ΠΟΛΥΩΝΥΜΙΚΟΣ ΔΑΚΤΥΛΙΟΣ

1. Πολυωνυμικός Δακτύλιος. Θα κατασκευάσουμε και θα μελετήσουμε τις βασικές ιδιότητες του πολυωνυμικού δακτυλίου D[u] πάνω σε μία ακέραια περιοχή D. Την ίδια κατασκευή κάνουμε και για τον F[u], F σώμα, Δ[u], Δ δακτύλιος .

Η κατασκευή του Δ[u] γίνεται ως εξής:

(1) Θεωρούμε το τυχόν στοιχείο u, και υποθέτουμε ότι, ορίζονται τα γινόμενα $u^0 = 1$, $u^1 = u$, $u^n = uu^{n-1} = u^{n-1}u$, για κάθε φυσικό αριθμό n. Το D[u] περιέχει όλα αυτά τα στοιχεία.

(2) Το D[u] περιέχει ακόμα και όλα τα γινόμενα λu^n, όπου $\lambda \in D$. Ιδιαίτερα, περιέχει τα στοιχεία $1u^n = u^n$ και $0u^k = 0$.

(3) Εν Δ[u] ορίζονται εκφράσεις της μορφής

(λ(u)) $\quad \lambda_n u^n + \lambda_{n-1}u^{n-1} + \cdots + \lambda_k u^k + \cdots + \lambda_1 u + \lambda_0$ με $\lambda_k \in \Delta$, και είναι (λ) = 0 ανν $\lambda_k = 0$ για όλα τα k = 0 , 1, . . . , n.

Ορολογία των D[u], Δ[u], F[u]. Το (λ) καλείται ***πολυώνυμο***. Τα λ_k καλούνται ***συντελεστές*** του πολυωνύμου. Ο u^n ($\lambda_n \neq 0$) είναι ο ***μεγιστοβάθμιος όρος*** του πολυωνύμου, n είναι ο ***βαθμός*** (degree) του πολυωνύμου. Γράφουμε n = deg(λ). ***Σταθερές*** καλούμε τα πολυώνυμα μηδενικού βαθμού. ***Μονικό*** (monic) καλείται το πολυώνυμο, που έχει συντελεστή του μεγιστοβαθμίου όρου την μονάδα του Δ.

Από τον ορισμό του Δ[u] είναι φανερό ότι το x δεν είναι απαραιτήτως στοιχείο του Δ[u]. Αν όμως το Δ έχει μοναδιαίο στοιχείο e, μπορούμε να ταυτίσουμε το u με το eu. Γι' αυτόν τον λόγο, όταν θεωρούμε δακτύλιο Δ, θα τον λαμβάνουμε αντιμεταθετικό και με μονάδα.

Το σύνολο Δ[u], D[u], F[u], καθίσταται αντιμεταθετικός δακτύλιος, αν ορίσουμε τις πράξεις πρόσθεση "+" και πολλαπλασιασμό "·" ως εξής: ***Άθροισμα*** α(u)+β(u) των πολυωνύμων α και β με degα = m και degβ = n, m ≤ n, είναι ένα πολυώνυμο r βαθμού, του οποίου ο συντελεστής του u^k, $0 \leq k \leq r$, είναι ο $\alpha_k + \beta_k$. (Για k > m, οι α_k είναι ίσοι με μηδέν). ***Γινόμενο*** α(u)β(u) των πολυωνύμων α και β, είναι ένα πολυώνυμο γ(u), με συντελεστή $\gamma_k = \sum_{i+j=k} \alpha_i \beta_j$, όπου $0 \leq k \leq m+n$,

Παρατηρήσεις. 1) Ο βαθμός του γινομένου πολυωνύμου γ(u) δεν μπορεί να είναι μεγαλύτερος του αθροίσματος deg(α)+deg(β), και αν $\alpha_m \beta_n \neq 0$ (δεν έχουμε, δηλαδή, διαιρέτες του μηδενός) $\deg \alpha\beta = \deg \alpha + \deg \beta$ 2) Το Δ(u) είναι ακεραία περιοχή, ανν Δ = D.

Στο εξής θα υποθέτουμε ότι οι συντελεστές παίρνονται από ένα σώμα F.

Ανάγωγο καλείται ένα πολυώνυμο, αν δεν αναλύεται σε γινόμενο άλλων πολυωνύμων, βαθμού ≥ 1. Λέμε ότι το β(u) ***διαιρεί*** το α(u), ανν $\exists\, \gamma(u) \in \Delta[u], D[u], F[u]$ με α = γβ. Γράφουμε και β | α.

Το γινόμενο δύο πολυωνύμων το βρίσκουμε εύκολα, αν εφαρμόσουμε την μέθοδο, που γίνεται φανερή στο παράδειγμά μας:

Να βρεθεί το γινόμενο των πολυωνύμων $\alpha(x) = 2x^4 + x^3 - 3x^2 + x + 1$

και , $\quad \beta(x) = (2x^2 - 1)$.

Χρησιμοποιούμε το σχήμα:

$$
\begin{array}{cccccccc}
 & & & 2 & 1 & -3 & 1 & 1 \\
 & & & & & 2 & 0 & -1 \\
\hline
 & & & -2 & -1 & 3 & -1 & -1 \\
+ & & & & & & & \\
 & -4 & -2 & -6 & 2 & 2 & & \\
\hline
 & -4 & -2 & -8 & 1 & 5 & -1 & -1
\end{array}
$$

$\alpha(x)\beta(x) = -4x^6 - 2x^5 - 8x^4 + x^3 + 5x^2 - x - 1$.

Το σχήμα αυτό του πολλαπλασιασμού δύο πολυωνύμων, είναι χρήσιμο και στην περίπτωση πολλαπλασιασμού μεγάλων ακεραίων αριθμών, περιπτώσεις, που τα μικρά computεράκια δεν διαθέτουν αρκετά ψηφία για να δείξουν ακέραιο αποτέλεσμα. Έστω π.χ. ότι έχουμε να πολλαπλασιάσουμε τους ακεραίους $\alpha = 12338977652$ και $\beta = 87996654210$. Αν το computεράκι μας δεν διαθέτη περισσότερα από δώδεκα ψηφία για να εκφράσει έναν ακέραιο, εργαζόμαστε ως εξής:
Γράφουμε $\alpha(t) = 12389t^5 + 776t^2 + 52t^0$, $\beta(t) = 87996t^5 + 5421t$, όπου $t = 10$. Στην συνέχεια εκτελούμε τους επιμέρους πολλαπλασιασμούς κατά το προηγούμενο σχήμα και προσθέτουμε, έτσι ώστε να βρούμε το γινόμενο $\alpha(t)\beta(t)$ και απ' αυτό το γινόμενο αβ.
Μια άλλη εφαρμογή του προηγούμενου σχήματος, έχουμε στο εξής πρόβλημα: Να βρεθεί το γινόμενο $(1+t)(1+t^2)(1+t^4)$. Έχουμε, συνοπτικά,

$$
\begin{array}{cccccccc}
 & & & & & 1 & 1 & \\
 & & & & 1 & 0 & 1 & \\
\hline
 & & & & & 1 & 1 & \\
 & & & & 1 & 1 & & \\
\hline
 & & & & 1 & 1 & 1 & 1 \\
 & & & 1 & 0 & 0 & 0 & 1 \\
\hline
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}
$$

δηλαδή, $t^7 + t^6 + t^5 + t^4 + t^3 + t^2 + t + 1$. Εύκολα, τώρα, το παραπάνω σχήμα γενικεύεται σε n παράγοντες, οπότε έχουμε ότι, $(1+t)(1+t^2)(1+t^{2^2})\cdots(1+t^{2^n}) = 1 + t + t^2 + \ldots + t^{2n-1}$.

Ο Δ[u] είναι κάτι περισσότερο από αντιμεταθετικός δακτύλιος. Είναι ακέραια περιοχή αν και μόνον αν ο Δ είναι ακεραία περιοχή. Πόρισμα του γεγονότος αυτού, είναι ότι, εν D[u], F[u] ισχύει ο νόμος της διαγραφής.

Μέσα στον δακτύλιο F[u] ισχύει ο αλγόριθμος της διαιρέσεως: Δοθέντων των α και β εν F[u], υπάρχουν τα q και r∈ F[u] με degr(u) < degβ(u), τέτοια ώστε,

α(u) = q(u)β(u)+r(u).

Οι απόδειξη της παραπάνω σχέσεως, βασίζεται στην γνωστή διαίρεση των πολυωνύμων, όπου, το r(u) υπολογίζεται αφαιρώντας από το α(u) διαδοχικά πολλαπλάσια του β(u), και γίνεται επαγωγικά, ως εξής: Έστω ότι dega(u) = k και ότι ο αλγόριθμος ισχύει για όλα τα πολυώνυμα βαθμού < k. Έστω m = degβ, m < k. Έστω ακόμα, α_k και β_m οι συντελεστές των μεγιστοβαθμίων όρων των πολυωνύμων α και β αντίστοιχα. Το πολυώνυμο $\left(\frac{\alpha_k}{\beta_m}u^{k-m}\right)\beta(u)$ είναι k βαθμού, και έχει συντελεστή του μεγιστοβαθμίου όρου, τον α_k. Το πολλαπλάσιο αυτό του β, το αφαιρούμε από το α, και λαβαίνουμε ένα πολυώνυμο α΄ βαθμού < α, το οποίο λόγω της υπόθεσης της επαγωγής, γράφεται α΄ = q΄β+r΄. Είναι, τότε, $\alpha = \left(\frac{\alpha_k}{\beta_m}u^{k-m} + \beta'\right)\beta(u) + r'$, όπως ακριβώς απαιτείται. Τα

πολυώνυμα q και r ορίζονται μονοσήμαντα. Πράγματι, αν είχαμε την σχέση qβ+r = q΄β+r΄, τότε, και (q΄–q)β = r–r΄, με deg(r–r΄) < degβ, β ≠ 0, άρα, αναγκαστικά, q΄–q = 0. Ο βαθμός του r είναι λοιπόν μηδέν ανν το β | α.

Εν F[u] μεταφέρονται όλα όσα είπαμε για την διαιρετότητα εν Z. (Βλέπε «Ακέραιοι Αριθμοί»). Έχουμε όμως μια μικρή μεταβολή στην ορολογία. Λέμε ***ανάγωγο*** εν F[u], και όχι ***πρώτο πολυώνυμο***. Τα πολυώνυμα α(u) και β(u) είναι ***μεταξύ τους πρώτα***, ανν (α, β) = 1. Ο μ.κ.δ (α, β) των πολυωνύμων α και β, είναι το ***monic*** πολυώνυμο d, που έχει την ιδιότητα να διαιρεί και το α και το β, και να διαιρείται από κάθε άλλο κοινό διαιρέτη των α και β. Ισχύει και εδώ η σχέση (ταυτότης του Bezout):

$$d(u) = s(u)\alpha(u)+t(u)\beta(u).$$

Αν το p(u) είναι ανάγωγο εν F[u] και p(u) | α(u)β(u), τότε ή p(u) | α(u) ή p(u) | β(u). Τέλος, κάθε πολυώνυμο μη μηδενικού βαθμού, εκφράζεται ως το γινόμενο μιάς σταθεράς c επί ανάγωγα monic πολυώνυμα, κατά ένα και μόνο τρόπο.

Παρατήρηση. Αν είχαμε ακόμα και $e(u)=(\alpha(u),\beta(u))$, τότε, επειδή ισχύουν αμφότερες οι σχέσεις $e(u)\,|\,d(u)$ και $d(u)\,|\,e(u)$ εν F[u], έπεται ότι $e(u)=\lambda d(u)$, $\lambda\in F[u]$, ή αντίστροφα. Για τον λόγο αυτό, ο d(u) ορίζεται ως το monic πολυώνυμο d όταν $\deg d(u)\geq 1$ ο 1, αν $\deg d(u)=0$.

Παράδειγμα. Να ευρεθεί ο μ.κ.δ. των πολυωνύμων $f(u) = -2-3u+u^2+3u^3+u^4$
και $g(u) = -8-4u+2u^2+u^3$.
Λύση. Εφαρμόζουμε τον αλγόριθμο του Ευκλείδη (σελ. 76). Είναι,

$f(u) = g(u)\,q_1(u) + r_1$ όπου $q_1(u) = 1+u$, $r_1(u) = 6+9u+3u^2$

$g(u) = r_1(u)\,q_2(u)+r_2$ όπου $q_2(u) = -\frac{1}{3}+\frac{1}{3}u$, $r_2(u) = -6-3u$

$r_1(u) = r_2(u)\,q_3(u)$ όπου $q_3(u) = -1-u$ $r_3(u) = 0$.

Ο μ.κ.δ. των πολυωνύμων f και g είναι το monic πολυώνυμο d = u+2, που αντιστοιχεί στο $r_2(u)$
Ισχύει ότι, $d = -q_2 f + (1+q_2q_1)g$.

Η διαίρεση δύο πολυωνύμων, και, τελικά, η εύρεση της ταυτότητας του Bezout γι' αυτά, διευκολίνεται, αν ακολουθήσουμε το σχήμα, που περιγράφεται στο παρακάτω παράδειγμα.

Παράδειγμα. Έστω, ότι θέλουμε να βρούμε τον μ.κ.δ. των $f(x)=16x^4-80x^3+96x^2+64x-128$ και $g(x)=4x^3-15x^2+12x+4$. Υπολογίζουμε τα $q_1(x)$ και $r_1(x)$ σύμφωνα με το σχήμα:

	g				4	-5	**$q_1(x)$**			
4	-15	12	4		16	-80	96	64	-128	**f(x)**
					4×4 = 16	4×(-15) = -60	4×12 = 48	4×4 = 16		
						-20	48	48	-128	
						-5×4 = -20	-5×(-15) = 75	-5×12 = -60	-5×4 = -20	
							-27	108	-108	**$r_1(x)$**

Είναι, $q_1(x)=4x-5$ και $r_1(x)=-27x^2+108x-108$, $f(x)=g(x)q_1(x)+r_1(x)$ (πρώτο βήμα).
Παρατηρούμε ότι $r_1(x)=27(-x^2+4x-4)$. Συνεχίζουμε τις διαιρέσεις: (δεύτερο βήμα)

	r_1			-4	-1	**$q_2(x)$**		
-1	4	-4		4	-15	12	4	**g(x)**
				-4×(-1) = 4	-4×4 = 16	-4×(-4) = 16		
					1	-4	4	
					-1×(-1) = 1	-1×4 = -4	-1×(-4) = 4	
					0	0	0	**r(x)**

Είναι, $q_2(x) = -4x - 1$, $r_2(x) = 0$, οπότε και $g(x) = -27(4x+1)(-x^2 + 4x - 4)$. Άρα, ο μ.κ.δ. των f(x) και g(x) είναι το $r_1(x) = -x^2 + 4x - 4$. Εδώ, έχουμε ότι, $r_1(x) \mid g(x)$ μιά και $g(x) = q_2(x)r_1(x)$, ως επίσης $f(x) = (q_2(x)r_1(x)q_1(x) + 27r_1(x)) = (q_2q_1 + 27)r_1$, δηλαδή, και $r_1(x) \mid f(x)$.

Παράδειγμα. Να βρεθεί ο μ.κ.δ. των $f(x) = x^4 + 1$ και $g(x) = x^2 - 1$. Έχουμε,

			1	0	1		
1	0	-1	1	0	0	0	1
			1×1 = 1	1×0 = 0	1×(-1) = -1		
			0	0	1	0	1
					1×1 = 1	1×0 = 0	1×(-1) = -1
					0	0	2

Άρα, $(f, g) = 1$. Έχουμε, ακόμα, $1 = \frac{1}{2}f(x) - \frac{1}{2}g(x)$

Θεώρημα. Αν F αντιμεταθετικό σώμα, τότε ο πολυωνυμικός δακτύλιος F[u] είναι περιοχή κυρίων ιδεωδών. (Βλέπε ενότητα "Ακέραιοι Αριθμοί" παράγραφος 10.)
Απόδειξη. Έστω J τυχόν ιδεώδες του F[u]. Αν J = (0), τότε δεν έχουμε τίποτα να δείξουμε. Έστω λοιπόν, J ≠ (0). Υποθέτουμε ότι, β είναι το ελαχίστου βαθμού πολυώνυμο, που ανήκει στον J. Για κάθε άλλο πολυώνυμο α του J, ο αλγόριθμος της διαιρέσεως δίδει ένα πηλίκο q και ένα υπόλοιπο r βαθμού < degβ, με r = α–qβ. Άτοπον.
Άρα r = 0, α = qβ, και συνεπώς, J = (β).

Λήμμα του Gauss. Αν ένα πολυώνυμο με ακεραίους συντελεστές είναι δυνατόν να γραφεί ως γινόμενο δύο πολυωνύμων, μικρότερου βαθμού, με ρητούς συντελεστές, τότε, γράφεται και ως γινόμενο δύο πολυωνύμων, μικρότερου βαθμού, με ακεραίους συντελεστές.
Απόδειξη. Έστω $f = gh$, όπου το f έχει ακεραίους συντελεστές, ενώ τα g και h ρητούς. Υποθέτουμε ότι, έχουμε διαιρέσει με τον μ.κ.δ. των συντελεστών των g και h αντίστοιχα, τους συντελεστές των g και h. Γράφουμε, λοιπόν,

$$g(x) = \frac{\alpha_n}{\beta_n}x^n + \frac{\alpha_{n-1}}{\beta_{n-1}}x^{n-1} + \ \ldots + \ \frac{\alpha_0}{\beta_0} \quad \text{και} \quad h(x) = \frac{\gamma_m}{\delta_m}x^m + \frac{\gamma_{m-1}}{\delta_{m-1}}x^{m-1} + \ \ldots + \ \frac{\gamma_0}{\delta_0},$$

όπου όλοι οι συντελεστές είναι ανάγωγα κλάσματα. Αν Β και Δ είναι το γινόμενο όλων των παρονομαστών β και δ αντίστοιχα, τότε το $Bg(x)$ και το $\Delta h(x)$ έχουν ακεραίους συντελεστές. Αν Α ο μ.κ.δ. των β και Γ ο μ.κ.δ. των δ, λαβαίνουμε, τελικά, τα πολυώνυμα

$$(B/A)g(x) = A_nx^n + A_{n-1}x^{n-1} + \ \ldots + \ A_0 \quad \text{και} \quad (\Delta/\Gamma)h(x) = \Gamma_mx^m + \Gamma_{m-1}x^{m-1} + \ \ldots + \ \Gamma_0.$$

Η $f = gh$ γίνεται, τώρα, $B\Delta f = A\Gamma\left(\frac{B}{A}g\right)\left(\frac{\Delta}{\Gamma}h\right)$. Παρατηρούμε, ότι, $A\Gamma \mid B\Delta$. Θέτουμε, λοιπόν, $E = \frac{B\Delta}{A\Gamma} \in \mathbb{Z}$, και γράφουμε,

$$Ef(x) = (A_nx^n + A_{n-1}x^{n-1} + \ \ldots + \ A_0)(\Gamma_mx^m + \Gamma_{m-1}x^{m-1} + \ \ldots + \ \Gamma_0). \quad (1)$$

Το Λήμμα θα έχει αποδειχθεί, αν δείξουμε ότι, $E = \pm 1$. Αν $E \neq \pm 1$, τότε το Ε θα έχει κάποιον πρώτο παράγοντα p. Ο p δεν διαιρεί όμως όλους τους συντελεστές Α, ούτε όλους τους συντελεστές Γ. Έστω, λοιπόν, A_i και Γ_j οι μικρότεροι συντελεστές από τους Α και Γ αντίστοιχα, που ο p δεν διαιρεί. Ας δούμε, τώρα, τον συντελεστή του x^{i+j}. Στο πολυώνυμο $f(x)$, στην (1), ο συντελεστής

του όρου αυτού, διαιρείται από τον Ε, και, συνεπώς, από τον p. Αν κάνουμε τον πολλαπλασιασμό που σημειώνεται στην (1), θα βρούμε για συντελεστή του όρου x^{i+j} τον $\sum_{k=0}^{i-1} A_k \Gamma_{i+j-k} + \sum_{k=i+1}^{i+j} A_k \Gamma_{i+j-k} + A_i \Gamma_j$. Ο p διαιρεί όλους τους $A_k, \forall k \neq i$ και όλους τους $\Gamma_\lambda, \forall \lambda \neq j$. Ο p συνεπώς, διαιρεί τους δύο πρώτους όρους του προηγούμενου αθροίσματος, δεν διαιρεί όμως, τον όρο $A_i \Gamma_j$. Άτοπον.

Πόρισμα. Ένα πολυώνυμο, που είναι ανάγωγο εν $Z[x]$, είναι ανάγωγο και εν $Q[x]$.

Θεώρημα. (Κριτήριο αναγωγιμότητας του Eisenstein). Έστω το πολυώνυμο $f \in Z[x]$, $f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \ \ldots + \ \alpha_0$. Αν υπάρχει πρώτος p τέτοιος ώστε: α) Ο p διαιρεί όλους τους συντελεστές α, εκτός από τον α_n. β) Ο p^2 δεν διαιρεί τον α_0. Το f είναι, τότε, ανάγωγο εν $Q[x]$.
Απόδειξη. Έστω ότι το f δεν είναι ανάγωγο εν $Q[x]$. Γράφεται, τότε, ως γινόμενο δύο πολυωνήμων $g(x) = \beta_k x^k + \beta_{k-1} x^{k-1} + \ \ldots + \ \beta_0$ και $h(x) = \gamma_m x^m + \gamma_{m-1} x^{m-1} + \ \ldots + \ \gamma_0$, όπου εί-ναι $k, m \geq 1$, και $\alpha_n = \beta_k \gamma_m$ και $\alpha_0 = \beta_0 \gamma_0$. Αφού ο p δεν διαιρεί τον α_n, δεν διαιρεί ούτε τον β_k, ούτε τον γ_m. Επίσης, επειδή ο p^2 δεν διαιρεί τον α_0, ο p δεν διαιρεί έναν από τους β_0, γ_0, και διαιρεί τον άλλο. Έστω, λοιπόν, ότι $p \mid \beta_0$, αλλά ο p δεν διαιρεί τον γ_0. Έστω, τώρα, β_j, $j \geq 1$, εκείνος ο συντελεστής β, με τον μικρότερο δείκτη j, τον οποίο ο p δεν διαιρεί. Ο συντελεστής α_j του x^j στο πολυώνυμο f διαιρείται από τον p. Στο γινόμενο gh ο συντελεστής του όρου x^j είναι ο $\sum_{k=0}^{j} \beta_k \gamma_{j-k}$, ο οποίος δεν διαιρείται από τον p. Άτοπον.

Παράδειγμα. Το πολυώνυμο $x^5 - 2$ είναι ανάγωγο εν $Q[x]$, μιά και εφαρμόζεται το κριτήριο με p = 2. Όμοια και για το $3x^5 + 7x^4 - 14x^2 + 7x + 56$, αν λάβουμε p = 7. Το κριτήριο δεν εφαρμόζεται στην περίπτωση των $x^3 - 3x - 1$, ή $x^4 + x^3 + x^2 + x + 1$, τα οποία, όμως, είναι ανάγωγα εν $Q[x]$. Ένας απλός όμως μετασχηματισμός, όπως είναι ο $x = u + 1$, είναι δυνατόν να οδηγήσει σε πολυώνυμο, στο οποίο εφαρμόζεται το κριτήριο του Eisenstein. Έτσι, π.χ., το $x^3 - 3x - 1$ μετατρέπεται στο $u^3 + 3u^2 - 3$, όπου με p = 3, εφαρμόζεται το κριτήριο. Ο προηγούμενος, λοιπόν, μετασχηματισμός, δεν επηρεάζει την αναγωγιμότητα του πολυωνύμου.

Ενδιαφέρον παρουσιάζει ο ***μετασχηματισμός του Tschirnhaus,*** $x = u - \frac{\alpha_{n-1}}{n}$, ο οποίος, μετασχηματίζει ένα monic πολυώνυμο, σε ένα άλλο, του οποίου λείπει ο όρος x^{n-1}. Π.χ. το $x^2 + \beta x + \gamma$, μετασχηματίζεται στο $(u - \beta/2)^2 + \beta(u - \beta/2) + \gamma = u^2 + \beta^2/2 + \gamma$.

Λήμμα. Το πολυώνυμο $f(x)$ είναι ανάγωγο, ανν το $f(x+1)$ είναι ανάγωγο.
Πράγματι, $f(x+1) = g(x)h(x)$, ανν $f(x) = g(x-1)h(x-1)$.

Παράδειγμα. Τα ***κυκλοτομικάπολυώνυμα*** $\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + 1$. Αρκεί να θέσουμε $x = x + 1$, οπότε λαβαίνουμε $\frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + px^{p-2} + \ldots + p$, και το πολυώνυμο αυτό, σύμφωνα με το κριτίριο του Eisenstein είναι ανάγωγο εν $Q[x]$..

Με την ίδια μέθοδο αποδεικνύεται ότι και το $\frac{x^{p^2}-1}{x^p-1} = x^{p(p-1)} + x^{p(p-2)} + \ldots + x^p + 1$ είναι ανάγωγο εν $Q[x]$..

2. Πολυώνυμα ανάγωγα εν F[x]. Έστω πολυώνυμο $f \in \Delta[x]$. Το στοιχείο ρ του δακτυλίου Δ καλείται ***ρίζα*** του f ***πολλαπλότητος*** k, αν και μόνον αν, το $(x-\rho)^k \mid f$, αλλά το $(x-\rho)^{k+1}$ δεν διαιρεί το f. Από τον αλγόριθμου του Ευκλείδη, είναι, $f = (x-\rho)^k q(x) + r(x)$, με $\deg r(x) = 0$, (βλέπε §25), Άρα, $r \in F$ και επειδή $(x-\rho)^k \mid f$, $r = 0 \in F$. Άρα, $f(\rho) = 0$.
Ο μ.κ.δ. των πολυωνύμων $x-\rho$ και $q(x)$ είναι ο $x^0 = 1$. Έχουμε, επίσης, $\deg f = k + \deg q$.
Επαγωγικά, έχουμε το θεώρημα.

Θεώρημα. Έστω το $f \in \Delta[x]$, με $\deg f \neq 0$, και ρ_i, $1 \le i \le k$, k ρίζες αυτού, με πολλαπλότητα αντίστοιχα, $k_1 \le k_i \le k_k$. Τότε, $f = (x-\rho_1)^{k_1} \cdots (x-\rho_k)^{k_k} q(x)$, όπου $q(x) \in \Delta[x]$, και $q(\rho_i) \neq 0$, $1 \le i \le k$, και με $k_1 + k_2 + \ldots + k_k \le \deg f$. Άρα, το f έχει το πολύ $\deg f$ ρίζες.

Παρατήρηση. Στην περίπτωση, που έχουμε ακεραία περιοχή D, η ανάλυση του f σε γινόμενο πρώτων παραγόντων, είναι μοναδική. Αν όμως έχουμε απλά δακτύλιο Δ, τότε η ανάλυση του f σε γινόμενο πρώτων παραγόντων δεν είναι μοναδική. Γιά παράδειγμα, έστω ότι έχουμε τον δακτύλιο Z_8 και το πολυώνυμο $f(x) = x^3 \in Z_8[x]$. Είναι, τότε, $f(0) = f(2) = f(2k) = 0$. Το $f(x)$ δεν έχει μοναδική ανάλυση σε γινόμενο πρώτων παραγόντων. Π.χ. $f = x^3 = x(x-4)^2 = (x-2)(x-4)^2$.
Ένα πολυώνυμο εν $F[x]$ είναι δυνατόν να αναλύεται σε γινόμενο παραγόντων, και όμως να μη έχει ρίζες εν F. Για παράδειγμα, το $(x^2+x+1)^2 \in Q[x]$.

Μία ***πολυωνυμική συνάρτηση*** p(x) λαβαίνεται, αν υποθέσουμε ότι το στοιχείο u, που χρησιμοποιήσαμε παραπάνω για να ορίσουμε ένα πολυώνυμο, είναι στοιχείο της D, F. Αυτόματα τότε, οι προηγούμενες σχέσεις που ορίζουν το άθροισμα και το γινόμενο δύο πολυωνύμων, γίνονται οι ταυτότητες (σχέσεις δηλαδή, που ισχύουν για κάθε $x \in D, F$)

$$(f+g)(x) = f(x)+g(x) \text{ και } fg(x) = f(x)g(x).$$

Πρόταση. Η πολυωνυμική συνάρτηση f(x) διαιρείται από την x−ρ, αν και μόνον αν f(ρ) = 0.

Απόδειξη. Εστω $f(x) = \sum_{k=0}^{n} \alpha_k x^k$. Είναι,

$$\sum_{k=0}^{n} \alpha_k x^k - \sum_{k=0}^{n} \alpha_k \rho^k = \sum_{k=0}^{n} \alpha_k (x^k - \rho^k) = \sum_{k=1}^{n} \alpha_k (x-\rho)(x^{k-1} + x^{k-2}\rho + \ldots + \rho^{k-1})$$

ή f(x) = f(ρ)+(x−ρ)s(x), όπου s(x) πολυωνυμική συνάρτηση βαθνού n−1.

Πόρισμα. Το υπόλοιπο ενός πολυωνύμου p(x), όταν διαιρεθεί με το (x−γ), είναι το p(γ).
Απόδειξη. Εχουμε ότι, p(x) = (x−γ)q(x)+r(x).

Πόρισμα. Έστω $f \in F[x]$. α) Αν $\deg f(x) = 1$, το f είναι ανάγωγο εν F[x]. β) Αν $\deg f(x) \ge 2$ και το f είναι ανάγωγο εν F[x], το f δεν έχει ρίζα εν F. γ) Αν $\deg f(x) = 2$ ή 3 και το f δεν έχει ρίζες εν F, τότε, το f είναι ανάγωγο εν F[x].

Πόρισμα. Αν δύο πολυωνυμικές συναρτήσεις $f, g \in \Delta[x]$, βαθμού $\deg f,\ \deg g \le n$, ταυτίζονται σε $n+1$ σημεία τους, είναι ίσες.
Απόδειξη. Έστω ότι, $h = f - g$, $\deg h \le n$. Τότε το h, έχει $n+1$ ρίζες, αντίθετα με το γεγονός ότι, το h είναι δυνατόν να έχει το πολύ n ρίζες. Άρα, $h = 0$.

Πρόταση. Εστω το $p(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ με συντελεστές α, ακεραίους. Κάθε ρητή ρίζα της εξισώσεως p(x) = 0, έχει τότε την μορφή $\frac{r}{s}$, όπου $r \mid \alpha_0$ και $s \mid \alpha_n$.
Απόδειξη. Θεωρούμε ότι, (r, s) = 1. Είναι τότε,

$$0 = s^n p\left(\frac{r}{s}\right) = \alpha_n r^n + \alpha_{n-1} r^{n-1} s + \ \ldots \ + \alpha_0 s^n$$

Αρα και, $-\alpha_n r^n = s(\alpha_{n-1} r^{n-1} + \cdots + \alpha_0 s^{n-1})$ οπότε, $s \mid \alpha_n r^n$, και συνεπώς, $s \mid \alpha_n$.
Επίσης, $-\alpha_0 s^n = r(\alpha_n r^{n-1} + \cdots + \alpha_1 s^{n-1})$ οπότε, $r \mid \alpha_0 s^n$, και συνεπώς, $r \mid \alpha_0$.

Πόρισμα. Κάθε ρητή ρίζα ενός monic πολυωνύμου με ακεραίους συντελεστές, είναι ακέραιος.

Παράδειγμα. Να βρεθούν οι ρητές ρίζες του $p(x) = 6x^3 - 2x^2 + 3x + 4$.
Λύση. Αν r/s μία ρητή ρίζα του p(x), πρέπει $r \mid 4$ και $s \mid 6$. Οι δυνατοί διαιρέτες είναι οι ±1, ±2, ±4 για τον r, και ±1, ±2, ±3, ±6 για τον s. Οι δυνατές ρητές ρίζες είναι λοιπόν, r/s = ±1, ±1/2, ±1/3, ±1/6, ±2, ±2/3, ±4, ±4/3. Ομως για τις τιμές αυτές, το p(x) δεν μηδενίζεται. Αρα το p(x) δεν έχει ρητή ρίζα.

Ορισμός. Ένα σώμα F λέγεται ***αλγεβρικά κλειστό,*** αν και μόνον αν πληροί μία από τις παρακάτω ισοδύναμες συνθήκες.
1) Κάθε πολυώνυμο $f \in F[x]$ με βαθμό $\deg f(x) > 0$, έχει μία τουλάχιστον ρίζα εν F.
2) Κάθε πολυώνυμο $f \in F[x]$ με βαθμό $\deg f(x) > 0$, διασπάτε εν F[x] σε γινόμενο παραγόντων πρώτου βαθμού.
3) Τα ανάγωγα πολυώνυμα του F[x] είναι τα πολυώνυμα του πρώτου βαθμού.

Οι ρίζες του $f(x) \in \mathbb{R}[x]$ είναι συζυγείς μιγαδικοί αριθμοί. Πράγματι, αν r μιγαδική ρίζα του $f(x)$, $f(r) = 0$, οπότε και, $\bar{f}(r) = f(\bar{r}) = 0$.

3. Πολυωνυμικές διαφορές. Στην παράγραφο αυτή, θα μεταφέρουμε την μεθοδολογία, που αναπτύξαμε στην § 16 σχετικά με τον τελεστή Δ, όταν ο χώρος που μελετάμε, είναι ο F[x].
Έστω, λοιπόν, πολυωνυμική συνάρτηση $f \in F[x]$, και x_i, $0 \le i \le n, n+1$ σημεία του πεδίου ορισμού της, σε γεωμετρική πρόοδο. Υποθέτουμε, δηλαδή, ότι $x_i = x_0 + ih$, όπου h σταθερά. Χρησιμοποιούν συνήθως και το σύμβολο Δx, για να δηλώσουν την σταθερά h.

Ορισμός. $\Delta f = f(x+h) - f(x)$. Η Δf καλείται ***πεπερασμένη διαφορά*** του f. Είναι, $\Delta : F[x] \to F[x]$. Επαγωγικά, ορίζουμε και $\Delta^n y = \Delta(\Delta^{n-1} y)$, όπου $y = f(x)$, $2 \le n$, $n \in \mathbb{N}$, $\Delta^1 = \Delta$ και, τέλος, $\Delta^0 = 1$, η ταυτοτική απεικόνιση $\Delta^0 f = f$.

Παρατήρηση. Αν $\deg f = n$, $\deg \Delta f = n - 1$ οπότε και, $\Delta^k f = 0$, για $k > n$, ενώ για $k = n$, η εικόνα $\Delta^k f$ του πολυωνύμου f, είναι πολυώνυμο μηδενικού βαθμού (δηλαδή, μία σταθερά).

Παράδειγμα. Αν $f(x) = x^2$ και $h = 1$, $\Delta f = (x+1)^2 - x^2 = 2x + 1$

και $\Delta^2 f = \{2(x+1)+1\} - \{2x+1\} = 2$. Για $n \geq 3$, $\Delta^n(x^2) = 0$.
Στην γενική περίπτωση, που $f(x) = a_0 x^n + a_1 x^{n-1} + \ \dots \ + a_n$, $\Delta f = n! a_0 h^n$.

Ο τελεστής Δ είναι γραμμικός: $\Delta(\lambda f + \mu g) = \lambda \Delta f + \mu \Delta g$, και έχει την ιδιότητα, $\Delta^m(\Delta^n f) = \Delta^{m+n} f$. Από τον ορισμό του Δf έπεται ότι, $f(x+h) = f(x) + \Delta f(x)$. Από τις προηγούμενες ιδιότητες έχουμε ότι, $f(x+h) = (1+\Delta) f(x)$, και, εφαρμόζοντας αυτή την σχέση n φορές διαδοχικά, $f(x+nh) = (1+\Delta)^n f(x)$. Τέλος, όπως και στην απόδειξη του τύπου του αθροίσματος του Newton (§16), λαβαίνουμε την σχέση,

$$f(x+nh) = \sum_{k=0}^{n} C(n,k) \Delta^k f(x).$$

Ο τύπος αυτός, σε συνδιασμό με την ταυτότητα $\Delta = (1+\Delta) - 1$ και το ανάπτυγμα του διωνύμου δίδουν την σχέση $\Delta^n f = [(1+\Delta)-1]^n f = \sum_{k=0}^{n} (-1)^k C(n,k)(1+\Delta)^{n-k}$, ή τέλος,

$$\Delta^n f(x) = \sum_{k=0}^{n} (-1)^k C(n,k) f(x+(n-k)h).$$

Ορισμός. Η ***γενικευμένη δύναμη*** $x^{[n]}$ του x, ορίζεται ως $x^{[n]} = \prod_{k=1}^{n} (x-(n-k)h)$.

Η γενικευμένη δύναμη του x συμπίπτει με την δύναμη του x, όταν h = 0.
Εφαρμόζουμε τον τελεστή Δ επί του $x^{[n]}$. Έχουμε,

$$\Delta x^{[n]} = (x+h)^{[n]} - x^{[n]} = (x+h)\prod_{k=2}^{n}(x+h-(n-k)h) - \prod_{k=1}^{n}(x-(n-k)h) =$$

$$\prod_{k=2}^{n}(x-(n-k)h)\{(x+h)-[x-(n-1)h]\} = \prod_{k=2}^{n}(x-(n-k)h)nh = nhx^{[n-1]}$$

Είναι, δηλαδή, $\Delta x^{[n]} = nhx^{[n-1]}$ (1). Επαγωγικά, βρίσκουμε ότι,

$$\Delta^k x^{[n]} = n(n-1) \ \cdots \ (n-k+1)h^k x^{[n-k]}.$$

Φανερά, για $k > n$, $\Delta^k x^{[n]} = 0$.

Εφαρμογή. Ο τύπος (1) δίδει τον εξής τύποι αθροίσεως: Έστω τα $n+1$ σημεία x_i, $0 \leq i \leq n$, με $x_i = x_0 + ih$. Θεωρούμε το άθροισμα $s_n = \sum_{i=0}^{n-1} x_i^{[k]}$. Από την (1) έχουμε, $x^{[k]} = \frac{\Delta x^{[k+1]}}{h(k+1)}$. Άρα και,

$$s_n = \sum_{i=0}^{n-1} x_i^{[k]} = \frac{x_n^{[k+1]} - x_0^{[k+1]}}{h(k+1)}.$$

Εφαρμογή. Ο ***τύπος παρεμβολής του Newton.*** Ζητάμε να βρούμε ένα πολυώνυμο f(x), το οποίο σε n σημεία x_i, $0 \leq i \leq n-1$, να λαβαίνει τις τιμές y_i. Δοκιμάζουμε το πολυώνυμο

$$f(x) = a_0 + a_1(x-x_0) + a_2(x-x_0)(x-x_1) + \ \dots \ + (x-x_0) \ \cdots \ (x-x_{n-1})$$

και θα πρέπει να προσδιορίσουμε τους συντελεστές a, έτσι ώστε $f(x_i) = y_i$.
Παρατηρούμε ότι, το f γράφεται

$$f(x) = a_0 + a_1(x-x_0)^{[1]} + a_2(x-x_0)^{[2]} + \ \dots \ + a_n(x-x_0)^{[n]}.$$

Θέτουμε $x = x_0$ και λαβαίνουμε $a_0 = f(x_0) = y_0$. Στη συνέχεια, σχηματίζουμε το Δf:

$$\Delta f = a_1 h + 2a_2 (x - x_0)^{[1]} h + 3a_3 (x - x_0)^2 h + \ \ldots + n a_n (x - x_0)^{n-1} h \ .$$

Θέτουμε $x = x_0$ και λαβαίνουμε $a_1 = \dfrac{\Delta f(x_0)}{h} = \dfrac{y_0}{h}$. Σχηματίζουμε το $\Delta^2 f$, και για $x = x_0$, λαβαίνουμε, $a_2 = \dfrac{\Delta^2 f(x_0)}{2! h^2} = \dfrac{\Delta^2 y_0}{2! h^2}$, κ.ο.κ., $a_k = \dfrac{\Delta^k f(x_0)}{k! h^k} = \dfrac{\Delta^k y_0}{k! h^k}$, $0 \le k \le n$.

Το ζητούμενο πολυώνυμο είναι, λοιπόν, το $f(x) = \sum_{k=0}^{n} \dfrac{\Delta^k y_0}{k! h^k} (x - x_0)^{[k]}$ (2).

Εκτελούμε, τέλος, τον μετασχηματισμό $q = \dfrac{x - x_0}{h}$, οπότε και,

$\dfrac{(x - x_0)^{[k]}}{h} = \prod_{i=0}^{k-1} \left\{ \dfrac{(x - x_0 - ih)}{h} \right\}$, και ο τύπος (2) λαβαίνει την τελική του μορφή, που είναι η

$$f(x) = y_0 + q\Delta y_0 + \frac{q(q-1)}{2!} \Delta^2 y_0 + \ \ldots \ + \frac{q(q-1) \ \cdots \ (q-n+1)}{n!} \Delta^n y_0 \ . \quad (3)$$

4. Παραγώγιση πολυωνύμου. Έστω το n-βαθμού πολυώνυμο $f \in F[x]$, F αντιμε-ταθετικό σώμα, $f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \ \cdots \ + \alpha_1 x + \alpha_0$. Το $n-1$ βαθμού πολυώνυμο $f' \in F[x]$, όπου $f'(x) = n\alpha_n x^{n-1} + (n-1)\alpha_{n-1} x^{n-2} + \ \cdots \ + \alpha_1$, καλείται ***παράγωγος*** του f.

Η απεικόνιση $D : F[x] \to F[x]$, που ορίζεται από την σχέση $f \mapsto f'$ καλείται ***παραγώγιση*** του f. Γράφουμε και $f' = Df$. Η απεικόνιση αυτή D, είναι μία injection, που έχει τις ιδιότητες:

α) $D(\alpha f + \beta g) = \alpha Df + \beta Dg$, $\alpha, \beta \in F$, (γραμμική ιδιότης), και,

β) $D(fg) = fDg + gDf$ (κανόνας του Leibniz).

Η ιδιότης του Leibniz γιά το γινόμενο δύο πολυωνύμων f και g, γενικεύεται και για το γινόμενο n πολυωνύμων f_i: $D(f_1 \ \cdots \ f_i \ \cdots \ f_n) = \sum_{i=1}^{n} f_1 \ \cdots \ Df_i \ \cdots \ f_n$. Ιδιαίτερα, έχουμε ότι, $D(f^k) = kf^{k-1} Df$.

Επαγωγικά, ορίζεται η ***n-παράγωγος*** της f, $f^{(n)}$, από την σχέση, $f^{(n)} = f^{(n-1)'}$. Γράφουμε και, $D^n f = f^{(n)}$, $D^0 f = f$. Ο κανόνας του Leibniz σε συνδυασμό με την γραμμική ιδιότητα δίδουν γιά την k παράγωγο του γινομένου δύο συναρτήσεων f και g έναν τύπο ανάλογο με τον τύπο του δυωνύμου του Newton (βλέπε §13): $D^n(fg) = \sum_{r=0}^{n} C(n,r)(D^r f)(D^{n-r} g)$.

Στην περίπτωση, που ζητάμε την n παράγωγο ενός n-βαθμού πολυωνύμου $f \in F[x]$ βρίσκουμε, ότι, $D^n f = n! \alpha_n$. Είναι, λοιπόν, $D^{n+1} f = 0$.

Θεώρημα. Έστω $f \in F[x]$, F αντιμεταθετικό σώμα, χαρακτηριστικής $\neq p$, p πρώτος. Το πολυώνυμο f έχει μία πολλαπλή ρίζα $\rho \in F$, ανν, $f(\rho) = f'(\rho) = \ \ldots \ = f^{(k-1)} = 0$, k η πολλαπλότης της ρίζας.

Απόδειξη. Γράφουμε, $f = (x - \rho)^k q(x)$.

Τότε, και $f' = k(x - \rho)^{k-1} q(x) + (x - \rho)^k q'(x)$. Επαγωγικά, ολοκληρώνεται η από-δειξη του θεωρήματος.

Πόρισμα. α) Αν το f(x) έχει ρίζα ρ πολλαπλότητας k, το f΄(x) έχει ρίζα ρ πολλαπλότητας k-1. Αν το f(x) έχει την ρ ως ***απλή*** ρίζα, (k = 1), το f΄(x) δεν έχει ρίζα το ρ. β) Αν το f΄(x) έχει ρίζα ρ πολλαπλότητας k-1 και f(ρ) = 0, τότε η ρ είναι ρίζα του f πολλαπλότητας k.

Παρατήρηση. Στην περίπτωση, που το σώμα F έχει χαρακτηριστική p (p πρώτος) και $(p,n)=1$, $n=\deg f$, $f=x^n-1$, το f έχει μόνον απλές ρίζες, μιά και $f'=nx^{n-1}$, $n\neq 0 \bmod p$, και συνεπώς, αν $f'(\rho)=0$, τότε και $\rho=$ πολλαπλάσιο του p, άρα $\rho^n-1\neq 0(\bmod p)$.

Τύπος του Taylor. Έστω το πολυώνυμο $f(x)=\lambda_n x^n+\lambda_{n-1}x^{n-1}+\cdots+\lambda_1 x+\lambda_0$, $f\in R[x]$. Θέτουμε, $x=y+\xi$, οπότε

$$f(x)=\Lambda_n(x-\xi)^n+\Lambda_{n-1}(x-\xi)^{n-1}+\cdots+\Lambda_1(x-\xi)+\Lambda_0 .$$

Είναι, $\Lambda_0=f(\xi)$. Επίσης, $f'(x)=n\Lambda_n(x-\xi)^{n-1}+(n-1)\Lambda_{n-1}(x-\xi)^{n-2}+\cdots+\Lambda_1$ απ' όπου έχουμε ότι, $\Lambda_1=f'(\xi)$. Με τον ίδιο τρόπο, $\Lambda_2=f'(\xi)/2!$, κ.λ.π., $\Lambda_n=f^{(n)}(\xi)/n!$. Είναι, λοιπόν,

$$f(x)=\frac{f^{(n)}(\xi)}{n!}(x-\xi)^n+\frac{f^{(n-1)}(\xi)}{(n-1)!}(x-\xi)^{n-1}+\cdots+f'(\xi)(x-\xi)+f(\xi).$$

5. Ρίζες πολυωνύμων βαθμού ≤ 4 εν $C[x]$. α) Εν $C[x]$ το πρωτοβάθμιο πολυώνυμο $x-\rho=0$ έχει πάντα την ρίζα $x=\rho$.

β) Γιά να βρούμε τις ρίζες του δευτεροβαθμίου πολυωνύμου $x^2+\beta x+\gamma$ (2), εφαρμόζουμε, πρώτα τον μετασχηματισμό του Tschirnhaus, $x=u-\beta/2$ (1), οπότε λαβαίνουμε το $(u-\beta/2)^2+\beta(u-\beta/2)+\gamma=u^2-\beta^2/4+\gamma$, απ' όπου είναι,

$u=\pm\sqrt{\frac{\beta^2-4\gamma}{4}}$, και από την (1) υπολογίζουμε την ρίζα του (2), που είναι η $\rho=\frac{-\beta\pm\sqrt{\beta^2-4\gamma}}{2}$. Οι ρίζες είναι πραγματικοί αριθμοί, όταν είναι $\Delta=\beta^2-4\gamma\geq 0$. Αν $\Delta<0$, οι ρίζες είναι συζυγείς μιγάδικοί αριθμοί.

Η ποσότης Δ καλείται ***διακρίνουσα*** του $f(x)$.

Στην περίπτωση, που ο συντελεστής α του x^2 είναι $0<\alpha\neq 1$, $\Delta=\beta^2-4\alpha\gamma$. Γιά $\Delta>0$, είναι $\alpha x^2+\beta x+\gamma=\alpha(x-\rho_1)(x-\rho_2)$.

Γιά $\Delta=0$, είναι $\alpha x^2+\beta x+\gamma=\alpha(x-\rho)^2$, $\rho=-\beta/2$.

Γιά $\Delta<0$, $\alpha x^2+\beta x+\gamma=\alpha(x-\rho)(x-\bar{\rho})$.

Οι ρίζες ρ_1 και ρ_2 του (2) έχουν άθροισμα $\rho_1+\rho_2=-\beta$ και γινόμενο $\rho_1\rho_2=\gamma$. Άρα και,

$\rho_1^2+\rho_2^2=\beta^2-2\gamma$, οπότε και $(\rho_1-\rho_2)^2=\beta^2-4\gamma=\Delta^2$.

Γραφική λύση της $x^2-ux+v=0,\ u,v>0$ **(1΄).** Θεωρούμε το καρτεσιανό επίπεδο Oxy και λαβαίνουμε σ' αυτό τα σημεία $A=(0,1)$ και $B=(u,v)$. Με διάμετρο την AB γράφουμε περιφέρεια κύκλου. Η τομή αυτής με τον άξονα Ox δίδει τις ρίζες της (1΄).

Πράγματι, αν K το κέντρο του κύκλου, $\overrightarrow{OK}=\frac{\overrightarrow{OA}+\overrightarrow{OB}}{2}=\frac{(0,1)+(u,v)}{2}=\frac{(u,1+v)}{2}$ και η ακτίνα του $R^2=\frac{(AB)^2}{4}=\frac{u^2+(1-v)^2}{4}$. Η εξίσωση, λοιπόν, της περιφέρειας του κύκλου αυτού είναι,

$\left(X-\frac{u}{2}\right)^2+\left(Y-\frac{1+v}{2}\right)^2=\frac{u^2+(1-v)^2}{4}$. Για $Y=0$ λαβαίνουμε $X^2-uX+\frac{u^2}{4}+\frac{(1+v)^2}{4}=\frac{u^2+(1-v)^2}{4}$, ή $X^2-uX+v=0$, σχέση που αποδεικνύει ότι τα σημεία $P=(X,0)$ είναι ρίζες της (1΄).

γ) Γιά να βρούμε τις ρίζες του τριτοβαθμίου πολυωνύμου $x^3+\beta x^2+\gamma x+\delta$ (3), εφαρμόζουμε, πρώτα τον μετασχηματισμό του Tschirnhaus, $x=t-\beta/3$ (1), οπότε λαβαίνουμε το $t^3+\left(\frac{\beta^2-2\beta+3\gamma}{3}\right)t-\frac{\beta\gamma-3\delta}{3}$, ή το t^3+pt+q (2). Στην συνέχεια θέτουμε $t=u+v$ (μέθοδος του ***Cardan*** 1545)

και έχουμε το $f(u,v)=u^3+v^3+(3uv+p)(u+v)+q$ (2΄).

Το f μηδενίζεται, αν λάβουμε τιμές u_0, v_0 γιά τα u, v, τέτοιες ώστε, $u_0^3+v_0^3=-q$ και $u_0^3v_0^3=-p^3/27$. Τα u_0^3 και v_0^3 είναι, λοιπόν, ρίζες της δευτεροβαθμίου εξισώσεως $w^2+qw+p^3/27=0$ (3΄). Άρα, $u_0^3,v_0^3=\frac{-q\pm\sqrt{q^2-4p^3/27}}{2}$, με $\Delta=q^2-4p^3/27$.

Έστω, τώρα, $u_0^3=\frac{-q+\sqrt{q^2-4p^3/27}}{2}=g$ και $v_0^3=\frac{-q-\sqrt{q^2-4p^3/27}}{2}=h$. Αν u_0 είναι μιά κάποια κυβική ρίζα του g, τότε, οι άλλες δύο ρίζες θα είναι οι ωu_0 και ω^2u_0 (ω, μία κυβική ρίζα της μονάδος, βλέπε §20). Εξ' άλλου, από την στιγμή που η u_0 επελέγει, η v_0 αναγκαστικά, προσδιορίζεται από την ισότητα $u_0v_0=-p/3$. Από την στιγμή που προσδιορίσαμε την v_0, και οι ωv_0, ω^2v_0 είναι κυβικές ρίζες του h. Από τις δύο τριάδες u_0, ωu_0, ω^2u_0 και v_0, ωv_0, ω^2v_0 που λάβαμε, τα ζεύγη (u_0,v_0), $(u_0\omega,v_0\omega^2)$ και $(u_0\omega^2,v_0\omega)$, δίδουν τις ρίζες (u_0^3,v_0^3) της (3΄). Το (2΄), μηδενίζεται, λοιπόν, από τις τιμές u_0+v_0, $u_0\omega+v_0\omega^2$ και $u_0\omega^2+v_0\omega$. Άρα οι ρίζες της (3) είναι οι

$$\rho_1=u_0+v_0-\frac{\beta}{3},\quad \rho_2=u_0\omega+v_0\omega^2-\frac{\beta}{3}\ \text{ και }\ \rho_3=u_0\omega^2+v_0\omega-\frac{\beta}{3}.$$

Παρατηρούμε ότι, $\rho_1+\rho_2+\rho_3=-\beta$, $\rho_1\rho_2+\rho_1\rho_3+\rho_2\rho_3=\gamma$, $\rho_1\rho_2\rho_3=-\delta$. Άρα και,

$\rho_1^2+\rho_2^2+\rho_3^2=\beta^2-2\gamma$. Την ποσότητα

$(\rho_1-\rho_2)^2(\rho_1-\rho_3)^2(\rho_2-\rho_3)^2=\prod_{i<j}(\rho_i-\rho_j)^2=18\beta\gamma\delta-4\beta^3\delta+\beta^2\gamma^2-4\gamma^3-27\delta^2$,

i, j = 1, 2, 3, την καλούν ***διακρίνουσα*** Δ της κυβικής (3).

Η διακρίνουσα Δ της κυβικής (2) είναι η $D=-4p^3-27q^2$. Χρησιμοποιόντας την D αντί της Δ, έχουμε το συμπέρασμα ότι, μία κυβική εξίσωση με πραγματικούς συντελεστές, έχει ρίζες πραγματικές, αν $D\ge 0$. Αν $D<0$, τότε έχει μία ρίζα πραγματική, και δύο συζυγείς μιγαδικές ρίζες. Γιά την περίπτωση D = 0, οπότε $u_0^3,v_0^3=\frac{-q}{2}$, έχουμε μοναδική ρίζα της (2) την $\rho=u_0+v_0=-2u_0$.

Είναι, $-2^3u_0^3-2pu_0+q=0$ ή $pu_0+3u_0^3=0$, απ' όπου, $u_0^2=-p/3$.

Άρα, η $t^3+pt+q=t^3-3u_0^2t-2u_0^3=t^3+2t^2u_0+u_0^2t-2u_0t^2-4tu_0^2-2u_0^3$

$=(t^2+2tu_0+u_0^2)(t-2u_0)=(t+u_0)^2(t-2u_0)$.

δ) Γιά να βρούμε τις ρίζες του τετερτοβαθμίου πολυωνύμου $x^4+\beta x^3+\gamma x^2+\delta x+\varepsilon$ (4), εφαρμόζουμε, πρώτα τον μετασχηματισμό του Tschirnhaus, $x=t-\beta/4$ (1), οπότε λαβαίνουμε το, t^4+pt^2+qt+r (4΄). Την pt^2+qt+r την μετασχηματίζουμε έτσι ώστε, η (4΄) να γίνει γινόμενο δύο δευτεροβαθμίων πολυωνύμων (μέθοδος ***Descartes*** 1637):

$$t^4+pt^2+qt+r=(t^2+ut+v)(t^2-ut+w)$$

όπου $v+w-u^2=p,\qquad u(w-v)=q,\qquad vw=r.$

Την ποσότητα

$(\rho_1-\rho_2)^2(\rho_1-\rho_3)^2(\rho_1-\rho_4)^2(\rho_2-\rho_3)^2(\rho_2-\rho_4)^4(\rho_3-\rho_4)^2=\prod_{i<j}(\rho_i-\rho_j)^2$, i, j = 1, 2, 3, 4 την καλούν ***διακρίνουσα*** Δ της (4).

6. Μέθοδος Horner. Την μέθοδο αυτή, την χρησιμοποιούμε γιά τον υπολογισμό της τιμής y της πολυωνυμικής συναρτήσεως $y=f(x)\in \mathbb{C}[x]$. Η μέθοδος αυτή, συνίσταται στο να γράψουμε το πολυώνυμο

$y=\lambda_n x^n+\lambda_{n-1}x^{n-1}+\ \cdots\ +\lambda_k x^k+\ \cdots\ +\lambda_1 x+\lambda_0$ στην μορφή

$(\ \ldots\ (((\lambda_n x+\lambda_{n-1})x+\lambda_{n-2})x+\ \ldots\ +\lambda_1)x+\lambda_0)$. Στην συνέχεια, υπολογίζουμε τις τιμές των παρενθέσεων που προέκυψαν, γιά την δοσμένη τιμή του x. Οι πράξεις διευκολείνονται, αν χρησιμοποιήσουμε το σχήμα:

	λ_n	λ_{n-1}	...	λ_0	ξ
+		$\xi\times\beta_n$	...	$\xi\times\beta_1$	
	β_n	β_{n-1}	...	$\beta_0=f(\xi)$	

Γιά παράδειγμα, έστω ότι θέλουμε να υπολογίσουμε την τιμή του $3x^3+2x^2-5x+7$, γιά την τιμή x = 3. Σύμφωνα με το παραποάνω σχήμα του Horner έχουμε,

	3	2	−5	7	3
+		$3\times3=9$	$3\times11=33$	$3\times28=84$	
	3	11	28	91	

Η τιμή $f(3)$ είναι 91

Έστω, τώρα, ότι θέλουμε στο δοθέν πολυώνυμο

$f(x)=\lambda_n x^n+\lambda_{n-1}x^{n-1}+\ \cdots\ +\lambda_1 x+\lambda_0$ να εκτελέσουμε τον μετασχηματισμό $x=y+\xi$ όπου ξ κάποια σταθερά. Το νέο πολυώνυμο που θα προκύψει, είναι το $f(y+\xi)=\Lambda_n y^n+\Lambda_{n-1}y^{n-1}+\ \cdots\ +\Lambda_1 y+\Lambda_0$ (1).

Γιά $y=0$, έχουμε τον σταθερό όρο $\Lambda_0=f(\xi)$. Στη συνέχεια, γράφουμε $f(x)=(x-\xi)f_1(x)+f(\xi)$, όπου το $f_1(x)$ είναι πολυώνυμο βαθμού $n-1$. Η (1) γιά $y=x-\xi$ δίδει

$$f(x)=\Lambda_n(x-\xi)^n+\Lambda_{n-1}(x-\xi)^{n-1}+\ \cdots\ +\Lambda_1(x-\xi)+\Lambda_0=$$

$$(x-\xi)[\Lambda_n(x-\xi)^{n-1}+\Lambda_{n-1}(x-\xi)^{n-2}+\ \cdots\ +\Lambda_1]+f(\xi)=(x-\xi)f_1(x)+f(\xi)$$

οπότε είναι και, $f_1(x)=\Lambda_n(x-\xi)^{n-1}+\Lambda_{n-1}(x-\xi)^{n-2}+\ \cdots\ +\Lambda_1$, και συνεπώς, $\Lambda_1=f_1(\xi)$.

Με τον ίδιο τρόπο, υπολογίζουμε ότι, $\Lambda_2=f_2(\xi)$, κ.ο.κ., $\Lambda_n=f_n(\xi)$, όπου έχουμε ότι, $f_k(x)=(x-\xi)f_{k+1}(x)+f_k(\xi)$, k = 0, 1, . . . , n. Τις τιμές $f_k(\xi)$ τις υπολογίζουμε με την μέθοδο του Horner, χρησιμοποιόντας το σχήμα, που περιγράφεται στο επόμενο παράδειγμα.

Παράδειγμα. Έστω ότι, θέλουμε να εφαρμόσουμε τον μετασχηματισμό του Tschirnhaus στο πολυώνυμο $x^4-8x^3+5x^2+2x-7$. Θέτουμε, λοιπόν, $x=y+2$. Το σχήμα του Hornet δίδει:

$$\begin{array}{lccccl}
1 & -8 & 5 & 2 & -7 & \\
+ & 2\times 1 & 2\times(-6) & 2\times(-7) & 2\times(-12) & \\
\hline
1 & -6 & -7 & -12 & -31=f_1 & \\
+ & 2\times 1 & 2\times(-4) & 2\times(-15) & & \\
\hline
1 & -4 & -15 & -42=f_2 & & \\
+ & 2\times 1 & 2\times(-2) & & & \\
\hline
1 & -2 & -19=f_3 & & & \\
+ & 2\times 1 & & & & \\
\hline
1 & 0=f_4 & & & & \\
\hline
1=f_5 & & & & &
\end{array}$$

Είναι, λοιπόν,
$f(y+2)=y^4-19y^2-42y-31$

7. Εύρεσις φραγμάτων γιά τις ρίζες του πολυωνύμου $f\in\mathbb{C}[x]$**.** Θεωρούμε το n-βαθμού πολυώνυμο $f(x)=\lambda_n x^n+\lambda_{n-1}x^{n-1}+\cdots+\lambda_1 x+\lambda_0$, και υποθέτουμε ότι αυτό έχει m διαφορετικές ρίζες $z_i\in\mathbb{C}$, $1\le i\le m\le n$.

Θεώρημα. Έστω $\Lambda=\max\{|\lambda_i|,\ 1\le i\le n\}$. Είναι, τότε, $|z_i|<1+\dfrac{\Lambda}{|\lambda_n|}$. Όλες, δηλαδή, οι ρίζες του $f(x)$, βρίσκονται μέσα σε έναν κύκλο του μιγαδικού επιπέδου $\mathbb{C}$ με κέντρο το σημείο Ο και ακτίνα $R=1+\dfrac{\Lambda}{|\lambda_n|}$.

Απόδειξη. Λαβαίνουμε $|x|>1$, οπότε

$$\begin{aligned}
|f(x)|&\ge|\lambda_n x^n|-(|\lambda_{n-1}x^{n-1}|+\cdots+|\lambda_1 x|+|\lambda_0|)\\
&\ge|\lambda_n||x^n|-\Lambda(|x^{n-1}|+\cdots+|x|+1)\\
&=|\lambda_n||x^n|-\Lambda\frac{x^n-1}{|x|-1}>\left(|\lambda_n|-\frac{\Lambda}{|x|-1}\right)|x^n|.
\end{aligned}$$

Αν, λοιπόν, $|\lambda_n|-\dfrac{\Lambda}{|x|-1}\ge 0$, δηλαδή, αν $|x|\ge 1+\dfrac{\Lambda}{|\lambda_n|}$, τότε, $|f(x)|>0$.

Ο μετασχηματισμός $x=1/y$ παρέχει άλλο ένα φράγμα γιά τις ρίζες του $f(x)$.

Πόρισμα. Έστω $\lambda_0 \neq 0$ και $K = \max\{|\lambda_i|,\ 0 \le i \le n-1\}$. Τότε, όλες οι ρίζες του $f(x)$ πληρούν την ανισότητα $|z_i| > \dfrac{1}{1+\dfrac{K}{|\lambda_0|}} = r$. Οι ρίζες τελικά του $f(x)$ βρίσκονται στο εσωτερικό ενός δακτυλίου του μιγαδικού επιπέδου με κέντρο το Ο και ακτίνες $0 \le r < |z_i| < R$.

Απόδειξη. Ο μετασχηματισμός $x = 1/y$ δίδει $f(x) = \dfrac{1}{y^n} f'(y)$, όπου $f'(y)$ n-βαθμού πολυώνυμο, το οποίο έχει ως συντελεστή του όρου y^k, $0 \le k \le n$, τον συντελεστή του όρου x^{n-k}. Η εφαρμογή του προηγούμενου κριτηρίου στο $f'(y)$, δίδει την ανισότητα $|z_i| > r$.

Φράγματα γιά τις πραγματικές ρίζες του $f(x)$. Έστω ότι, το $f(x)$ έχει τις m πραγματικές ρίζες ρ_i, $1 \le i \le m$. Θεωρούμε τις εξισώσεις:

$$f(x) = 0,\ f_1(x) = x^n f(1/x) = 0,\ f_2(x) = f(-x) = 0 \text{ και } f_3(x) = x^n f(-1/x) = 0.$$

Με R και κατάλληλο δείκτη, συμβολίζουμε ένα άνω φράγμα αντιστοίχως, των ριζών των προηγουμένων εξισώσεων. Το $1/R$ θα είναι, τότε, ένα κάτω φράγμα. Αν ρ^+ θετική ρίζα του $f(x)$, εφ' όσον υπάρχει, και ρ^- αρνητική, τότε είναι, $1/R_1 \le \rho^+ \le R$ και $-R_2 \le \rho^- \le 1/R_3$.

Θεώρημα του Lagrange. Έστω $\lambda_n > 0$ και λ_{n-k} ο πρώτος από τους αρνητικούς συντελεστές του $f(x)$. Τότε ο $R = 1 + \sqrt[n-k]{\dfrac{B}{\lambda_n}}$,

όπου $B = \max\{|\lambda_i|,\ \lambda_i,$ αρνητικός συντελεστής$\}$, είναι ένα άνω φράγμα των θετικών πραγματικών ριζών του $f(x)$. Το $1/R_1$ είναι ένα κάτω φράγμα των θετικών πραγματικών ριζών του $f(x)$.

Απόδειξη. Έστω $x > 1$. Αν αντικαταστήσουμε κάθε μη αρνητικό συντελεστή του πολυωνύμου $f(x)$ με το μηδέν και κάθε αρνητικό συντελεστή με το B, θα έχουμε, τότε, την ανισό-τητα $f(x) \ge \lambda_n x^n - B(x^{n-k} + \ \dots\ + 1) = \lambda_n x^n - B\dfrac{x^{n-k+1}-1}{x-1}$. Άρα, γιά $x > 1$ έχουμε,

$$f(x) > \lambda_n x^n - B\frac{x^{n-k+1}-1}{x-1} = \frac{x^{n-k+1}-1}{x-1}\left(\lambda_0 x^{\kappa-1}(x-1) - B\right) > \frac{x^{n-k+1}-1}{x-1}\left(\lambda_0 (x-1)^k - B\right).$$

Συνεπώς και γιά $x \ge 1 + \sqrt[n-k]{\dfrac{B}{\lambda_n}} = R$, είναι $f(x) > 0$. Όλες, λοιπόν, οι θετικές ρίζες του $f(x)$ πληρούν την ανισότητα, $x^+ < R$.

Παράδειγμα. Έστω το $2x^5 - 100x^2 + 2x - 1 = 0$. Είναι $B = \max\{100,\ 1\} = 100$. Άρα ένα άνω φράγμα των θετικών πραγματικών ριζών του πολυωνύμου αυτού, είναι το

$$R = 1 + \sqrt[3]{\frac{100}{2}} = 1 + \sqrt[3]{50}$$

Στην συνέχεια, εκτελούμε τον μετασχηματισμό $y = 1/x$, οπότε γιά $x > 1$ λαμβάνουμε, το $-2 + 100y^3 - 2y^4 + y^5 = 0$. Είναι, B = 2, οπότε και

$$R_1 = 1 + \sqrt[3]{1} = 2, \text{ και } r = 1/2 = 0.5.$$

Γιά να βρούμε φράγματα γιά τις αρνητικές ρίζες, θέτουμε, $x = -y$, οπότε η εξίσωσή μες γίνεται $2x^5 + 100x^2 + 2x + 1 = 0$, η οποία δεν έχει αρνητικές ρίζες.

Θεώρημα (Newton). Αν γιά $x=\gamma$, $f(\gamma)\geq 0$, και επίσης, $f^{(k)}(\gamma)\geq 0$, $1\leq k\leq n$. Η τιμή, τότε $R=\gamma$, είναι ένα άνω φράγμα των θετικών ριζών της εξισώσεως $f(x)=0$.
Απόδειξη. Είναι άμεση συνέπεια του τύπου του Taylor, μιά και γιά $x\geq\gamma$, $f(x)\geq 0$, και συνεπώς γιά τις θετικές ρίζες του $f(x)$, ισχύει ότι, $x^{+}\leq\gamma$.

8. Πραγματικές ρίζες του $f\in R[x]$**.** Στην παράγραφο αυτή, θα δούμε με ποιό τρόπο υπολογίζουμε το πλήθος των ριζών του $f(x)$, που βρίσκονται μέσα σε ένα διάστημα της πραγματικής ευθείας (θεώρηματα των ***Sturm*** (1803-1855) και ***Budan-Fourier***). Στην συνέχεια, θα εκθέσουμε τον ***κανόνα των προσήμων*** του ***Descartes.***

Παρατήρηση. Αν γιά ένα κλειστό διάστημα $[\alpha,\beta]\subset R$, ισχύει ότι $f(\alpha)f(\beta)<0$, τότε στο εσωτερικό του διαστήματος $[\alpha,\beta]$, υπάρχει ένας περιττός αριθμός ριζών του f. Αν έχουμε $f(\alpha)f(\beta)>0$, τότε είτε δεν υπάρχει ρίζα στο $[\alpha,\beta]$, είτε έχουμε άρτιο αριθμό ριζών στο εσωτερικό του. (Η κάθε ρίζα μετράται με την πολλαπλότητά της).

Ορισμός. Έστω ένα διατεταγμένο σύνολο πραγματικών αριθμών $\gamma_i\neq 0,\ 1,2\leq i\leq n$. Θα λέμε ότι έχουμε ***μεταβολή προσήμου*** στο διαδοχικό ζεύγος (γ_i,γ_{i+1}), αν και μόνον αν $\gamma_i\gamma_{i+1}<0$. Το πλήθος των μεταβολών προσήμου συμβολίζεται με $\underline{N}(\gamma_1,\gamma_n)$. Γράφουμε $\underline{N}(\gamma)$, αν γνωρίζουμε τα όρια γ_1,γ_n της μεταβολής του γ. Στην περίπτωση, που επιτρέπουμε να έχουμε και μηδενικά ανάμεσα στους αριθμούς γ, έστω m το πλήθος, τούτα τα λαβαίνουμε ως στοιχεία γ, με πρόσημο $(-1)^{m-k}$, όπου $1\leq k\leq m$. Λαβαίνουμε έτσι, τον αριθμό $\overline{N}(\gamma_1,\gamma_n)$. Αντίστοιχα, έχουμε, τον $\overline{N}(\gamma)$. Είναι, $\underline{N}(\gamma)\leq\overline{N}(\gamma)$.

Παράδειγμα. Έστω το σύνολο των πραγματικών αριθμών $\gamma_i\neq 0,\ 1,2\leq i\leq 5$, (1, 0, 0,−3, 1). Εδώ, έχουμε, $m=2,\ k=1,2$. Άρα, $\underline{N}(\gamma)=2$, και $\overline{N}(\gamma)=4$.

Η ***ακολουθία του Sturm*** $f(x),f_1(x),\ \ldots\ ,f_m(x)$ γιά ένα πολυώνυμο $f(x)$ σχηματίζεται ως εξής: $f_1(x)=f'(x)$, $f_2(x)$ είναι το -1 υπόλοιπο της διαιρέσεως του $f(x)$ από το $f_1(x)$, $f_3(x)$ είναι το -1 υπόλοιπο της διαιρέσεως του $f_1(x)$ από το $f_2(x)$, κ.ο.κ. Με $N(\gamma)$ συμβολίζουμε το πλήθος των μεταβολών του προσήμου της ακολουθίας $f(\gamma),f_1(\gamma),\ \ldots\ ,f_m(\gamma)$. Αν κάποιος από τους αριθμούς αυτούς είναι το μηδέν, τον διαγράφουμε από την ακολουθία $f_i(\gamma)$.

Θεώρημα του Sturm. Αν το $f(x)$ δεν έχει πολλαπλές ρίζες και $f(\alpha)\neq 0$, $f(\beta)\neq 0$, τότε, το πλήθος των πραγματικών ριζών που έχει το $f(x)$, όταν $\alpha\leq x\leq\beta$, ισούται με $\underline{N}(\alpha)-\underline{N}(\beta)$.

Πόρισμα. Αν $f(0)\neq 0$, τότε ο αριθμός N_+ των θετικών, και ο αριθμός N_- των αρνητικών ριζών του $f(x)$ είναι, $N_+=\underline{N}(0)-\underline{N}(+\infty)$ και $N_-=\underline{N}(-\infty)-\underline{N}(0)$.

Πόρισμα. Όλες οι ρίζες του n-βαθμού πολυωνύμου $f(x)$ είναι πραγματικές, αν και μόνον αν $\underline{N}(-\infty)-\underline{N}(+\infty)=n$.

Παράδειγμα. Γιά να βρούμε το πλήθος των θετικών και αρνητικών ριζών του πολυωνύμου $f(x)=x^4-4x+1$, υπολογίζουμε τα

$f_1(x)=4x^3-4=4(x^3-1)$, και, επειδή $(x^3-1)x-3x+1=f(x)$, $f_2(x)=3x-1$, και, τέλος, $f_3(x)=1$. Είναι, $f(0)=1,\ f_1(0)=-4,\ f_2(0)=-1,\ f_3(0)=1$, συνεπώς, $\underline{N}(0)=2$, επίσης, υπολογίζουμε ότι, $\underline{N}(-\infty)=2,\ \underline{N}(+\infty)=0$.

Είναι, λοιπόν, $N_+=\underline{N}(0)-\underline{N}(+\infty)=2$, και $N_-=\underline{N}(-\infty)-\underline{N}(0)=0$.

Το $f(x)$ έχει, λοιπόν, δύο θετικές ρίζες. Άρα, έχει ακόμα δύο μιγαδικές ρίζες.

Θεώρημα Butan-Fourier. Έστω το πολυώνυμο $f(x)\,|\,[\alpha,\beta]\subset R$, με $f(\alpha),f(\beta)\neq 0$. Το πλήθος, τότε, $N(\alpha,\beta)$ των πραγματικών ριζών του $f(x)$, που βρίσκονται μέσα στο $[\alpha,\beta]$, είναι $N(\alpha,\beta)=\Delta N-2k$, όπου $\Delta N=\underline{N}(\alpha)-\overline{N}(\beta)$, $\underline{N}(\alpha)$, $\overline{N}(\beta)$ ο αριθμός μεταβολής προσήμου γιά τις ακολουθίες, αντίστοιχα, $f(x),\ f'(x),\ \ldots,f^{(n)}(x)$ (1), όπου $x=\alpha$, και $x=\beta$.

Ο υπολογισμός του $N(x)$, γίνεται εύκολα, αν αναπτύξουμε κατά Taylor το $f(x)$, και στην συνέχεια εφαρμόσουμε τον κανόνα του Horner. Πράγματι είναι, γιά $x=\alpha+h$,

$$f(\alpha+h)=\frac{f^{(n)}(\alpha)}{n!}h^n+\frac{f^{(n-1)}(\alpha)}{(n-1)!}h^{n-1}+\ \cdots\ +f'(\alpha)h+f(\alpha)\quad(2)$$

και γιά $x=\beta+h$,

$$f(\beta+h)=\frac{f^{(n)}(\beta)}{n!}h^n+\frac{f^{(n-1)}(\beta)}{(n-1)!}h^{n-1}+\ \cdots\ +f'(\beta)h+f(\beta)\qquad(3).$$

Το πλήθος, λοιπόν, των μεταβολών του προσήμου της ακολουθίας (1), συμπίπτει με αυτό των συντελεστών των παραστάσεων (2) και (3).

Παράδειγμα. Θα προσδιορίσουμε το πλήθος των πραγματικών ριζών του

$$f(x)=x^3-x^2+2x-3$$

στο διάστημα $[0,2]$.

Προφανώς, το $N(0)=3$, όπως έπεται από την ακολουθία (−3, 2, −1, 1), που προκύπτει από τις παραγώγους του $f(x)$ στο μηδέν. Γιά να βρούμε το $N(2)$, υπολογίζουμε τους συντελεστές του το $f(2+h)$ με την μέθοδο του Horner:

1	−1	2	3	2
+	2	2	8	
1	1	4	[5]	
+	2	6		
1	3	[10]		
+	2			
1	[5]			
[1]				

Έχουμε, λοιπόν, την ακολουθία, (5, 10, 5, 1) απ' όπου είναι, $N(2)=0$.

Άρα, $\Delta N=N(0)-N(2)=3$.

Έχουμε συνεπώς τρείς πραγματικές ρίζες στο διάστημα $[0,2]$.

Κανόνας του Descartes. Προκύπτει από την εφαρμογή του προηγούμενου θεωρήματος στο διάστημα $[0,+\infty]$. Είναι ο εξής: Ο αριθμός των θετικών ριζών του $f(x)$, κάθε ρίζα μετρά με την πολλαπλότητά της, ισούται με τον αριθμό των μεταβολών του προσήμου στην ακολουθία των συντελεστών του πολυωνύμου, όπου μηδενικός συντελεστής δεν προσμετράται, ή είναι μικρότερος απ' αυτόν, κατά ένα άρτιο πολλαπλάσιο.

Γιά τις αρνητικές ρίζες, εφαρμόζουμε τον προηγούμενο κανόνα στο $f(-x)$.

9. Συμμετρικές συναρτήσεις. Μία πολυωνυμική συνάρτηση n μεταβλητών επί ενός σώματος F, έχει την μορφή $f(x_1, x_2, \ldots, x_n) = \sum_{i_1, i_2, \ldots, i_n} \alpha x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ όπου οι συντελεστές $\alpha \in F$.

Ομογενές είναι το $f(x_1, x_2, \ldots, x_n)$ ***βαθμού*** k, αν και μόνον αν, όταν $x_i = ty_i$, $1 \le i \le n$ τότε $f(ty_1, ty_2, \ldots, ty_n) = t^k f(y_1, y_2, \ldots, y_n)$. Παράδειγμα ομογενούς πολυωνύμου τριών μεταβληυών x, y, z δευτέρου βαθμού, αποτελεί το $f(x, y, z) = x^2 + yz$.

Συμμετρικό λέγεται το $f(x_1, x_2, \ldots, x_n)$, αν και μόνον αν, γιά μία οιαδήποτε μετάθεση, βλέπε §11, $p \in S_p$ ισχύει ότι, $f(x_1, x_2, \ldots, x_n) = f(x_{p(1)}, x_{p(2)}, \ldots, x_{p(n)})$. Παράδειγμα ομογενούς και συμμετρικού πολυωνύμου τριών μεταβλητών x, y, z και πρώτου βαθμού, αποτελεί το $f(x, y, z) = x + y + z$. Το $f(x, y, z) = x^2 + yz$ δεν είναι συμμετρικό πολυώνυμο.

Τα ομογενή και συμμετρικά πολυώνυμα τριών μεταβλητών, πρώτου, δευτέρου και τρίτου βαθμού αντίστοιχα, είναι τα $\sigma_1 = x + y + z$, $\sigma_2 = xy + yz + zx$, $\sigma_3 = xyz$.

Τα ομογενή και συμμετρικά πολυώνυμα, καλούνται ***στοιχειώδεις συμμετρικές συναρτήσεις.***

Οι στοιχειώδεις συμμετρικές συναρτήσεις σ_i, $1 \le i \le n$, βαθμού i, εμφανίζονται ως συντελεστές στο ανάπτυγμα του γινομένου $\prod_{i=1}^{n} (x - x_i)$ (1). Είναι,

$$\prod_{i=1}^{n} (x - x_i) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \ \ldots \ + (-1)^n \sigma_n$$

όπου

$$\sigma_1 = x_1 + x_2 + \ \ldots \ + x_n$$
$$\sigma_2 = x_1x_2 + x_1x_3 + \ \ldots \ + x_2x_3 + \ \ldots \ + x_{n-1}x_n$$
$$\ldots \qquad \ldots$$
$$\sigma_n = x_1x_2 \cdots x_n .$$

Στην περίπτωση, που, x_i είναι οι n ρίζες ενός monic πολυωνύμου n βαθμού, τότε, επειδή αυτό λαβαίνει την μορφή (1), έχουμε το συμπέρασμα ότι, το άθροισμα των ριζών του ισούται με τον συντελεστή του όρου n-1 βαθμού, κ.λ.π. το γινόμενο των ριζών ισούται με τον σταθερό όρο του πολυωνύμου.

Θεώρημα. Μία ρητή έκφραση στοιχειωδών συμμετρικών πολυωνύμων, είναι συμμετρικό πολυώνυμο. Αντίστροφα, κάθε συμμετρικό πολυώνυμο, είναι δυνατόν να γραφεί ως ρητή έκφραση στοιχειωδών συμμετρικών συναρτήσεων.

Πόρισμα. Έστω το n βαθμού πολυώνυμο $f(x) \in F[x]$, και $\rho_1, \rho_2, \ldots, \rho_n$ οι ρίζες του. Αν $p(x_1, x_2, \ldots, x_n)$ οιοδήποτε συμμετρικό πολυώνυμο n μεταβλητών επί του F, τότε ο αριθμός $p(\rho_1, \rho_2, \ldots, \rho_n) \in F$.

Παράδειγμα. Έστω το $f(x) \in \mathbb{Q}[x]$, $f(x) = x^2 + 2x - 1$, το οποίο έχει ρίζες $\rho_1 = -1 + \sqrt{2}$ και $\rho_2 = -1 - \sqrt{2}$. Ας λάβουμε, τώρα, ένα οιαδήποτε συμμετρικό πολυώνυμο δύο μεταβλητών, π.χ. το $p(x_1, x_2) = x_1^3 + x_2^3$.

Είναι, τότε, $p(\rho_1, \rho_2) = \rho_1^3 + \rho_2^3 = (-1 + \sqrt{2})^3 + (-1 - \sqrt{2})^3 = -14 \in \mathbb{Q}$.

10. Ορισμός. (Βλέπε και ενότητα "Ακέραιοι Αριθμοί", §10). ***Αλγεβρικός*** επί ενός σώματος F καλείται ένας αριθμός a, ανν, αυτός είναι ρίζα κάποιου πολυωνύμου $f(x) \in F[x]$. Ο a μπορεί και

να μη ανήκει στο F. Για παράδειγμα, ο $a=\sqrt{2}$ είναι ρίζα του $Q[x] \ni x^2-2=0$, αλλά $\sqrt{2} \notin Q$.

Ελάχιστο πολυώνυμο του a, είναι εκείνο ελαχίστου βαθμού monik πολυώνυμο του $F[x]$, που έχει το a ρίζα. Το ελάχιστο πολυώνυμο m(x) του a είναι και μοναδικό. Πράγματι, κάθε άλλο πολυώνυμο $f(x)$ που έχει ρίζα το a, διαιρύμενο από το m(x) δίδει την $f(x)=m(x)q(x)+r(x)$ η οποία, γιά $x=a$ δίδει $r(a)=0$. Έχουμε, λοιπόν, πολυώνυμο $r(x) \in F[x]$ που έχει ρίζα το a, και είναι βαθμού $< \deg m(x)$. Το $r(x)$ είναι συνεπώς το μηδενικό πολυώνυμο, και άρα, $m(x) \mid f(x)$ και επειδή $\deg m(x) =$ ελάχιστος, έπεται ότι το m(x) είναι μοναδικό, και μάλιστα, αυτό διαιρεί κάθε άλλο πολυώνυμο, που έχει το a ρίζα.

Πόρισμα. Δύο πολυώνυμα $f(x)$ και $g(x)$ χωρίς κοινή ρίζα, είναι πρώτα μεταξύ τους.
Μιά και στην περίπτωση που είχαν κοινή ρίζα a, το ελάχιστο πολυώνυμο του a θα διαιρούσε αμφότερα τα πολυώνυμα $f(x)$ και $g(x)$**.**

Πρόταση. Ένα ανάγωγο πολυώνυμο n βαθμού έχει μόνον απλές ρίζες.
Απόδειξη. Έστω ότι το $f(x) \in F[x]$ είχε μία δυπλή ρίζα ρ. Είναι, τότε $f(x)=a_n(x-\rho)^2 g(x)$. Άρα, και $f'(x)=a_n(x-\rho)^2 g'(x)+2a_n(x-\rho)g(x)$. Η ρ είναι ρίζα και του $f'(x)$. Τώρα, επειδή το f είναι ανάγωγο, αναγκαστηκά έχει την μορφή $f(x)=cm(x)$, όπου m(x) το ελάχιστο πολυώνυμο της ρίζας ρ επί του $F[x]$. Όμως, $\deg f' < \deg f$. Άτοπον.

Πρόταση. Ένα ιδεώδες $(p(x)) \neq \{0\}$ του $F[x]$ είναι μέγιστο, ανν το $p(x)$ είναι ανάγωγο εν F.
Απόδειξη. Έστω ότι το $(p(x)) \neq \{0\}$ είναι ένα μέγιστο ιδεώδες του $F[x]$. Τότε, $(p(x)) \subset F[x]$ και συνεπώς, $p(x) \neq F$ Στην περίπτωση που είχαμε ότι $p(x)$, $p(x)=f(x)g(x)$ το $p(x)$ σαν μέγιστο, θα ήταν και πρώτο, άρα είτε $f(x) \in (p(x))$ είτε $g(x) \in (p(x))$. Σε κάθε περίπτωση όμως, ο βαθμός του πολυωνύμου θα ήταν $< \deg p(x)$, άτοπον. Το $p(x)$ είναι, λοιπόν, ανάγωγον.
Αντίστροφα. Έστω το $p(x)$ ανάγωγον επί το F, και έστω N ιδεώδες, με $(p(x)) \subseteq N \subseteq F[x]$. Σύμφωνα με το Θεώρημα της §1, το N είναι κύριο ιδεώδες, συνεπώς, $N=(g(x))$ για κάποιο $g(x) \in N$. Όμως, $p(x) \in N$, άρα $p(x)=g(x)q(x)$. Το $p(x)$ ανάγωγον, άρα είτε το $g(x)$ είτε το $q(x)$ είναι μηδενικού βαθμού. Αν $\deg g(x)=0$, τότε $(g(x))=N=F[x]$. Αν $\deg q(x)=0$, τότε $q(x)=c \in F$ και $g(x)=c^{-1}p(x) \in (p(x))$. Άρα, $N=(p(x))$. Αποκλείεται, λοιπόν η σχέση $(p(x)) \subset N \subset F[x]$. Το $(p(x))$ συνεπώς μέγιστο.

Όπως είδαμε στην ενότητα "Ακέραιοι Αριθμοί" §10, η $a(x) \equiv b(x)$ ανν $b(x)-a(x) \in (p(x))$ είναι μία σχέση ισοδυναμίας επί του $F[x]$. Το $F[x]/(p(x))$ είναι σώμα, μια και το $(p(x))$ μέγιστο ιδεώδες του $F[x]$. Το μηδενικό στοιχείο του $F[x]/(p(x))$ είναι βέβαια το $(p(x))$.

Ορισμός. Έστω F υπόσωμα του σώματος E και $a \in E$. Ορίζουμε την απεικόνιση:

$$\varphi_a : F[x] \to E,$$

από την σχέση $a(x)\varphi_a=(a_n x^n+a_{n-1}x^{n-1}+\ \dots\ +a_0)\varphi_a=a_n a^n+a_{n-1}a^{n-1}+\ \dots\ +a_0$.

Πρόταση. Η απεικόνιση φ_a είναι ένας ομομορφισμός του $F[x]$ επί του E. Επίσης, η ταυτότης $x\varphi_a=a$ δεν είναι τίποτε άλλο, από τον ταυτοτικό ισομορφισμό $a\varphi_a=a$.

Απόδειξη. Θα πρέπει να δείξουμε τις σχέσεις : $(a(x)+b(x))\varphi_a = a(x)\varphi_a + b(x)\varphi_a$ (1) για την πρόσθεση, και $(a(x)b(x))\varphi_a = a(x)\varphi_a b(x)\varphi_a$ (2) για τον πολλαπλασιασμό, όπου
$a(x) = a_n x^n + a_{n-1}x^{n-1} + \ \dots\ + a_0$, $b(x) = b_m x^m + b_{m-1}x^{m-1} + \ \dots\ + b_0 \in F[x]$, $m \geq n$.

Είναι: $a(x)+b(x) = \sum_{\lambda=0}^{m}(a_\lambda + b_\lambda)x^\lambda$, με $a_j = 0$, $n < j \leq m$.

Η σχέση $\sum_{\lambda=0}^{m}(a_\lambda + b_\lambda)x^\lambda = \sum_{\lambda=0}^{m}(a_\lambda)x^\lambda + \sum_{\lambda=0}^{m}(b_\lambda)x^\lambda$ παρέχει την (1).

Είναι: $a(x)b(x) = \sum_{s=0}^{m+n}c_s x^s$, όπου $c_s = \sum_{i+j=s}a_i b_j$. Άρα $(a(x)b(x))\varphi_a = \sum_{s=0}^{m+n}c_s a^s$, που ισούται με το $(a_n a^n + a_{n-1}a^{n-1} + \ \dots\ + a_0)(b_n a^n + b_{n-1}a^{n-1} + \ \dots\ + b_0)$, που είναι το $a(x)\varphi_a b(x)\varphi_b$, οπότε έχουμα και την (2).

Παρατήρηση. Ο πυρήνας $\mathrm{Ker}\varphi_a$ του ομομορφισμού φ_a αποτελείται από το σύνολο των στοιχείων (= πολυωνύμων) του $F[x]$, που μηδενίζονται αν θέσουμε $x = a$.
Είναι, λοιπόν, $\mathrm{Ker}\varphi_a = (p(x))$ όπου το $p(x)$ ανάγωγο, με ρίζα το $a \in E$.

Θεώρημα (Kronecker). Έστω F σώμα και $f(x) \in F[x]$. Υπάρχει τότε μία επέκταση E του F και ένα στοιχείο $a \in E$, το οποίο είναι ρίζα του πολυωνύμου $f(x)$.
Απόδειξη. Έστω ότι το $f(x)$ έχει γίνει γινόμενο αναγώγων εν F πολυωνύμων, και έστω $p(x)$ ένα τέτοιο πολυώνυμο. Ζητάμε να βρούμε μία επέκταση E του F που να περιέχει ένα στοιχείο a τέτοιο ώστε $p(a) = 0$. Το $(p(x))$ μέγιστο ιδεώδες του $F[x]$, και συνεπώς το $F[x]/(p(x))$ είναι σώμα, σύμφωνα με ότι είπαμε παραπάνω. Μπορούμε να ταυτίσουμε το σώμα F με κάποιο υπόσωμα του $F[x]/(p(x))$ μέσω του μορφισμού $\psi : F \to F[x]/(p(x))$ που δίδεται από την, $\alpha\psi = \alpha + (p(x))$, $\alpha \in F$. Η ψ είναι ισομορφισμός. Πράγματι, η σχέση $\alpha\psi + (p(x)) = \beta\psi + (p(x))$ δίδει την $\alpha - \beta = 0 \in F$. Μέσω του ισομορφισμού αυτού, το F ταυτίζεται με το $\{\alpha + (p(x)),\ \alpha \in F\}$. Μπορούμε, συνεπώς, να θεωρούμε το $E = F[x]/(p(x))$ σαν μια επέκταση το $F[x]$. Θα δείξουμε ότι το E περιέχει μία ρίζα a του $p(x)$. Θέτουμε $a = x + (p(x))$, $a \in E$, και θεωρούμε τον ομομορφισμό $\varphi_a : F[x] \to E$. Αν $a(x) = a_n x^n + a_{n-1}x^{n-1} + \ \dots\ + a_0 \in F[x]$, τότε για $a = x + (p(x))$ είναι και
$a(a)\varphi_a = a_n(x + (p(x)))^n + a_{n-1}(x + (p(x)))^{n-1} + \dots + a_1(x + (p(x))) + a_0 \in F[x]/(p(x))$.
$a(x)\varphi_a = a_n(x^n + (p(x))) + a_{n-1}(x^{n-1} + (p(x))) + \dots + a_1(x + (p(x))) + a_0 = p(x) + (p(x)) \in (p(x))$
που είναι το μηδενικό στοιχείο του E. Άρα, το $a = x + (p(x))$ είναι ρίζα του $p(x) \in F[x]/(p(x))$
Άρα και, $f(a) = 0$.

Παράδειγμα. Έστω $F = \mathsf{R}$ και $f(x) = x^2 + 1$, πολυώνυμο ανάγωγο εν R. Το (x^2+1) είναι μέγιστο ιδεώδες του R, και άρα το $\mathsf{R}/(x^2+1) = E$ σώμα. Έστω $a = x + (x^2+1)$. Υπολογίζουμε μέσα στο E το $a^2 + 1 + (x^2+1) = (x + (x^2+1))^2 + 1 = x^2 + 1 + (x^2+1) = (x^2+1) = [0]$. Το a είναι λοιπόν, ρίζα του $f(x)$ εν E. Το σώμα E ταυτίζεται, βέβαια, με το σώμα C των μιγαδικών αριθμών.

Πόρισμα. Το σύνολο των αλγεβρικών αριθμών επί του F αποτελεί σώμα.