p_r = u_{r-1} q_r ... q_s$. Αλλά p_r ανάγωγο, συνεπώς $r = s$.

3 Θεώρημα του Fermat και Περιοχές Μονοσήμαντης Ανάλυσης

Ο Γάλλος δικηγόρος και μαθηματικός *Pierre de Fermat* (1601-1665). Ασχολήθηκε, όπως πολλοί μαθηματικοί της εποχής του, με το να κατανοήσει αλλά και να συμπληρώσει-διορθώσει και επεκτείνει μαθηματικά κείμενα των Απολλώνιου, Αρχιμήδη και Διόφαντου. Οι εργασίες αυτών των μαθηματικών της αρχαιότητας, όσες διεσώθηκαν μέχρι την εποχή του *Fermat*, συχνά ήταν μερικώς κατεστραμμένες ή και λανθασμένες από τους δεκάδες αντιγραφείς και μερικές φορές από ατυχείς μεταγλωττίσεις που μεσολάβησαν ως τότε. Ο *Fermat* συνδύασε την μελέτη των Ελλήνων Μαθηματικών με τις αλγεβρικές μεθόδους του *Vieta* (1540-1603). Εργάστηκε στην Αναλυτική Γεωμετρία και στον Διαφορικό Λογισμό αλλά η κύρια συμβολή του ήταν στη Θεωρία των Αριθμών.

Το 1635 ο *Fermat* διαβάζοντας το όγδοο πρόβλημα του δεύτερου βιβλίου της Αριθμητικής του Διόφαντου διατύπωσε στο περιθώριο του βιβλίου την πρόταση που σήμερα ονομάζεται τελευταίο θεώρημα του *Fermat*[2]:

Θεώρημα 3.1 *Δεν υπάρχουν ακέραιοι μη μηδενικοί αριθμοί x, y, z τέτοιοι ώστε να ικανοποιείται η σχέση $x^n + y^n = z^n$ για $n \geq 3$.*

Ο *Fermat* απέδειξε την πρόταση αυτή για $n = 4$ με την μέθοδο της άπειρης καθόδου [3] και αργότερα ο *Euler* έδωσε την απόδειξη για $n = 3$ και $n = 4$. Παρακάτω σκιαγραφείται η μέθοδος του *Fermat* της άπειρης καθόδου.
Ο *Fermat* ονομάζει ύψος h της τριάδας ακεραίων (x, y, z) τον μέγιστο αριθμό απο τους $|x|, |y|, |z|$ και αποδεικνύει ότι αν η τριάδα ακεραίων (x_1, y_1, z_1) ικανοποιεί την σχέση $x^4 + y^4 = z^4$ τότε υπάρχει μια άλλη τριάδα ακεραίων (x_2, y_2, z_2) με ύψος $h_2 < h_1$ που ικανοποιεί την σχέση $x^4 + y^4 = z^4$. Επειδή όμως οι φυσικοί που είναι μικρότεροι του h_1 είναι πεπερασμένοι σε πλήθος, η σχέση $x^4 + y^4 = z^4$ δεν μπορεί να ικανοποιείται απο καμιά τριάδα ακεραίων αριθμών.

Οι *Dirichlet*(1828) και *Legendre*(1830), ανεξάρτητα ο ένας από τον άλλον, απέδειξαν την πρόταση για $n = 5$. Το 1832 ο *Legendre* απέδειξε το Θεώρημα του *Fermat* για $n = 14$. Το 1837 ο *Lame* έδωσε την απόδειξη για $n = 7$ και δέκα χρόνια αργότερα έδωσε μια λάθος απόδειξη της γενικής πρότασης του *Fermat*. Το λάθος που έκανε ο *Lame* ήταν να υποθέσει ότι η μονοσήμαντη ανάλυση σε γινόμενο πρώτων που ισχύει στους ακεραίους ισχύει και σε πιο γενικούς δακτύλιους. Κάτι που δεν ισχύει, όπως φαίνεται για παράδειγμα στον δακτύλιο

$$\mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} | m, n \in \mathbb{Z}\}$$

[2] Ο *Fermat* έκανε πολλές εικασίες στα Μαθηματικά. Στα επόμενα 200 χρόνια όλες οι εικασίες αποδείχτηκαν και θεωρήθηκαν Θεωρήματα, εκτός από μία που και για αυτό έμεινε στην Ιστορία σαν το τελευταίο θεώρημα του *Fermat*.

[3] Η πρόταση για $n = 4$ διατυπώθηκε και αποδείχθηκε για πρώτη φορά απο τον *Leonardo Fibonacci* (1170-1250) το 1225 στο βιβλίο του *Liber quadratorum*.

όπου

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Οι αριθμοί $2, 3, (1 + \sqrt{-5}), (1 - \sqrt{-5})$ είναι ανάγωγοι και δεν είναι ισοδύναμοι μεταξύ τους. Άρα ο δακτύλιος $\mathbb{Z}[\sqrt{-5}]$ δεν είναι περιοχή μονοσήμαντης ανάλυσης (είναι ακέραια περιοχή αφού είναι υποσύνολο των μιγαδικών αριθμών, που δεν έχει διαιρέτες του μηδενός).
Το λάθος του *Lame* το εντόπισε αμέσως ο *Liouville*. Λίγο αργότερα σε κάποιες περιπτώσεις δακτυλίων ο *Kummer* ξεπέρασε το πρόβλημα της μονοσήμαντης ανάλυσης εισάγοντας ένα νέο είδος αριθμών, τους ιδεώδεις αριθμούς, από τους οποίους προέρχεται η σημερινή έννοια του ιδεώδους στην Άλγεβρα. Οι ιδεώδεις αριθμοί (ιδεώδη) του *Kummer* προέρχονται από την αντικατάσταση ενός αριθμού με όλα τα πολλαπλάσιά του, δηλαδή του 2 από το $(2) = 2\mathbb{Z}[\sqrt{-5}] = \{2a | a \in \mathbb{Z}[\sqrt{-5}]\}$ ή και ιδεώδεις αριθμούς που προέρχονται από συνδυασμούς περισσότερων αριθμών, για παράδειγμα

$$(3, 1+\sqrt{-5}) = 3\mathbb{Z}[\sqrt{-5}]+(1+\sqrt{-5})\mathbb{Z}[\sqrt{-5}] = \{a3+b(1+\sqrt{-5})|a \in \mathbb{Z}[\sqrt{-5}], b \in \mathbb{Z}[\sqrt{-5}]\}.$$

Σήμερα λέμε ιδεώδες ένα υποσύνολο I ενός (μεταθετικού) δακτυλίου R αν ισχύει:
α) $0 \in I$
β) Αν $f, g \in I$, τότε $f - g \in I$
γ) Αν $f \in I$ και $r \in R$ τότε $rf \in I$.
Ειδικότερα αν $f_1, ..., f_n$ είναι οποιαδήποτε στοιχεία ενός (μεταθετικού) δακτυλίου το σύνολο

$$(f_1, \ldots, f_n) = \{r_1 f_1 + \cdots + r_n f_n | r_1, \ldots, r_n \in R\}$$

είναι ιδεώδες, το ιδεώδες που παράγεται από τα $f_1, ..., f_n$.
Στα ιδεώδη μπορούμε να ορίσουμε διάφορες αλγεβρικές πράξεις, όπως το άθροισμα και το γινόμενο:
Ορισμός Αν I και J είναι ιδεώδη ενός δακτυλίου R, τότε το άθροισμα των I και J είναι το σύνολο

$$I + J = \{f + g | f \in I, g \in J\}$$

και το γινόμενο των I και J είναι το σύνολο

$$IJ = \{f_1 g_1 + f_2 g_2 + \cdots + f_n g_n | f_1, \cdots, f_n \in I, g_1, \cdots, g_n \in J\},$$

δηλαδή πεπερασμένα αθροίσματα γινομένων στοιχείων του I με στοιχεία του J.

Το άθροισμα $I + J$ και το γινόμενο δύο ιδεωδών είναι ιδεώδη[4].
Στο παράδειγμα με το 6 στο δακτύλιο $\mathbb{Z}[\sqrt{-5}]$ θα δούμε με ποιό τρόπο ο *Kummer* κατάφερε να έχει μονοσήμαντη ανάλυση σε γινόμενο **πρώτων** ιδεωδών. Ένας ιδεώδης

[4]Δείξτε ότι το $I + J$ είναι ιδεώδες του R και μάλιστα το μικρότερο ιδεώδες του R που περιέχει τα ιδεώδη I και J. Επιπλέον αν το $I = (f_1, ..., f_n)$ και $J = (g_1, ..., g_s)$ τότε $I + J = (f_1, .., f_n, g_1, ..., g_s)$. Επίσης δείξτε ότι το IJ είναι ιδεώδες του R. Επιπλέον αν το $I = (f_1, ..., f_n)$ και $J = (g_1, ..., g_s)$ τότε $IJ = (f_1 g_1, f_1 g_2, .., f_1 g_s, f_2 g_1, f_2 g_2 ..., f_2 g_s, ...f_3 g_1, ...f_n g_1, ...f_n g_s)$.

αριθμός (ένα ιδεώδες) $P \neq R$ λέγεται πρώτος (πρώτο ιδεώδες) αν ισχύει $xy \in P$ τότε $x \in P$ ή $y \in P$. Οι πρώτοι ιδεώδεις αριθμοί (τα πρώτα ιδεώδη) παίζουν τον ρόλο των ανάγωγων στοιχείων. Αν θέσουμε

$$P_1 = (2, 1+\sqrt{-5}) = 2\mathbb{Z}[\sqrt{-5}] + (1+\sqrt{-5})\mathbb{Z}[\sqrt{-5}],$$

$$P_2 = (3, 1+\sqrt{-5}) = 3Z[\sqrt{-5}] + (1+\sqrt{-5})\mathbb{Z}[\sqrt{-5}]$$

και

$$P_3 = (3, 1-\sqrt{-5}) = 3Z[\sqrt{-5}] + (1-\sqrt{-5})\mathbb{Z}[\sqrt{-5}],$$

τότε τα P_1, P_2, P_3 είναι τα πρώτα ιδεώδη και έχουμε: $(2) = P_1P_1$, $(3) = P_2P_3$, $((1+\sqrt{-5})) = P_1P_2$ και $((1-\sqrt{-5})) = P_1P_3$. Έτσι πετυχαίνεται η μονοσήμαντη ανάλυση σε γινόμενο πρώτων ιδεωδών αριθμών (πρώτων ιδεωδών), που είναι

$$P_1P_1P_2P_3 = (2)(3) = (6) = ((1+\sqrt{-5}))((1\sqrt{-5})) = P_1P_2P_1P_3.$$

Κάτι παρόμοιο όμως δεν συμβαίνει σε κάθε δακτύλιο. Δακτύλιοι για τους οποίους κάθε γνήσιο (δηλ. διαφορετικό από τον δακτύλιο) ιδεώδες μπορεί να γραφτεί σαν γινόμενο πεπερασμένου πλήθους πρώτων ιδεωδών ονομάζονται σήμερα **περιοχές του** *Dedekind*.
Ο *Kummer* κατάφερε να αποδείξει το τελευταίο θεώρημα του *Fermat* χρησιμοποιώντας την έννοια του ιδεώδους αριθμού για πολλά n και ανάμεσα σε αυτά για όλα τα μικρότερα του 100 εκτός 37, 59 και 67. Συγκρίνοντας τα αποτελέσματα, όσον αφορά το θεώρημα του *Fermat* στα 200 χρόνια από τον *Fermat* ως τον *Kummer*, με τα αποτελέσματα του *Kummer* βλέπουμε πως η ιδέα της εισαγωγής των ιδεωδών έδωσε άμεσα εντυπωσιακά αποτελέσματα. Σήμερα η ιδέα του ιδεώδους αποτελεί μια από τις πιο βασικές έννοιες της Άλγεβρας.

4 Εικασία Mordell-Θεωρήματα Faltings και Wiles

Οι καμπύλες του Fermat είναι επίπεδες αλγεβρικές καμπύλες της μορφής $V(F_n)$, όπου F_n είναι το πολυώνυμο x^n+y^n-1. Το τελευταίο θεώρημα του *Fermat* είναι ισοδύναμο με τον ισχυρισμό ότι οι καμπύλες του Fermat δεν έχουν σημεία με ρητές συντεταγμένες για $n > 2$ εκτός απο τα $(1,0)$, $(0,1)$ για n περιττό και $(1,0), (-1,0), (0,1), (0,-1)$ για n άρτιο. Ο *Mordell* στις αρχές του εικοστού αιώνα παρατήρησε ότι ο λόγος που δεν έχουν πολλά ρητά σημεία οι καμπύλες του *Fermat* δεν ήταν ο βαθμός των καμπυλών που ήταν μεγάλος, αλλά το γένος. Το γένος είναι μια τοπολογική αναλλοίωτη των αλγεβρικών καμπυλών που στην περίπτωση της καμπύλης $V(F_n)$ είναι $g = (n-1)(n-2)/2$. Ο *Mordell* έκανε την εικασία ότι όταν μια καμπύλη έχει γένος $g > 1$ τότε έχει πεπερασμένα σε πλήθος σημεία με ρητές συντεταγμένες. Η εικασία του *Mordell* είναι πολύ πιο γενική πρόταση από το τελευταίο θεώρημα του *Fermat* και πολύ πιο σημαντική. Κορυφαίοι μαθηματικοί της Θεωρίας Αριθμών θεωρούσαν την πρόταση αυτή τόσο δύσκολη

που νόμιζαν ότι οι μαθηματικοί δεν θα μπορούσαν να την αποδείξουν ποτέ και για αυτό δεν θα έπρεπε να λέγεται καν εικασία.

Η πραγματικότητα όμως τους διέψευσε όταν το 1983 ο νεαρός τότε Γερμανός μαθηματικός $Gerd\ Faltings$ απέδειξε την εικασία του $Mordell$[5].
Η απόδειξη όμως της εικασίας του $Mordell$-Θεώρημα $Faltings$ συνεπάγεται ότι οι καμπύλες του $Fermat$ έχουν πεπερασμένο πλήθος σημείων με ρητές συντεταγμένες αλλά δεν αποδεικνύει το τελευταίο θεώρημα του $Fermat$. Όμως μετά την απόδειξη της εικασίας του $Mordell$, τα αποτελέσματα στο τελευταίο θεώρημα του $Fermat$ άρχισαν να διαδέχονται το ένα το άλλο. Βρέθηκαν διάφορες εικασίες που η απόδειξη οποιασδήποτε από αυτές συνεπαγόταν την απόδειξη του τελευταίου θεωρήματος του $Fermat$. Μια από αυτές ήταν και η εικασία των $Taniyama$-$Shimura$.

Το 1994, ο $Andrew\ Wiles$ καταφέρνει και αποδεικνύει την εικασία των $Taniyama$-$Shimura$[6] κι έτσι ολοκληρώνεται μετά από περισσότερα από 350 χρόνια προσπάθειας εκατοντάδων μαθηματικών από όλο τον κόσμο η απόδειξη του τελευταίου θεωρήματος του $Fermat$.

5 Παράγωγος Πολυωνύμου

Αν $f(x) = a_0 + a_1x + ... + a_nx^n$ πολυώνυμο του $D[x]$ τότε ορίζουμε παράγωγο του f το πολυώνυμο $f' = a_1 + 2a_2x + ... + na_nx^{n-1} \in D[x]$. Από τον ορισμό έχουμε τις παρακάτω ιδιότητες για την παράγωγο:

- $(f+g)' = f' + g'$
- $a \in D \Rightarrow a' = 0$
- $a \in D, (af)' = af'$
- $(fg)' = f'g + fg'$
- $(f^n)' = nf^{n-1}f'$.

Θεώρημα 5.1 Έστω g ανάγωγο και μη σταθερό πολυώνυμο του $D[x]$ τότε το $g^2|f$ αν και μόνο αν $g|f$ και $g|f'$.

[5]Faltings, Gerd (1983), Inventiones Mathematicae 73 (3): 349-366

[6]Η απόδειξη δημοσιεύτηκε την επόμενη χρονιά στο κορυφαίο περιοδικό *Annals of Mathematics*, *A. Wiles*, *Modular elliptic curves and Fermat's Last Theorem*, *Annals of Mathematics*, 141 (1995), 443-551.

Απόδειξη Αν $g^2|f$ τότε υπάρχει h, έτσι ώστε $f = g^2h$, αλλά τότε $f' = g^2h' + 2gg'h$ και άρα $g|f'$. Αντίστροφα αν $g|f$ και $g|f'$ τότε $f = gq$ και $f' = gq' + g'q$. Όμως $g|f'$ άρα $g|g'q$. Το g είναι ανάγωγο άρα $g|g'$ ή $g|q$. Το πρώτο είναι αδύνατο αφού $degg' = degg - 1 < degg$. Συνεπώς $g|q$, δηλαδή $g^2|f$.

Στο επόμενο θεώρημα D είναι ακέραια περιοχή τέτοια ώστε το σύνολο των ρητών $\mathbb{Q}$ είναι υποσύνολο του D, για παράδειγμα το D μπορεί να είναι το ίδιο το $\mathbb{Q}$ ή οι πραγματικοί $\mathbb{R}$,ή οι μιγαδικοί $\mathbb{C}$, ή οι πολυωνυμικοί δακτύλιοι $\mathbb{Q}[y], \mathbb{R}[y], \mathbb{C}[y], \mathbb{Q}[y,z], ...$

Θεώρημα 5.2 $(Taylor)$ Έστω $f \in D[x]$ πολυώνυμο βαθμού n και $a \in D$ τότε $f(x) = f(a) + f'(a)(x-a) + \frac{1}{2!}f''(a)(x-a)^2 + ... + \frac{1}{n!}f^{(n)}(a)(x-a)^n$.

Απόδειξη Έστω

$$f(x+a) = a_0 + a_1x + ... + a_nx^n$$

τότε

$$f'(x+a) = a_1 + 2a_2x + ... + na_nx^{n-1}$$
$$f''(x+a) = 2a_2 + 6a_3x + ... + n(n-1)a_nx^{n-1}$$
$$...$$
$$f^{(n)}(x+a) = n!a_n$$

Βάζοντας στις παραπάνω εξισώσεις $x = 0$ έχουμε:

$$a_0 = f(a),$$
$$a_1 = f'(a),$$
$$a_2 = \frac{f''(a)}{2!},$$
$$...,$$
$$a_n = \frac{f^{(n)}(a)}{n!}.$$

Αντικαθιστώντας στην

$$f(x+a) = a_0 + a_1x + ... + a_nx^n$$

και θέτοντας στην θέση του x το $x - a$ έχουμε το Θεώρημα του $Taylor$.

6 Εφαρμογή στις ρητές καμπύλες

Πρόταση 6.1 Οι καμπύλες του *Fermat* $V(x^n + y^n - 1) \subset \mathbb{C}^2$ για $n \geq 3$ δεν είναι ρητές.

Απόδειξη Έστω ότι για κάποιο $n \geq 3$ η καμπύλη του *Fermat* $V(x^n + y^n - 1)$ είναι ρητή. Τότε θα υπάρχουν ρητές συναρτήσεις $x(t), y(t)$ έτσι ώστε $x(t)^n + y(t)^n = 1$. Αφού $x(t), y(t)$ είναι ρητές, θα υπάρχουν πολυώνυμα $p(t), q(t), r(t)$ που δεν έχουν κοινό παράγοντα έτσι ώστε $x(t) = \frac{p(t)}{q(t)}$ και $y(t) = \frac{r(t)}{q(t)}$ (αν είχαν κοινό παράγοντα θα μπορούσαμε να τον απλοποιήσουμε). Για τα πολυώνυμα $p(t), q(t), r(t) \in \mathbb{C}[t]$ έχουμε την εξίσωση $p^n + r^n = q^n$ και παραγωγίζοντας $np^{n-1}p' + nr^{n-1}r' = nq^{n-1}q'$. Από την σχέση $p^n + r^n = q^n$ έχουμε ότι ανα δύο τα πολυώνυμα $p(t), q(t), r(t)$ δεν έχουν κοινό παράγοντα, γιατί αν είχαν δύο από αυτά κοινό παράγοντα τότε ο οποιοσδήποτε ανάγωγος παράγοντας του θα διαιρούσε και το τρίτο, δηλαδή και τα τρία θα είχαν έναν κοινό παράγοντα, που όμως το αποκλείσαμε παραπάνω.
Από τα τρία πολυώνυμα $p(t), q(t), r(t)$ κάποιο έχει το μεγαλύτερο βαθμό, έστω το $r(t)$, δηλαδή $deg(r(t)) \geq deg(p(t))$ και $deg(r(t)) \geq deg(q(t))$.
Θεωρούμε τις δύο εξισώσεις $p^n + r^n = q^n$ και $np^{n-1}p' + nr^{n-1}r' = nq^{n-1}q'$. Πολλαπλασιάζουμε την πρώτη με p' και την δεύτερη με p και τις αφαιρούμε. Τότε έχουμε $r^{n-1}(p'r - r'p) = q^{n-1}(p'q - q'p)$. Ο δακτύλιος $\mathbb{C}[t]$ είναι περιοχή μονοσήμαντης ανάλυσης, αφού ο , σαν σώμα, είναι περιοχή μονοσήμαντης ανάλυσης. Αναλύοντας και τα δύο μέλη της εξίσωσης σε γινόμενο αναγώγων προκύπτει ότι κανένας από τους ανάγωγους παράγοντες του r^{n-1} δεν εμφανίζεται στην ανάλυση του q^{n-1}. Άρα όλοι θα πρέπει να εμφανίζονται στην ανάλυση του $(p'q - q'p)$. Συνεπώς το r^{n-1} διαιρεί το $(p'q - q'p)$, άρα $(p'q - q'p) = Ar^{n-1}$. Τότε $deg(p'q - q'p) = deg(Ar^{n-1})$, όμως $deg(p'q - q'p) = degp + degq - 1$ και $deg(Ar^{n-1}) = degA + (n-1)degr \geq (n-1)degr \geq 2degr \geq degp + degq\, degp + degq - 1$, που είναι άτοπο.

7 Απαλοιφή

Το πρόβλημα της απαλοιφής είναι να βρεθούν οι συνθήκες που πρέπει να ικανοποιούνται από τους συντελεστές δύο πολυωνύμων ώστε τα δύο πολυώνυμα να έχουν κοινό παράγοντα. Έστω K σώμα και $f, g \in K[x]$, τότε τα f, g έχουν κοινό παράγοντα, που δεν είναι σταθερός, αν το h (ο μέγιστος κοινός διαιρέτης) δεν είναι σταθερό.
Η απόδειξη είναι προφανής. Το σημαντικό του θεωρήματος αυτού είναι ότι μέσω της απόδειξης του θεωρήματος 2.2.13 αν υπάρχει κοινός παράγοντας μπορεί να βρεθεί. Όμως η διαδικασία εύρεσης είναι πολύ μεγάλη. Θα δούμε παρακάτω μια διαφορετική διαδικασία που μας πληροφορεί αν τα δύο πολυώνυμα έχουν κοινό παράγοντα χωρίς όμως να τον βρίσκει. Η διαδικασία αυτή θα μας δώσει πολλά και εντυπωσιακά αποτελέσματα σε όλη τη διάρκεια του μαθήματος.

Έστω $f(x) = a_0 + a_1x + ... + a_nx^n$ και $g(x) = b_0 + b_1x + ... + b_mx^m$ δύο πολυώνυμα με $a_n \neq 0$ και $b_m \neq 0$ και συντελεστές από μια περιοχή μονοσήμαντης ανάλυσης D.

Θεώρημα 7.1 Τα πολυώνυμα f, g έχουν κοινό παράγοντα, που δεν είναι σταθερός (δηλαδή δεν είναι στοιχείο του D), αν και μόνο αν υπάρχουν μη μηδενικά πολυώνυμα y, f βαθμών μικρότερων των n και m αντίστοιχα, τέτοια ώστε $\varphi f = \psi g$.

Απόδειξη Έστω ότι τα f, g έχουν κοινό παράγοντα το h που δεν είναι σταθερός. Τότε $f = \psi h$ και $g = \varphi h$. Άρα $\varphi f = \psi g$ και τα ψ, φ έχουν βαθμούς μικρότερους των n και m αντίστοιχα. Αντίστροφα, αν υπάρχουν μη μηδενικά πολυώνυμα ψ, φ βαθμών μικρότερων των n και m αντίστοιχα, τέτοια ώστε $\varphi f = \psi g$, τότε αναλύουμε τα πολυώνυμα φ, f, ψ, g σε γινόμενα αναγώγων. Οι ανάγωγοι παράγοντες του g ή ισοδύναμοί τους πρέπει όλοι να εμφανίζονται στο γινόμενο φf. Όμως $degf < degg$, άρα δεν μπορεί όλοι να εμφανίζονται στο φ. Θα πρέπει κάποιοι να εμφανίζονται και στο f. Άρα τα f, g έχουν κοινό παράγοντα που δεν είναι σταθερός.

Θεώρημα 7.2 Τα πολυώνυμα f, g έχουν κοινό παράγοντα που δεν είναι σταθερός, αν και μόνο αν

$$R(f,g;x) = \begin{vmatrix} a_0 & a_1 & . & . & . & a_n & 0 & 0 & 0 \\ 0 & a_0 & a_1 & . & . & . & a_n & 0 & 0 \\ . & . & . & . & . & . & . & . & . \\ 0 & . & . & a_0 & a_1 & . & . & . & a_n \\ b_0 & b_1 & . & b_{m-1} & b_m & 0 & 0 & 0 & 0 \\ 0 & b_0 & . & . & b_{m-1} & b_m & 0 & 0 & 0 \\ . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & b_0 & . & . & b_{m-1} & b_m & 0 \\ 0 & 0 & 0 & 0 & b_0 & . & . & b_{m-1} & b_m \end{vmatrix},$$

όπου η ορίζουσα είναι $m + n$ τάξης και έχει m σειρές από a_i και n σειρές από b_i.

Απόδειξη Υποθέτουμε ότι τα f, g έχουν κοινό παράγοντα (που δεν είναι σταθερός) τότε υπάρχουν μη μηδενικά πολυώνυμα ψ, φ βαθμών μικρότερων των n και m αντίστοιχα, τέτοια ώστε $\varphi f = \psi g$. Έστω $\psi = c_0 + c_1x + ... + c_{n-1}x^{n-1}$ και $\varphi = d_0 + d_1x + ... + d_{m-1}x^{m-1}$, όπου ένα τουλάχιστον από τα c_i είναι διάφορο του μηδενός και ένα τουλάχιστον από τα d_i είναι διάφορο του μηδενός. Από την εξίσωση

$$(d_0 + d_1x + ... + d_{m-1}x^{m-1})(a_0 + a_1x + ... + a_nx^n) = \varphi f =$$
$$= \psi g = (c_0 + c_1x + ... + c_{n-1}x^{n-1})(b_0 + b_1x + ... + b_mx^m)$$

προκύπτει το ίδιο πολυώνυμο βαθμού $m + n - 1$ και από τις δύο πλευρές. Άρα οι συντελεστές ομοβάθμιων όρων είναι ίσοι, δηλαδή

$$d_0a_0 = c_0b_0$$
$$d_0a_1 + d_1a_0 = c_0b_1 + c_1b_0$$
$$...$$
$$d_{m-1}a_n = c_{n-1}b_m$$

Οι παραπάνω $m+n$ εξισώσεις μπορούν να θεωρηθούν σαν ένα γραμμικό ομογενές σύστημα με $m+n$ αγνώστους, τους $d_0, d_1, ..., d_{m-1}, -c_0, -c_1, ..., -c_{n-1}$, που ξέρουμε ότι έχει μια τουλάχιστον μη μηδενική λύση, αφού ένα τουλάχιστον από τα c_i είναι διάφορο του μηδενός. Άρα η ορίζουσα των συντελεστών, που είναι το $R(f, g; x)$, είναι ίση με μηδέν. (Ή διαφορετικά από την εξίσωση $\varphi f = \psi g$ έχουμε ότι τα $m + n$ διανύσματα $f, xf, x^2f, ..., x^{m-1}f, g, xg, ..., x^{n-1}g$ του διανυσματικού χώρου $K[x]$, όπου K είναι το σώμα κλασμάτων του D, είναι γραμμικά εξαρτημένα άρα $R(f, g; x) = 0$)
Αντίστροφα, αν $R(f, g; x) = 0$ τότε το ομογενές σύστημα έχει μη μηδενική λύση πάνω από το σώμα κλασμάτων K του D. Ώστε, πολλαπλασιάζοντας με κάποιο κοινό παρονομαστή, το σύστημα έχει μη μηδενική λύση πάνω από το D. Άρα υπάρχουν μη μηδενικά πολυώνυμα φ, ψ τέτοια ώστε $\varphi f = \psi g$, δηλαδή τα πολυώνυμα f, g έχουν κοινό παράγοντα, που δεν είναι σταθερός.

Ορισμός 7.3 Το $R(f, g; x)$ λέγεται **απαλοίφουσα** των πολυωνύμων f, g. Η απαλοίφουσα ενός πολυωνύμου f και της παραγώγου του f' λέγεται **διακρίνουσα** του f.

Θεώρημα 7.4 Υπάρχουν πολυώνυμα A και B βαθμών το πολύ $m-1$ και $n-1$ αντίστοιχα, τέτοια ώστε $R(f, g; x) = Af + Bg$.

Απόδειξη Έστω $A_{i,1}$ ο συμπαράγοντας του στοιχείου $a_{i,1}$ της πρώτης στήλης του πίνακα

$$\begin{pmatrix} a_0 & a_1 & . & . & . & a_n & 0 & 0 & 0 \\ 0 & a_0 & a_1 & . & . & . & a_n & 0 & 0 \\ . & . & . & . & . & . & . & . & . \\ 0 & . & . & a_0 & a_1 & . & . & . & a_n \\ b_0 & b_1 & . & b_{m-1} & b_m & 0 & 0 & 0 & 0 \\ 0 & b_0 & . & . & b_{m-1} & b_m & 0 & 0 & 0 \\ . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & b_0 & . & . & b_{m-1} & b_m & 0 \\ 0 & 0 & 0 & 0 & b_0 & . & . & b_{m-1} & b_m \end{pmatrix},$$

Τότε $(A_{1,1} + A_{2,1}x + ... + A_{m,1}x^{m-1})f + (A_{m+1,1} + A_{m+2,1}x + ... + A_{m+n,1}x^{n-1})g = (A_{1,1}a_0 + A_{m+1,1}b_0) + (A_{1,1}a_1 + A_{2,1}a_0 + A_{m+1,1}b_1 + A_{m+2,1}b_0)x + ... + (A_{m,1}a_n + A_{m+n,1}b_m)x^{m+n-1} = R(f, g; x) + 0x + ... + 0x^{m+n-1} = R(f, g; x)$.

Αυτό ισχύει επειδή

1. $(A_{1,1}a_0 + A_{m+1,1}b_0)$ είναι το άθροισμα των στοιχείων της πρώτης στήλης επί τους

συμπαράγοντές τους, που είναι η ορίζουσα του πίνακα, δηλ. $R(f, g; x)$

2. $(A_{1,1}a_1 + A_{2,1}a_0 + A_{m+1,1}b_1 + A_{m+2,1}b_0)$ είναι το άθροισμα των γινομένων των στοιχείων της δεύτερης στήλης επί τους συμπαράγοντες των στοιχείων της πρώτης στήλης, που είναι μηδέν. Όσο δηλαδή η ορίζουσα του προηγούμενου πίνακα αν αντικαταστήσουμε τα στοιχεία της πρώτης στήλης με αυτά της δεύτερης.

3. . . .

$m+n$. $(A_{m,1}a_n + A_{m+n}b_m)$ είναι το άθροισμα των γινομένων των στοιχείων της $m+n$ στήλης επί τους συμπαράγοντες των στοιχείων της πρώτης στήλης που είναι μηδέν. Όσο δηλαδή η ορίζουσα το προηγούμενου πίνακα αν αντικαταστήσουμε τα στοιχεία της πρώτης στήλης με αυτά της $m+n$ στήλης.

Ασκήσεις

- 1. Δείξτε ότι οι μονάδες του $D[x]$ είναι οι μονάδες του D, όπου D είναι ακέραια περιοχή.
- 2. Δείξτε ότι ο δακτύλιος $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \epsilon \mathbb{Z}\}$ είναι ακέραια περιοχή και τα μόνα στοιχεία που είναι μονάδες είναι τα $1, -1$.
- 3. Δείξτε ότι τα στοιχεία $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ του $\mathbb{Z}[\sqrt{-5}]$ είναι ανάγωγα. Δείξτε ότι ο $\mathbb{Z}[\sqrt{-5}]$ δεν είναι περιοχή μονοσήμαντης ανάλυσης.
- 4. Δείξτε ότι για τα ιδεώδη $P_1 = (2, 1 + \sqrt{-5})$, $P_2 = (3, 1 + \sqrt{-5})$, $P_3 = (3, 1 - \sqrt{-5})$ του $\mathbb{Z}[\sqrt{-5}]$ ισχύει:
  - **α)** $(2) = P_1 P_1$,
  - **β)** $(3) = P_2 P_3$,
  - **γ)** $(1 + \sqrt{-5}) = P_1 P_2$, και
  - **δ)** $(1 - \sqrt{-5}) = P_1 P_3$.
- 5. Δείξτε ότι τα ιδεώδη $P_1 = (2, 1+\sqrt{-5})$, $P_2 = (3, 1+\sqrt{-5})$, $P_3 = (3, 1-\sqrt{-5})$ είναι πρώτα.
- 6. Δίνεται η ρητή καμπύλη με $x(t) = t^3 - 1$ και $y(t) = \frac{t}{t^2+1}$, να βρεθεί η εξίσωση $f(x, y) = 0$ της καμπύλης.