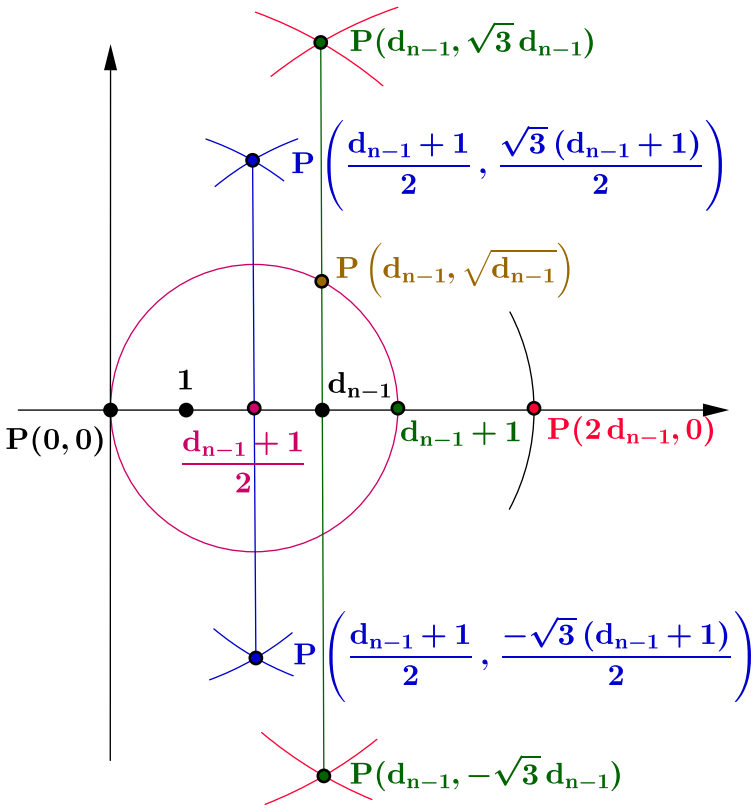
ΓΕΩΜΕΤΡΙΚΕΣ ΚΑΤΑΣΚΕΥΕΣ ΣΤΟ ΕΠΙΠΕΔΟ ΜΕ ΚΑΝΟΝΑ ΚΑΙ ΔΙΑΒΗΤΗ

ΗΛΙΑΣ ΛΑΜΠΑΚΗΣ



4ο ΓΥΜΝΑΣΙΟ ΠΥΡΓΟΥ–ΗΛΕΙΑΣ, 2015

ΕΙΣΑΓΩΓΗ

Η ευθεία και ο κύκλος είναι η πιο απλές και εύκολα κατανοητές γραμμές που συναντάμε γύρω μας στη φύση, στις κατασκευές. Αυτό ώθησε τους Αρχαίους Έλληνες να θεωρήσουν την ευθεία και τον κύκλο ως τα βασικά γεωμετρικά αντικείμενα μέσω των τομών των οποίων κάθε άλλο σημείο στο επίπεδο θα πρέπει να προσδιορίζεται.

Η μακραίωνη προσπάθεια επίλυσης των γνωστών περίφημων τεσσάρων γεωμετρικών προβλημάτων κατασκευών με κανόνα και διαβήτη δηλαδή,

- Ο διπλασιασμός δοθέντος κύβου,
- Η τριχοτόμηση δοθείσης γωνίας,
- Ο τετραγωνισμός δοθέντος κύκλου,
- Η κατασκευή κανονικών πολυγώνων,

οδήγησε στην δημιουργία της θεωρίας των γεωμετρικών κατασκευών στο επίπεδο με κανόνα και διαβήτη. Ειδικότερα, στην διατύπωση και απόδειξη ικανών και αναγκαίων συνθηκών ώστε ένας μιγαδικός αριθμός, (δηλαδή, η εικόνα του στο μιγαδικό επίπεδο), να είναι κατασκευάσιμος με κανόνα και διαβήτη.

Η θεωρία αυτή στις μέρες μας συναντάται στην ελληνική και ξένη βιβλιογραφία σε συμπυκνωμένη μορφή είτε ως παράρτημα είτε κατανεμημένη σε μερικές παραγράφους συγγραμμάτων που έχουν ως κύριο αντικείμενο διαπραγμάτευσης την θεωρία Galois. Σκοπός της παρούσης μονογραφίας είναι να,

- Παρουσιάσει το πλήρες εύρος της θεωρίας γεωμετρικών κατασκευών στο επίπεδο με κανόνα και διαβήτη χωρίς συντομεύσεις, συμπυκνώσεις, με πλήρεις αποδείξεις όλων των ενδιαμέσων βημάτων που απαιτούνται για την διατύπωση και απόδειξη των ικανών και αναγκαίων συνθηκών κατασκευασημότητας μιγαδικών αριθμών με κανόνα και διαβήτη.

- Παρουσιάσει τις αποδείξεις του αδυνάτου, (υπό τον περιορισμό της χρήσης κανόνα και διαβήτη), του διπλασιασμού δοθέντος κύβου, τριχοτόμησης δοθείσης γωνίας, τετραγωνισμού δοθέντος κύκλου. Ιδιαίτερη προσοχή δίνεται στην παρουσίαση της απόδειξης της υπερβατικότητας του π επί του $\mathbb{Q}$ ώστε να είναι όσο το δυνατόν κατανοητή και προσιτή.

- Παρουσιάσει την απόδειξη της ικανής συνθήκης που πρέπει να ικανοποιεί το πλήθος των πλευρών κανονικού n-γώνου ώστε αυτό να είναι κατασκευάσιμο με κανόνα και διαβήτη με τρόπο που να μην εδράζεται ως συνήθως σε αποτελέσματα της θεωρίας Galois ώστε να μην είναι απαραίτητο προαπαιτούμενο η γνώση αυτής. Ουσιαστικά, παρουσιάζεται απόδειξη στηριγμένη στις τεχνικές που αναφέρονται στην αντίστοιχη απόδειξη του Gauss και η οποία σπάνια συναντάται στην βιβλιογραφία.

Η παρούσα αποτελεί δεύτερη «έκδοση» της μονογραφίας που είχε αναρτηθεί τον Δεκέμβριο του 2015 με διορθώσεις τόσο σε τυπογραφικά λάθη όσο και σε λάθος στην απόδειξη της παραγράφου 37. Με την νέα προσέγγιση στην παράγραφο 37 οι παράγραφοι 40, 41 παραλείπονται. Η αρίθμηση των μαθηματικών παραστάσεων από την παράγραφο 42, (μετά την παράλειψη των παραγράφων 40, 41), συνεχίζει όπως ήταν.

ΓΕΩΜΕΤΡΙΚΕΣ ΚΑΤΑΣΚΕΥΕΣ ΣΤΟ ΕΠΙΠΕΔΟ ΜΕ ΚΑΝΟΝΑ ΚΑΙ ΔΙΑΒΗΤΗ

1. Θα συμβολίζουμε με S ένα σύνολο σημείων του επιπέδου πεπερασμένου πλήθους. Θα λέμε ότι δύο επίπεδα σχήματα τέμνονται αν έχουν κοινό ή κοινά σημεία. Υπ΄ αυτή την έννοια και η επαφή θα θεωρείται «εκφυλισμένη» τομή.

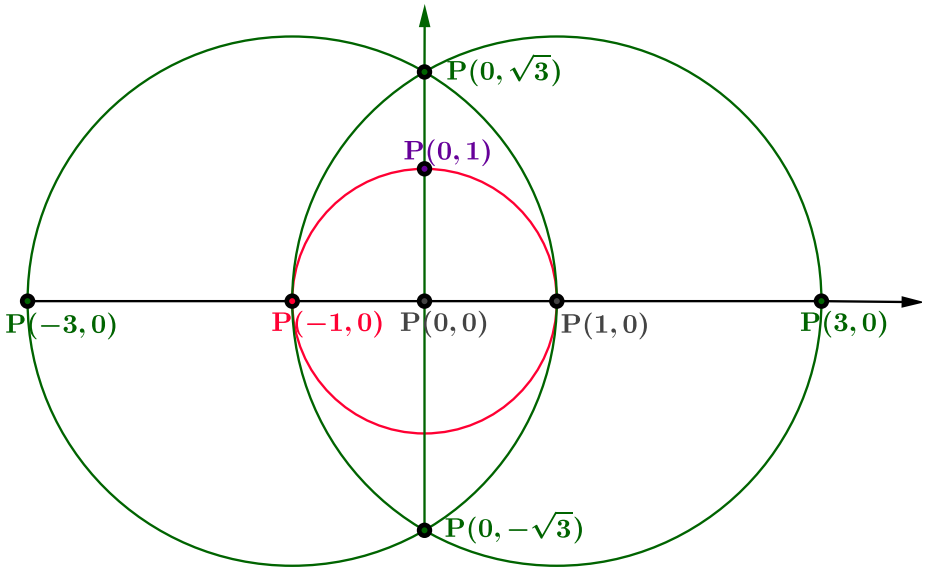
2. Θα λέμε ότι η ευθεία L του επιπέδου είναι μία S-ευθεία αν αυτή διέρχεται από δύο στοιχεία του S, (δηλαδή δύο σημεία που ανήκουν στο S).

3. Θα λέμε ότι ένας κύκλος K είναι ένας S-κύκλος αν το κέντρο του και ένα σημείο του είναι στοιχεία του S.

4. Δοθέντος ευθυγράμμου τμήματος του επιπέδου, λαμβανομένου ως μονάδα μέτρησης των λοιπών ευθυγράμμων τμημάτων του επιπέδου, θα συμβολίζουμε με $P(0,0)$ το ένα άκρο του και με $P(1,0)$ το άλλο άκρο του.

5. Δοθέντος ενός συνόλου S, θέτουμε $S_0 = S$. Θα λέμε ότι ένα σημείο του επιπέδου που δεν ανήκει στο S_0 είναι κατασκευάσιμο με κανόνα και διαβήτη, (κ.κ.δ.), από το S_0 σε 1 βήμα αν το σημείο αυτό ανήκει στην τομή είτε δύο S_0-ευθειών, είτε μίας S_0-ευθείας και ενός S_0-κύκλου, είτε δύο S_0-κύκλων. Το σύνολο όλων των κ.κ.δ. από το S_0 σε 1 βήμα σημείων του επιπέδου μαζί με τα σημεία που ανήκουν στο S_0 θα συμβολίζεται με το S_1. Επαγωγικώς, θα λέμε ότι ένα σημείο του επιπέδου που δεν ανήκει στο S_0 είναι κ.κ.δ. από το S_0 σε n βήματα αν το σημείο αυτό είναι κ.κ.δ. από το S_{n-1} σε 1 βήμα. Από τα προηγούμενα προκύπτει ότι, $S_0 \subset S_1 \subset \cdots \subset S_n$.

6. Έστω $S_0 = \{P(0,0), P(1,0)\}$. Η S_0-ευθεία $L(P(0,0), P(1,0))$ και ο S_0-κύκλος $K(P(0,0), \overline{P(0,0)P(1,0)})$, (με κέντρο το σημείο $P(0,0)$ και ακτίνα το ευθύγραμμο τμήμα $\overline{P(0,0)P(1,0)}$), ορίζουν, (Σχήμα 1), σημείο $P(-1,0)$ αντιδιαμετρικό του $P(1,0)$ και κ.κ.δ. από το S_0 σε 1 βήμα. $P(-1,0) \in S_1$. Οι S_1-κύκλοι $K(P(1,0), \overline{P(1,0)P(-1,0)})$, $K(P(-1,0), \overline{P(-1,0)P(1,0)})$ ορίζουν, (Σχήμα 1), τα σημεία $P(0, \pm\sqrt{3})$ κ.κ.δ. από το S_0 σε 2 βήματα. Άρα, η ευθεία $L(P(0,\sqrt{3}),$



Σχήμα 1.

$P(0,-\sqrt{3})$) είναι S_2-ευθεία κ.κ.δ από το S_0 σε 2 βήματα. Ο S_0 και κατ΄ επέκταση S_2-κύκλος $K(P(0,0),\overline{P(0,0)P(1,0)})$ και η S_2-ευθεία $L(P(0,\sqrt{3}),\ P(0,-\sqrt{3}))$ ορίζουν το σημείο $P(0,1)$ και κατ΄ επέκταση το ευθύγραμμο τμήμα $\overline{P(0,0),P(0,1)}$ είναι κ.κ.δ. από το S_0 σε 3 βήματα. Δείξαμε ότι λαμβανομένου ενός ευθυγράμμου τμήματος $\overline{P(0,0),P(1,0)}$ ως μονάδα μέτρησης των ευθυγράμμων τμημάτων του επιπέδου το γνωστό μας Καρτεσιανό σύστημα αξόνων είναι κ.κ.δ. από το αρχικό σύνολο σημείων του επιπέδου S_0 σε 3 βήματα. Δεν εννοούμε ότι όλοι οι πραγματικοί αριθμοί που θεωρητικώς αντιπροσωπεύονται από τετμημένες και τεταγμένες επί των αξόνων ενός Καρτεσιανού συστήματος είναι κ.κ.δ. από το S_0 σε πεπερασμένο πλήθος βημάτων. Εννοούμε ότι οι δύο κάθετοι μεταξύ τους άξονες εφοδιασμένοι με την ίδια μονάδα μέτρησης ως «γεωμετρικά αντικείμενα» είναι κ.κ.δ. από το S_0 σε πεπερασμένο πλήθος βημάτων.

7. Έστω $F \subseteq \mathbb{C}$. Το F θα λέγεται σώμα αν για κάθε $f_1, f_2 \in F$, τότε και $f_1 \pm f_2 \in F$, $f_1 \cdot f_2 \in F$ και για κάθε $f \in F - \{0\}$ το $f^{-1} \in F$. Από τα προηγούμενα και τις ιδιότητες της πρόσθεσης και του πολλαπλασιασμού στο $\mathbb{C}$ έπεται ότι για $f \in F$, το $0 = f - f \in F$. Για $f \in F - \{0\}$, το $1 = f \cdot f^{-1} \in F$. Για $f \in F$, το $-f = 0 - f \in F$. Η πρόσθεση στο F είναι αντιμεταθετική, προσετεριστική, ο πολλαπλασιασμός είναι αντιμεταθετικός, προσετεριστικός και επιμεριστικός.

Έστω σύνολο S, (παράγραφος 1). Αν οι συντεταγμένες των στοιχείων του S ανήκουν σε σώμα F τότε οι συντελεστές των εξισώσεων των S-ευθειών και των S-κύκλων ανήκουν στο F. Έστω $P(a,b)$, $P(g,d)$ στοιχεία του S με $a,b,g,d \in F$. Έστω L η S-ευθεία που ορίζεται από τα $P(a,b)$, $P(g,d)$. Αν $a = g$ η εξίσωση της L είναι $x + 0\,y - a = 0$ και το συμπέρασμα ισχύει. Αν $b = d$ η εξίσωση της L είναι $0\,x + y - b = 0$ και το συμπέρασμα ισχύει. Αν $a \neq g$ και $b \neq d$ η εξίσωση της L είναι,

$$\frac{d-b}{g-a}\,x - y + \frac{b\,g - a\,d}{g-a} = 0,$$

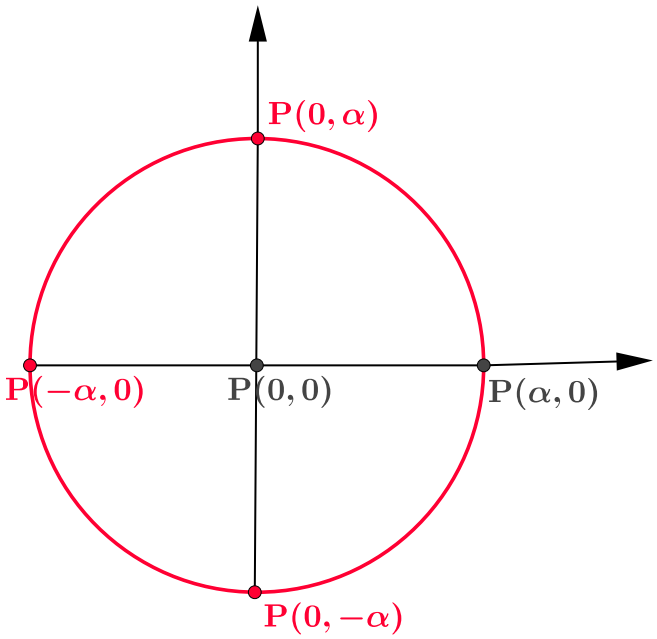
και το συμπέρασμα ισχύει από τις ιδιότητες του σώματος F. Αν $P(a,b)$ το κέντρο και $P(g,d)$ ένα σημείο του S-κύκλου K, η εξίσωση του Κ είναι,

$$(x-a)^2 + (y-b)^2 = (g-a)^2 + (d-b)^2,$$

και το συμπέρασμα ισχύει από τις ιδιότητες του σώματος F.

8. Θα λέμε ότι ένας πραγματικός αριθμός a είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων αν το σημείο $P(a,0)$ είναι κ.κ.δ. από το S_0 σε πεπερασμένο πλήθος βημάτων.

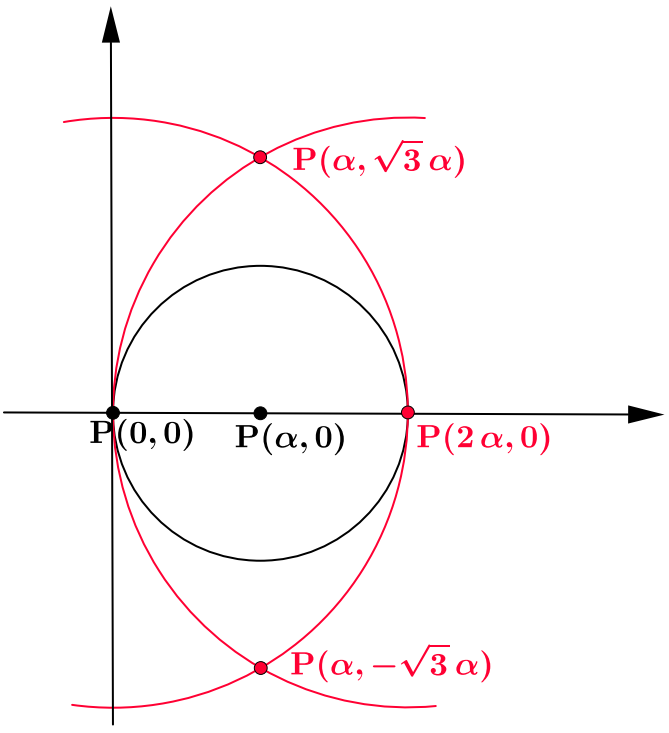
9. Όταν το σημείο $P(a,0)$ είναι κ.κ.δ. από το S_0 σε πεπερασμένο πλήθος βημάτων τότε και τα σημεία $P(0,a)$, $P(-a,0)$, $P(0,-a)$ είναι κ.κ.δ. από το S_0 σε πεπερασμένο πλήθος βημάτων. Έστω ότι το σημείο $P(a,0)$ είναι κ.κ.δ. από το S_0 σε n βήματα, (Σχήμα 2). Τότε ο κύκλος $K(P(0,0),\overline{P(0,0)P(a,0)})$ είναι ένας S_n-κύκλος. Στην παράγραφο 6 δείξαμε ότι ο άξονας $y'y$ είναι κ.κ.δ. από το S_0 σε 2 βήματα. Οπότε ο κύκλος K και ο άξονας $y'y$ είναι S_m-κύκλος και S_m-ευθεία αντιστοίχως, όπου $m = \max\{2,n\}$. Επειδή, $S_0 \subset S_m$ έπεται ότι ο άξονας $x'x$ που είναι μία S_0-ευθεία, είναι και S_m-ευθεία. Τελικώς, τα σημεία $P(0,a)$, $P(-a,0)$, $P(0,-a)$ προσδιορίζονται ως τομές των $x'x$, $y'y$ με τον κύκλο K και ανήκουν στο S_{m+1}. Είναι κ.κ.δ. από το S_0 σε πεπερασμένο πλήθος βημάτων. Ομοίως, αν το $P(0,a)$ είναι κ.κ.δ. και τα $P(a,0)$, $P(-a,0)$, $P(0,-a)$ είναι κ.κ.δ.



Σχήμα 2.

10. Θα λέμε ότι ο μιγαδικός αριθμός $z = a + b\,i$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων αν το σημείο $P(a, b)$ είναι κ.κ.δ. από το S_0 σε πεπερασμένο πλήθος βημάτων.

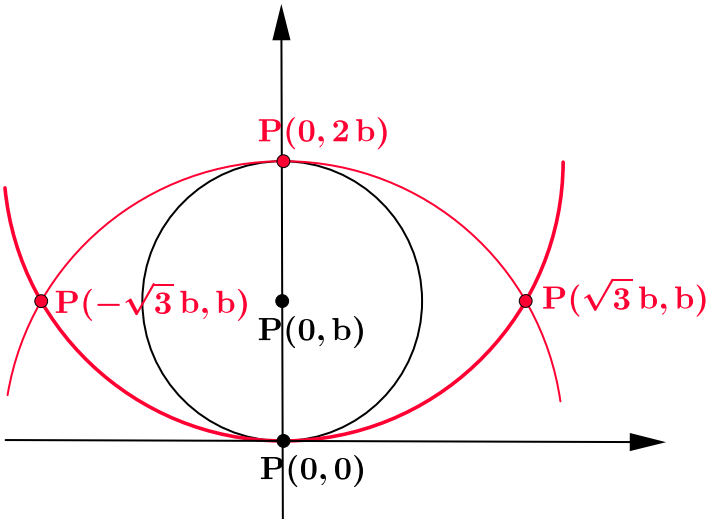
11. Έστω ότι το σημείο $P(a, 0)$ είναι κ.κ.δ. από το S_0 σε πεπερασμένο πλήθος βημάτων. Τότε και τα σημεία $P(a, \pm\sqrt{3}\,a)$ είναι κ.κ.δ. από το S_0 σε πεπερασμένο πλήθος βημάτων. Το $P(a, 0)$ είναι κ.κ.δ. από το S_0 σε n βήματα, (Σχήμα 3).



Σχήμα 3.

Ο άξονας $x'x$ είναι μία S_n-ευθεία. Ο κύκλος $K_1(P(a,0), \overline{P(a,0)P(0,0)})$ είναι ένας S_n-κύκλος. Το σημείο $P(2\,a,0)$ που προσδιορίζεται ως τομή του άξονα $x'x$ και του κύκλου K_1 ανήκει στο S_{n+1}. Οι κύκλοι $K_2(P(0,0), \overline{P(0,0)P(2\,a,0)})$ και $K_3(P(2\,a,0), \overline{P(2\,a,0)P(0,0)})$ είναι S_{n+1}-κύκλοι. Τα σημεία $P(a, \pm\sqrt{3}\,a)$ που προσδιορίζονται ως τομές των κύκλων K_2 και K_3 ανήκουν στο S_{n+2} και άρα είναι κ.κ.δ. από το S_0 σε $n+2$ βήματα.

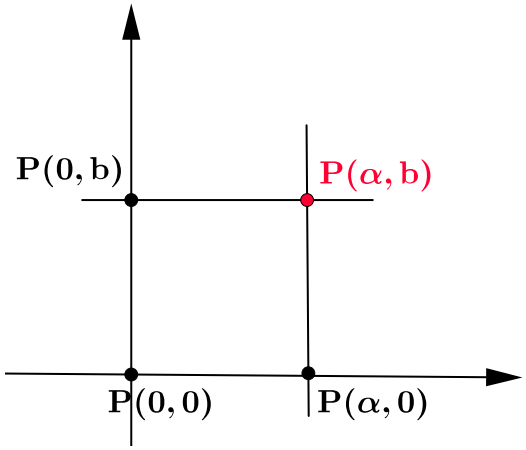
12. Έστω ότι το σημείο $P(0,b)$ είναι κ.κ.δ. από το S_0 σε πεπερασμένο πλήθος βημάτων. Τότε και τα σημεία $P(\pm\sqrt{3}\,b, b)$ είναι κ.κ.δ. από το S_0 σε πεπερασμένο πλήθος βημάτων. Το $P(0,b)$ είναι κ.κ.δ. από το S_0 σε n βήματα, (Σχήμα 4).



Σχήμα 4.

Ο άξονας $y'y$ είναι μία S_n-ευθεία. Ο κύκλος $K_1(P(0,b), \overline{P(0,b)P(0,0)})$ είναι ένας S_n-κύκλος. Το σημείο $P(0,2\,b)$ που προσδιορίζεται ως τομή του άξονα $y'y$ και του κύκλου K_1 ανήκει στο S_{n+1}. Οι κύκλοι $K_2(P(0,0), \overline{P(0,0)P(0,2\,b)})$ και $K_3(P(0,2\,b), \overline{P(0,2\,b)P(0,0)})$ είναι S_{n+1}-κύκλοι. Τα σημεία $P(\pm\sqrt{3}\,b, b)$ που προσδιορίζονται ως τομές των κύκλων K_2 και K_3 ανήκουν στο S_{n+2} και άρα είναι κ.κ.δ. από το S_0 σε $n+2$ βήματα.

13.

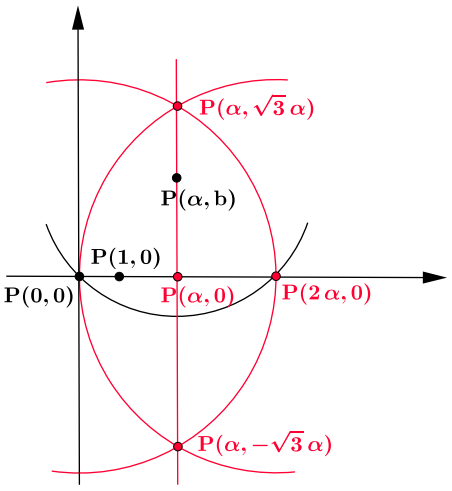


Σχήμα 5.

Έστω ότι τα σημεία $P(a,0)$, $P(0,b)$ με $a\,b \neq 0$ είναι κ.κ.δ. από το S_0 σε πεπερασμένο πλήθος βημάτων. Τότε και το σημείο $P(a,b)$ είναι κ.κ.δ. από το S_0

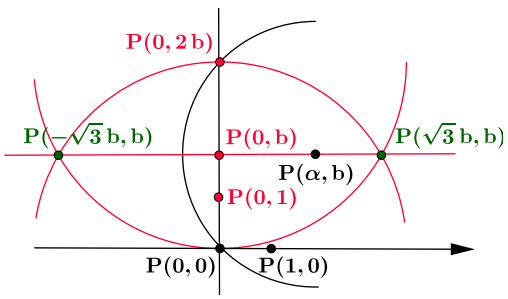
σε πεπερασμένο πλήθος βημάτων. Τα $P(a,0)$, $P(0,b)$ με $a\,b \neq 0$ είναι κ.κ.δ. από το S_0 σε n, m βήματα, (Σχήμα 5). Θέτουμε $k = \max\{n,m\}$. Τότε $S_n \subseteq S_k$ και $S_m \subseteq S_k$. Από τις παραγράφους 11 και 12 προκύπτει ότι τα σημεία $P(a,\sqrt{3}\,a)$ και $P(\sqrt{3}\,b,b)$ ανήκουν στο S_{k+2}. Οι ευθείες $L_1(P(a,0),P(a,\sqrt{3}\,a))$ και $L_2(P(0,b),P(\sqrt{3}\,b,b))$ είναι S_{k+2} ευθείες. Το σημείο $P(a,b)$ που προσδιορίζεται ως τομή των L_1 και L_2 ανήκει στο S_{k+3} και είναι κ.κ.δ. από το S_0 σε $k+3$ βήματα.

14. Αν το σημείο $P(a,b)$ είναι κ.κ.δ. από το S_0 σε πεπερασμένο πλήθος βημάτων τότε και το σημείο $P(a,0)$ είναι κ.κ.δ. από το S_0 σε πεπερασμένο πλήθος βημάτων. Το $P(a,b)$ είναι κ.κ.δ. από το S_0 σε n βήματα, (Σχήμα 6). Ο κύκλος $K(P(a,b),\overline{P(a,b)P(0,0)})$ είναι S_n-κύκλος. Η ευθεία $x'x$ είναι S_n ευθεία. Το σημείο $P(2\,a,0)$ που προσδιορίζεται ως τομή του κύκλου K και της ευθείας $x'x$ ανήκει στο S_{n+1}. Στην παράγραφο 11 δείξαμε ότι αν το $P(2\,a,0)$ ανήκει στο S_{n+1} τότε, τα $P(a,\pm\sqrt{3}\,a)$ είναι κ.κ.δ. από το S_0 σε $n+2$ βήματα. Ο άξονας $x'x$ και η ευθεία $L(P(a,\sqrt{3}\,a),P(a,-\sqrt{3}\,a))$ είναι S_{n+2}-ευθείες. Το σημείο $P(a,0)$ που προσδιορίζεται ως τομή των $x'x$ και L ανήκει στο S_{n+3} και είναι κ.κ.δ. από το S_0 σε $n+3$ βήματα.



Σχήμα 6.

15.



Σχήμα 7.

Αν το σημείο $P(a,b)$ είναι κ.κ.δ. από το S_0 σε πεπερασμένο πλήθος βημάτων τότε και το σημείο $P(0,b)$ είναι κ.κ.δ. από το S_0 σε πεπερασμένο πλήθος βημάτων. Το $P(a,b)$ είναι κ.κ.δ. από το S_0 σε m βήματα, (Σχήμα 7). Ο κύκλος $K(P(a,b),\overline{P(a,b)P(0,0)})$ είναι S_m-κύκλος. Η ευθεία $y'y$ είναι S_2 ευθεία. Αν

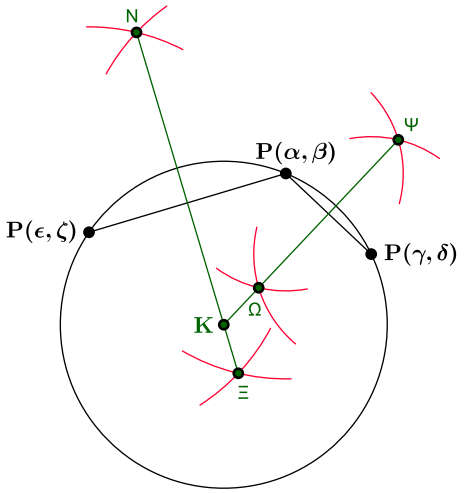
$n = \max\{m, 2\}$, ο κύκλος K και η ευθεία $y'y$ είναι S_n-κύκλος και ευθεία αντίστοιχα. Το σημείο $P(0, 2\,b)$ που προσδιορίζεται ως τομή του κύκλου K και της ευθείας $y'y$ ανήκει στο S_{n+1}. Στην παράγραφο 12 δείξαμε ότι αν το σημείο $P(0, 2\,b)$ ανήκει στο S_{n+1} τότε, και τα $P(\pm\sqrt{3}\,b, b)$ είναι κ.κ.δ. από το S_0 σε $n + 2$ βήματα. Η ευθεία $L(P(\sqrt{3}\,b, b), P(-\sqrt{3}\,b, b))$ είναι μία S_{n+2}-ευθεία. Επειδή, $S_n \subset S_{n+2}$ έπεται ότι η ευθεία $y'y$ είναι S_{n+2}-ευθεία. Το σημείο $P(0, b)$ που προσδιορίζεται ως τομή των $y'y$ και L ανήκει στο S_{n+3} και είναι κ.κ.δ. από το S_0 σε $n + 3$ βήματα.

16. Αν ένας μιγαδικός αριθμός $z = a+b\,i$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων τότε από τις παραγράφους 8, 9, 10, 14, 15 προκύπτει ότι και το $Re(z) = a$, $Im(z) = b$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων.

17. Αν οι πραγματικοί αριθμοί a, b είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων από τις παραγράφους 8, 9, 10, 13 προκύπτει ότι και ο μιγαδικός αριθμός $z = a+b\,i$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων.

18. Αν ο πραγματικός αριθμός b είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων από τις παραγράφους 8, 9, 10 προκύπτει ότι και ο φανταστικός αριθμός $z = b\,i$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων.

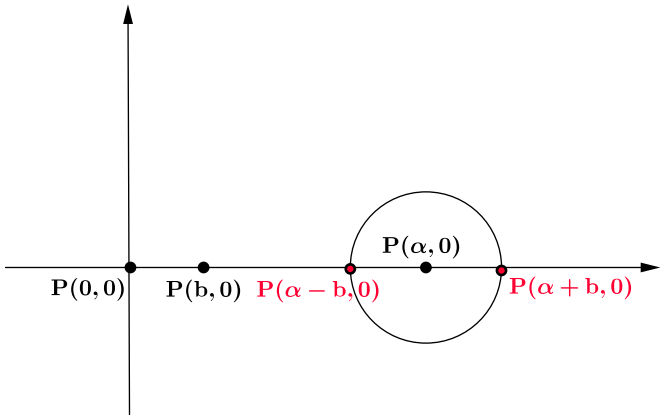
19. Αν τα σημεία $P(a, \beta)$, $P(\gamma, \delta)$, $P(\varepsilon, \zeta)$ είναι κ.κ.δ. από το S_0 σε n, m, k βήματα αντιστοίχως τότε ο κύκλος που ορίζουν είναι ένας S_{t+2}-κύκλος, με $t = \max\{n, m, k\}$, (Σχήμα 8). Τα $P(a, \beta)$, $P(\gamma, \delta)$, $P(\varepsilon, \zeta)$ ανήκουν στο S_t. Οι κύκλοι $K_1(P(a, \beta), \overline{P(a, \beta)P(\gamma, \delta)})$, $K_2(P(\gamma, \delta), \overline{P(\gamma, \delta)P(a, \beta)})$, $K_3(P(a, \beta), \overline{P(a, \beta)P(\varepsilon, \zeta)})$, $K_4(P(\varepsilon, \zeta), \overline{P(\varepsilon, \zeta)P(a, \beta)})$, είναι S_t-κύκλοι. Τα σημεία N, Ξ, Ψ, Ω που ορίζονται ως τομές των S_t-κύκλων K_1, K_2, K_3, K_4, ανήκουν στο S_{t+1}. Οι ευθείες $L_1(N, \Xi)$ και $L_2(\Psi, \Omega)$ είναι S_{t+1}-ευθείες. Το κέντρο του κύκλου K, που ορίζεται ως τομή των S_{t+1}-ευθειών L_1, L_2 ανήκει στο S_{t+2} και είναι κ.κ.δ. από το S_0 σε $t + 2$ βήματα.



Σχήμα 8.

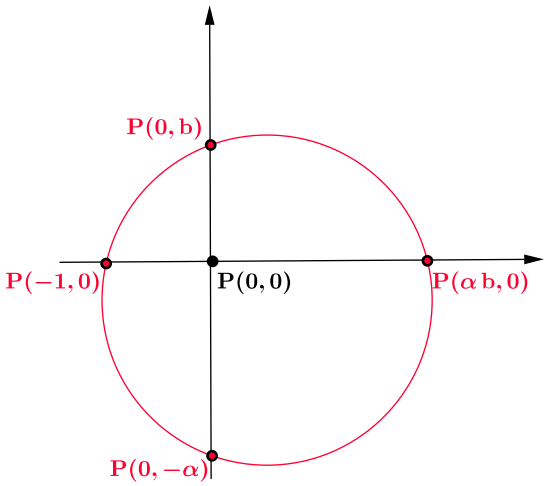
20. Αν ο πραγματικός αριθμός α είναι κ.κ.δ σε πεπερασμένο πλήθος βημάτων τότε οι παράγραφοι 8, 9 συνεπάγονται ότι και ο $-a$ είναι κ.κ.δ σε πεπερασμένο πλήθος βημάτων.

21. Αν οι θετικοί πραγματικοί αριθμοί a, b, με $a > b$, είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων τότε και οι $a+b$, $a-b$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Έστω ότι οι a, b είναι κ.κ.δ σε n, m βήματα αντιστοίχως, (Σχήμα 9). Τα σημεία $P(a,0)$, $P(b,0)$ ανήκουν στο S_t, με $t = \max\{n,m\}$. Ο κύκλος $K(P(a,0), \overline{P(0,0)P(b,0)})$ είναι ένας S_t-κύκλος. Τα σημεία $P(a \pm b, 0)$ που προσδιορίζονται ως τομές του κύκλου K με τον άξονα $x'x$ ανήκουν στο S_{t+1} και είναι κ.κ.δ. από το S_0 σε $t+1$ βήματα.



Σχήμα 9.

22. Αν οι θετικοί πραγματικοί αριθμοί a, b είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων τότε και οι $a\,b$, a/b είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Έστω ότι οι a, b είναι κ.κ.δ. σε n, m βήματα αντιστοίχως, (Σχήματα 10, 11). Τα σημεία $P(a,0)$, $P(b,0)$ ανήκουν στο S_k, με $k = \max\{n,m\}$. Από την παράγραφο 9 προ-

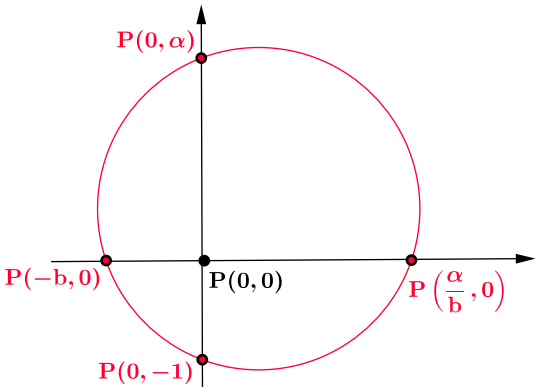


Σχήμα 10.

κύπτει ότι τα σημεία $P(-1,0)$, $P(0,b)$, $P(0,-a)$ ανήκουν στο S_{k+1}. Από την παράγραφο 19 προκύπτει ότι ο κύκλος K που ορίζεται από τα $P(-1,0)$, $P(0,b)$, $P(0,-a)$ είναι ένας S_{k+3}-κύκλος. Το σημείο $P(a\,b,0)$ που προσδιορίζεται ως τομή του κύκλου K με τον άξονα $x'x$ ανήκει στο S_{k+4} και είναι κ.κ.δ. από το S_0 σε $k+4$ βήματα.

Επίσης, τα σημεία $P(-b,0)$, $P(0,-1)$, $P(0,a)$ ανήκουν στο S_t με $t = \max\{k+1, 3\}$. Από την παράγραφο 19 προκύπτει ότι ο κύκλος K που ορίζεται από τα

$P(-b,0)$, $P(0,-1)$, $P(0,a)$ είναι ένας S_{t+3}-κύκλος. Το σημείο $P(a/b,0)$ που προσδιορίζεται ως τομή του κύκλου K με τον άξονα $x'x$ ανήκει στο S_{t+4} και είναι κ.κ.δ. από το S_0 σε $t+4$ βήματα.



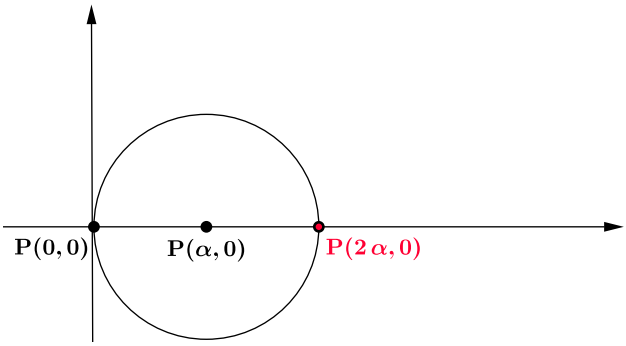
Σχήμα 11.

23. Έστω a, b δύο πραγματικοί αριθμοί, (με $|a|>|b|$), κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Αν $a>0$ και $b>0$ από τις παραγράφους 21, 22 προκύπτει ότι και οι $a\pm b$, $a\,b$, a/b είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων.

Αν $a>0$ και $b<0$ τότε, $|a|>|b| \Rightarrow a>-b>0$ και από τις παραγράφους 20, 21, 22 προκύπτει ότι ο $-b>0$ και κατ΄ επέκταση οι $a\pm(-b)=a\mp b$, $a\,(-b)=-a\,b>0$, $-(-a\,b)=a\,b$, $a/(-b)=-(a/b)>0$, $-(-(a/b))=a/b$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων.

Αν $a<0$ και $b<0$ τότε, $|a|>|b| \Rightarrow -a>-b>0$ και από τις παραγράφους 20, 21, 22 προκύπτει ότι οι $-a>0$, $-b>0$ και κατ΄ επέκταση οι $(-a)\pm(-b)=-(a\pm b)$, $-(-(a\pm b))=a\pm b$, $(-a)\,(-b)=a\,b$, $(-a)/(-b)=a/b$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων.

24. Αν ο θετικός πραγματικός αριθμός a είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων τότε και ο $n\,a$, (με $n\in\mathbb{N}-\{0\}$), είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Έστω ότι ο a είναι κ.κ.δ. σε m βήματα, (Σχήμα 12). Ο κύκλος $K_1(P(a,0),\overline{P(a,0)P(0,0)})$ είναι ένας S_m-κύκλος. Το σημείο $P(2\,a,0)$ που προσδιορίζεται ως τομή του κύκλου K_1 και του άξονα $x'x$ ανήκει στο S_{m+1} και είναι κ.κ.δ. από το S_0 σε $m+1$ βήματα. Ο $2\,a$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Επαγωγικώς, μπορούμε να κ.κ.δ. σε πεπερασμένο πλήθος βημάτων τον $n\,a$, (με $n>2$), ως τομή του άξονα $x'x$ με τον S_{m+n-2}-κύκλο $K_{n-1}(P((n-1)\,a,0),\overline{P(a,0)P(0,0)})$.



Σχήμα 12.

25. Αν ο θετικός πραγματικός αριθμός a είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων τότε από τις παραγράφους 20, 24 προκύπτει ότι και ο $-(n\,a) = (-n)\,a$, (με $n \in \mathbb{N} - \{0\}$), είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων.

26. Αν ο πραγματικός αριθμός a είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων τότε από τις παραγράφους 24, 25 προκύπτει ότι και ο $k\,a$, (με $k \in \mathbb{Z} - \{0\}$), είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων.

27. Έστω a, b δύο μη μηδενικοί πραγματικοί αριθμοί κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Αν $a \neq b$, με $|a| > |b|$, από την παράγραφο 23 προκύπτει ότι και οι $a \pm b$, $a\,b$, a/b είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων.

Αν $a \neq b$, με $|a| < |b|$ οπότε και $|-a| < |b|$, από τις παραγράφους 20, 22, 23 προκύπτει ότι και οι $-a$, $b \pm (-a)$, $-(b \pm (-a)) = a \mp b$, $a\,b$, a/b είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων.

Παρατήρηση : Όπως προκύπτει από τις παραγράφους 22, 23 η κ.κ.δ. των $a\,b$, a/b δεν εξαρτάται από την διάταξη των a, b. Εξετάζουμε περιπτώσεις σε σχέση με την διάταξη των a, b μόνο για την κατασκευή των $a \pm b$. Και αυτή όμως η κατασκευή με την ολοκλήρωση της παρούσης παραγράφου καθίσταται ανεξάρτητη της διάταξης των a, b.

Αν $a = b$ τότε από την παράγραφο 26 προκύπτει ότι $a + b = 2\,a$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. $a - b = 0$ είναι προφανώς κ.κ.δ. σε πεπερασμένο πλήθος βημάτων αφού το σημείο $P(0,0)$ ανήκει στο S_0. Επίσης, από την πιο πάνω παρατήρηση οι $a\,b$, a/b είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων.

28. Έστω a, b δύο μη μηδενικοί πραγματικοί αριθμοί κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Όπως προκύπτει από την παράγραφο 27 και οι $a \pm b$, $a\,b$, a/b είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Η κατασκευές δεν εξαρτώνται από την διάταξη των a, b.

29. Έστω $\mathcal{K}$ το σύνολο των πραγματικών αριθμών που είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Το σημείο $P(0,0)$ ανήκει στο S_0 δηλαδή, είναι κ.κ.δ. από το S_0 σε 0 βήματα. Από την παράγραφο 8 προκύπτει ότι ο $0 \in \mathcal{K}$. Το σημείο $P(1,0)$ ανήκει στο S_0 δηλαδή, είναι κ.κ.δ. από το S_0 σε 0 βήματα. Από την παράγραφο 8 προκύπτει ότι ο $1 \in \mathcal{K}$. Έστω δύο μη μηδενικά στοιχεία a, b του $\mathcal{K}$. Από την παράγραφο 28 προκύπτει ότι οι $a \pm b$, $a\,b$, a/b είναι στοιχεία του $\mathcal{K}$. Εάν b μη μηδενικό στοιχείο του $\mathcal{K}$ τότε από την κ.κ.δ. του b και την παράγραφο 20 το $-b$ είναι στοιχείο του $\mathcal{K}$. Εάν $a = 1$ και b μη μηδενικό στοιχείο του $\mathcal{K}$ τότε από τα προηγούμενα το $a/b = 1/b = b^{-1}$ είναι στοιχείο του $\mathcal{K}$. Η πρόσθεση και ο πολλαπλασιασμός στο $\mathcal{K}$ είναι αντιμεταθετική-ός, προσετεριστική-ός, επιμεριστικός επειδή το $\mathcal{K}$ είναι υποσύνολο του $\mathbb{R}$. Ισχύουν οι προϋποθέσεις που περιγράφονται στην αρχή της παραγράφου 7. Το $\mathcal{K}$ είναι σώμα, (υποσώμα του $\mathbb{R}$).

30. Έστω $\mathcal{C}$ το σύνολο των μιγαδικών αριθμών που είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Επειδή $\mathbb{R} \subset \mathbb{C}$ κάθε στοιχείο του $\mathcal{K}$ ως πραγματικός αριθμός είναι και μιγαδικός. Άρα οι 0, 1 ανήκουν στο $\mathbb{C}$. Έστω $z_1 = a_1 + b_1\,i$, $z_2 = a_2 + b_2\,i$ δύο στοιχεία του $\mathbb{C}$. Από την παράγραφο 16 προκύπτει ότι οι a_1, a_2, b_1, b_2 ανήκουν στο $\mathcal{K}$. Επειδή το $\mathcal{K}$ είναι σώμα, οι $a_1 \pm a_2$, $b_1 \pm b_2$, $a_1\,a_2 \pm b_1\,b_2$, $a_1\,b_2 \pm a_2\,b_1$, $a_2^2 + b_2^2$ ανήκουν στο $\mathcal{K}$. Από την παράγραφο 17 προκύπτει ότι και

οι,

$$\begin{aligned} z_1 \pm z_2 &= (a_1 \pm a_2) + (b_1 \pm b_2)\, i, \\ z_1\, z_2 &= (a_1\, a_2 - b_1\, b_2) + (a_1\, b_2 + a_2\, b_1)\, i, \\ \frac{z_1}{z_2} &= \frac{a_1\, a_2 + b_1\, b_2}{a_2^2 + b_2^2} - \frac{a_1\, b_2 - a_2\, b_1}{a_2^2 + b_2^2}\, i, \ \ (z_2 \neq 0), \end{aligned}$$

ανήκουν στο $\mathcal{C}$. Αν $z = a + b\, i$ ένα στοιχείο του $\mathcal{C}$ από την παράγραφο 16 τα a, b ανήκουν στο $\mathcal{K}$. Επειδή το $\mathcal{K}$ είναι σώμα και τα $-a$, $-b$ ανήκουν στο $\mathcal{K}$. Από την παράγραφο 17 προκύπτει ότι και ο $-z = (-a) + (-b)\, i$ ανήκει στο $\mathcal{C}$. Αν $z = a + b\, i \neq 0$, $(|a| + |b| \neq 0)$, ανήκει στο $\mathcal{C}$ όπως και προηγουμένως τα a, b ανήκουν στο $\mathcal{K}$. Επειδή το $\mathcal{K}$ είναι σώμα και τα,

$$\frac{a}{a^2 + b^2} \ , \ \frac{-b}{a^2 + b^2} \ ,$$

ανήκουν στο $\mathcal{K}$. Από την παράγραφο 17 και ο,

$$z^{-1} = \frac{1}{z} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\, i \ ,$$

ανήκει στο $\mathcal{C}$. Η πρόσθεση και ο πολλαπλασιασμός στο $\mathcal{C}$ είναι αντιμεταθετική-ός, προσετεριστική-ός, επιμεριστικός επειδή το $\mathcal{C}$ είναι υποσύνολο του $\mathbb{C}$.Βλέπουμε, ότι και για το $\mathcal{C}$ ισχύουν οι προϋποθέσεις που περιγράφονται στην αρχή της παραγράφου 7. Το $\mathcal{C}$ είναι σώμα, (υποσώμα του $\mathbb{C}$).

31. Έστω F ένα υποσώμα του $\mathbb{R}$, (ένα σώμα που είναι υποσύνολο του $\mathbb{R}$). d στοιχείο του $\mathbb{R}$ τέτοιο ώστε $d \in F$, $d > 0$, ενώ $\sqrt{d} \notin F$. Θα συμβολίζουμε με $F(\sqrt{d})$ το σύνολο $\{a + b\sqrt{d} \ : \ \forall\, a, b \in F\}$. Είναι άμεσο να δείξει κάποιος ότι οι προϋποθέσεις που περιγράφονται στην αρχή της παραγράφου 7 ικανοποιούνται από το $F(\sqrt{d})$. Το $F(\sqrt{d})$ είναι ένα σώμα, (ένα υποσώμα του $\mathbb{R}$).

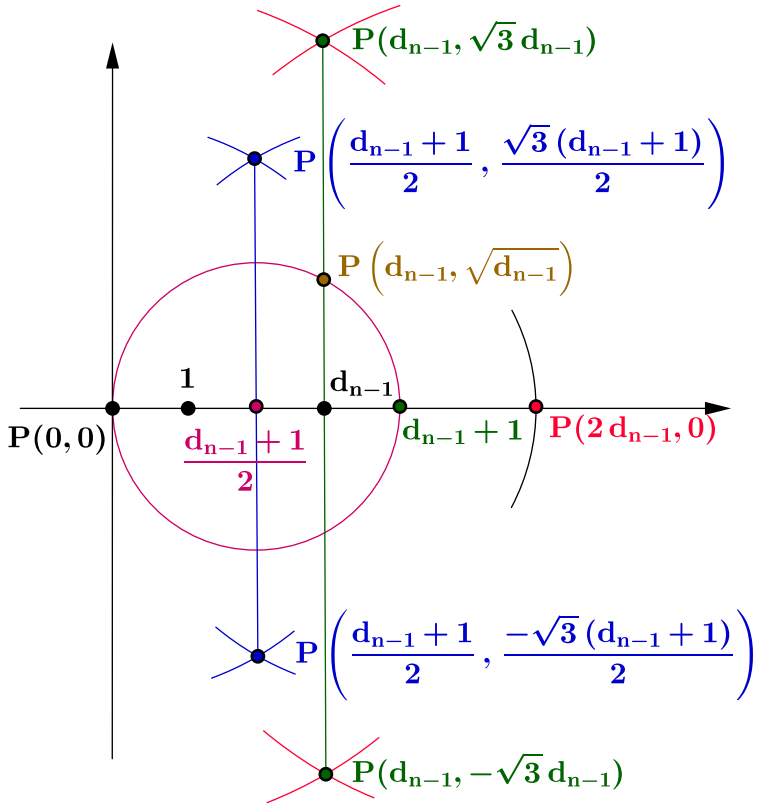
Ομοίως αν z είναι μιγαδικός αριθμός και F υποσώμα του $\mathbb{C}$, ώστε $z \in F$, $\sqrt{z} \notin F$ το σύνολο $F(\sqrt{z}) = \{a + b\sqrt{z} \ : \ \forall\, a, b \in F\}$ μπορεί άμεσα να αποδειχθεί ότι είναι σώμα, (υποσώμα του $\mathbb{C}$).

32. Έστω $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n$ μία σειρά υποσωμάτων του $\mathbb{R}$ ώστε $F_i = F_{i-1}(\sqrt{d_{i-1}})$ με $d_{i-1} > 0$, $d_{i-1} \in F_{i-1}$, $\sqrt{d_{i-1}} \notin F_{i-1}$, $i = 1, 2, \ldots, n$. Θα δείξουμε ότι $F_n \subset \mathcal{K}$ δηλαδή, ότι τα στοιχεία του F_n είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Θα προχωρήσουμε εφαρμόζοντας επαγωγή στο n.

Όπως δείξαμε στην παράγραφο 29 το $\mathcal{K}$ είναι σώμα. Το $1 \in \mathcal{K}$. Οπότε από τις ιδιότητες του σώματος και οι $m = \sum_{i=1}^{m} 1$, $-m = \sum_{i=1}^{m} (-1)$ ανήκουν στο $\mathcal{K}$ για κάθε $m \in \mathbb{N} - \{0\}$. Το 0 ανήκει στο $\mathcal{K}$. Δείξαμε ότι κάθε ακέραιος ανήκει στο $\mathcal{K}$. Έστω οι ακέραιοι m, k, $(k \neq 0)$. Αυτοί ανήκουν στο $\mathcal{K}$. Το $\mathcal{K}$ ως σώμα περιέχει και το πηλίκο τους m/k. Δείξαμε ότι και κάθε ρητός ανήκει στο $\mathcal{K}$. Δηλαδή, για $n = 0$, $\mathbb{Q} = F_0 \subset \mathcal{K}$. Όλοι οι ρητοί είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων.

Υποθέτουμε το συμπέρασμα για $n-1$. Δηλαδή, υποθέτουμε ότι αν $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1}$ είναι μία σειρά υποσωμάτων του $\mathbb{R}$ ώστε $F_i = F_{i-1}(\sqrt{d_{i-1}})$ με $d_{i-1} > 0$, $d_{i-1} \in F_{i-1}$, $\sqrt{d_{i-1}} \notin F_{i-1}$, $i = 1, 2, \ldots, n-1$ τότε το $F_{n-1} \subset \mathcal{K}$. Θέτουμε $F_n = F_{n-1}(\sqrt{d_{n-1}})$ με $d_{n-1} > 0$, $d_{n-1} \in F_{n-1}$, $\sqrt{d_{n-1}} \notin F_{n-1}$. Αφού το $d_{n-1} \in F_{n-1}$ και $F_{n-1} \subset \mathcal{K}$ έπεται ότι ο d_{n-1} είναι κ.κ.δ. σε πεπερασμένο

πλήθος βημάτων. Κατ' επέκταση, από την παράγραφο 8 προκύπτει ότι και το σημείο $P(d_{n-1},0)$ είναι κ.κ.δ. από το S_0 σε πεπερασμένο πλήθος βημάτων, έστω p, (Σχήμα 13). Ο κύκλος $K_1(P(d_{n-1},0),\overline{P(d_{n-1},0)P(0,0)})$ είναι ένας S_p-κύκλος. Το σημείο $P(2\,d_{n-1},0)$ που προσδιορίζεται ως τομή του άξονα $x'x$ με τον κύκλο K_1 ανήκει στο S_{p+1} και είναι κ.κ.δ. από το S_0 σε $p+1$ βήματα. Οι κύκλοι $K_2(P(0,0),\overline{P(0,0)P(2\,d_{n-1},0)})$, $K_3(P(2\,d_{n-1},0),\overline{P(2\,d_{n-1},0)P(0,0)})$ είναι



Σχήμα 13.

S_{p+1}-κύκλοι. Τα σημεία $P(d_{n-1},\pm\sqrt{3}\,d_{n-1})$ που προσδιορίζονται ως τομή των κύκλων K_2, K_3 ανήκουν στο S_{p+2} και είναι κ.κ.δ. από το S_0 σε $p+2$ βήματα. Ο κύκλος $K_4(P(d_{n-1},0),\overline{P(0,0)P(1,0)})$ είναι ένας S_p-κύκλος. Το σημείο $P(d_{n-1}+1,0)$ που προσδιορίζεται ως τομή του άξονα $x'x$ με τον κύκλο K_4 ανήκει στο S_{p+1} άρα και στο S_{p+2}, (αφού από την παράγραφο 5, $S_{p+1}\subset S_{p+2}$), και είναι κ.κ.δ. από το S_0 σε $p+2$ βήματα. Οι κύκλοι $K_5(P(0,0),\overline{P(0,0)P(d_{n-1}+1,0)})$, $K_6(P(d_{n-1}+1,0),\overline{P(d_{n-1}+1,0)P(0,0)})$ είναι S_{p+2}-κύκλοι.

Τα σημεία $P\left(\frac{d_{n-1}+1}{2},\pm\frac{\sqrt{3}\,(d_{n-1}+1)}{2}\right)$ που προσδιορίζονται ως τομή των κύκλων K_5, K_6 ανήκουν στο S_{p+3} και είναι κ.κ.δ. από το S_0 σε $p+3$ βήματα. Όσα σημεία έχουμε κατασκευάσει έως τώρα και ανήκουν στο S_{p+2} ανήκουν και στο S_{p+3}, (επειδή το $S_{p+2}\subset S_{p+3}$).

Η ευθεία $L_1\left(P\left(\frac{d_{n-1}+1}{2},\frac{\sqrt{3}\,(d_{n-1}+1)}{2}\right),P\left(\frac{d_{n-1}+1}{2},\frac{-\sqrt{3}\,(d_{n-1}+1)}{2}\right)\right)$ είναι μία S_{p+3} ευθεία. Το σημείο $P\left(\frac{d_{n-1}+1}{2},0\right)$ που προσδιορίζεται ως τομή του άξονα $x'x$ και της ευθείας L_1 ανήκει στο S_{p+4} και είναι κ.κ.δ. από το S_0 σε $p+4$ βήματα. Η

ευθεία $L_2(P(d_{n-1},0),P(d_{n-1},\sqrt{3}\,d_{n-1}))$ είναι μία S_{p+3} άρα και μία S_{p+4}-ευθεία. Ο κύκλος $K_7\left(P\left(\frac{d_{n-1}+1}{2},0\right),\overline{P\left(\frac{d_{n-1}+1}{2},0\right)P(0,0)}\right)$ είναι ένας S_{p+4}-κύκλος. Το σημείο $P(d_{n-1},\sqrt{d_{n-1}})$ που προσδιορίζεται ως τομή της ευθείας L_2 και του κύκλου K_7 ανήκει στο S_{p+5} και είναι κ.κ.δ. από το S_0 σε $p+5$ βήματα.

Από την παράγραφο 15 και το σημείο $P(0,\sqrt{d_{n-1}})$ είναι κ.κ.δ. από το S_0 σε $p+8$ βήματα. Άρα το σημείο $P(0,\sqrt{d_{n-1}})$ ανήκει στο S_{p+8}. Ο κύκλος $K_8(P(0,0),\overline{P(0,0)P(0,\sqrt{d_{n-1}})})$ είναι ένας S_{p+8}-κύκλος. Το σημείο $P(\sqrt{d_{n-1}},0)$ που προσδιορίζεται ως τομή του άξονα $x'x$ με τον κύκλο K_8 ανήκει στο S_{p+9} και είναι κ.κ.δ. από το S_0 σε $p+9$ βήματα. Από την παράγραφο 8 προκύπτει ότι ο πραγματικός αριθμός $\sqrt{d_{n-1}}$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων και άρα $\sqrt{d_{n-1}}\in\mathcal{K}$.

Τα στοιχεία του F_n είναι της μορφής $a+b\sqrt{d_{n-1}}$ για κάθε a, b από το F_{n-1}. Από την υπόθεση της επαγωγής το $F_{n-1}\subset\mathcal{K}$. Επειδή το $\mathcal{K}$ είναι σώμα και περιέχει όλα τα στοιχεία του F_{n-1} καθώς και την $\sqrt{d_{n-1}}$ θα περιέχει και όλες τις εκφράσεις $a+b\sqrt{d_{n-1}}$ για κάθε a, b από το F_{n-1}. Τελικώς δείξαμε ότι $F_n\subset\mathcal{K}$.

33. Θα δείξουμε ότι κάθε σύνολο S_n όπως αυτό ορίσθηκε στην παράγραφο 5 περιέχει πεπερασμένο πλήθος από τα σημεία του επιπέδου. Προχωρούμε εφαρμόζοντας επαγωγή στο n. Για $n=0$, το $S_0=\{P(0,0),P(1,0)\}$ περιέχει ακριβώς δύο σημεία του επιπέδου και το συμπέρασμα ισχύει.

Υποθέτουμε ότι το S_{n-1} περιέχει πεπερασμένο πλήθος από τα σημεία του επιπέδου. Άρα, μπορούμε να επιλέξουμε πεπερασμένο πλήθος ζευγών σημείων από τα σημεία του επιπέδου που ανήκουν στο S_{n-1}. Από τις παραγράφους 2, 3 προκύπτει ότι κάθε ζεύγος σημείων που ανήκει στο S_{n-1} ορίζει μία S_{n-1}-ευθεία και έναν S_{n-1}-κύκλο. Άρα, μπορούμε να επιλέξουμε πεπερασμένο πλήθος S_{n-1}-ευθειών και κύκλων.

Από τον ορισμό της παραγράφου 5, το S_n αποτελείται από όλα τα σημεία του επιπέδου που ανήκουν στο S_{n-1} μαζί με όλα τα σημεία του επιπέδου που είναι κ.κ.δ. από το S_{n-1} σε 1 βήμα. Από την παράγραφο 5 προκύπτει ότι τα σημεία του επιπέδου που είναι κ.κ.δ. από το S_{n-1} σε 1 βήμα είναι όσα προσδιορίζονται ως τομή δύο S_{n-1}-ευθειών, μίας S_{n-1}-ευθείας και ενός S_{n-1}-κύκλου, δύο S_{n-1}-κύκλων. Λόγω του πεπερασμένου πλήθους των S_{n-1}-ευθειών και κύκλων, τα σημεία που προσδιορίζονται ως τομές τους είναι πεπερασμένου πλήθους. Άρα, το S_n αποτελείται από όλα τα σημεία του επιπέδου που ανήκουν στο S_{n-1} που είναι πεπερασμένου πλήθους, (υπόθεση επαγωγής), μαζί με τα πεπερασμένου πλήθους σημεία του επιπέδου που είναι κ.κ.δ. από το S_{n-1} σε 1 βήμα. Το συμπέρασμα απεδείχθη για n.

34. Έστω F ένα υποσύμα του $\mathbb{R}$. Αν οι συντελεστές των εξισώσεων δύο ευθειών του επιπέδου ανήκουν στο F τότε και οι συντεταγμένες των σημείων τομής των ευθειών αυτών, (εφ΄ όσον αυτές τέμνονται), ανήκουν στο F. Έστω $L_1: a_1\,x+b_1\,y=g_1$, $L_2: a_2\,x+b_2\,y=g_2$, οι εξισώσεις δύο ευθειών του επιπέδου ώστε a_1,b_1,g_1,a_2,b_2,g_2 να ανήκουν στο F. Οι ευθείες αυτές τέμνονται αν και μόνο αν το σύστημα των εξισώσεών τους έχει μοναδική λύση. Η λύση αυτή εφ΄

όσον υπάρχει δίνεται από,

$$x = \frac{\begin{vmatrix} g_1 & b_1 \\ g_2 & b_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}} = \frac{g_1\,b_2 - g_2\,b_1}{a_1\,b_2 - a_2\,b_1}\ ,\ y = \frac{\begin{vmatrix} a_1 & g_1 \\ a_2 & g_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}} = \frac{a_1\,g_2 - a_2\,g_1}{a_1\,b_2 - a_2\,b_1}\,. \qquad (1)$$

Επειδή τα $a_1, b_1, g_1, a_2, b_2, g_2$ ανήκουν στο F και το F είναι σώμα, από τις ιδιότητες του σώματος οι συντεταγμένες του (1) ανήκουν στο F.

35. Έστω F ένα υποσώμα του $\mathbb{R}$. Αν οι συντελεστές των εξισώσεων μίας ευθείας και ενός κύκλου του επιπέδου ανήκουν στο F τότε και οι συντεταγμένες των σημείων τομής της ευθείας και του κύκλου, (εφ' όσον τέμνονται), ανήκουν είτε στο F, είτε στο $F(\sqrt{d})$ με $d > 0$, $d \in F$, $\sqrt{d} \notin F$. Έστω $L : a_1\,x + b_1\,y = g_1$, $K : (x - a_2)^2 + (y - b_2)^2 = g_2^2$ οι εξισώσεις μίας ευθείας και ενός κύκλου του επιπέδου ώστε $a_1, b_1, g_1, a_2, b_2, g_2$ να ανήκουν στο F. Η ευθεία και ο κύκλος τέμνονται αν και μόνο αν το σύστημα των εξισώσεών τους έχει είτε δύο ακριβώς λύσεις είτε μία λύση αλγεβρικής πολλαπλότητας δύο. Από τον ορισμό της ευθείας στην Αναλυτική Γεωμετρία γνωρίζουμε ότι $|a_1| + |b_1| \neq 0$. Αν $b_1 \neq 0$ το σύστημα των L, K ισοδυνάμως γίνεται,

$$\begin{cases} y = b_1^{-1}\,g_1 - b_1^{-1}\,a_1\,x \\ (x - a_2)^2 + [(b_1^{-1}\,g_1 - b_2) - (b_1^{-1}\,a_1\,x)]^2 = g_2^2 \end{cases} \qquad (2)$$

Εκτελώντας τις πράξεις, η δευτεροβάθμια εξίσωση του συστήματος (2) μπορεί να πάρει την μορφή,

$$A\,x^2 + B\,x + G = 0, \qquad (3)$$

με τα A, B, G να ανήκουν στο σώμα F ως αποτελέσματα προσθέσεων, αφαιρέσεων, πολλαπλασιασμών και διαιρέσεων μεταξύ των $a_1, b_1, g_1, a_2, b_2, g_2$ που ανήκουν στο σώμα F. Επειδή $A = (b_1^{-1}\,a_1)^2 + 1 > 0$, και θεωρώντας ότι οι L και K τέμνονται, $(d = B^2 - 4\,A\,G \geq 0)$, η (3) έχει ως ρίζες,

$$x_{1,2} = \frac{-B \pm \sqrt{d}}{2\,A}\ . \qquad (4)$$

(2) και (4) συνεπάγονται ότι οι συντεταγμένες των δύο, (ή του ενός αν $d = 0$ αλγεβρικής πολλαπλότητας δύο), σημείων-(ου) τομής των L και K είναι,

$$\left(\frac{-B \pm \sqrt{d}}{2\,A}\ ,\ b_1^{-1}\,g_1 - b_1^{-1}\,a_1\,\frac{-B \pm \sqrt{d}}{2\,A}\right). \qquad (5)$$

Αν $\sqrt{d} \in F$ τότε οι συντεταγμένες του (5) ανήκουν στο σώμα F ως αποτελέσματα προσθέσεων, αφαιρέσεων, πολλαπλασιασμών και διαιρέσεων μεταξύ των $a_1, b_1, g_1, A, B, \sqrt{d}$ που ανήκουν στο σώμα F.

Αν $\sqrt{d} \notin F$ τότε, $d \neq 0$ γιατί αν $d = 0$, τότε $\sqrt{d} = 0 \in F$ αφού το F είναι σώμα. Αφού $d \neq 0$, και οι L, K τέμνονται έπεται ότι $d > 0$ και $d = B^2 - 4\,A\,G \in F$ ως αποτέλεσμα πολλαπλασιασμού και αφαίρεσης μεταξύ των A, B, G που ανήκουν στο σώμα F. Οι συντεταγμένες του (5) είναι της μορφής $H + X\,\sqrt{d}$ με H, X στοιχεία του σώματος F ως αποτελέσματα των τεσσάρων πράξεων μεταξύ

των $a_1, b_1, g_1, A, B, \sqrt{d}$ που ανήκουν στο σώμα F. Από τα προηγούμενα και την παράγραφο 31 προκύπτει ότι οι συντεταγμένες του (5) ανήκουν στο σώμα $F(\sqrt{d})$ με $d > 0$, $d \in F$, $\sqrt{d} \notin F$.

Με ακριβώς ανάλογο τρόπο μπορούμε να δείξουμε το αποτέλεσμα για $a_1 \neq 0$.

36. Έστω F ένα υποσώμα του $\mathbb{R}$. Αν οι συντελεστές των εξισώσεων δύο κύκλων του επιπέδου ανήκουν στο F τότε και οι συντεταγμένες των σημείων τομής των κύκλων αυτών, (εφ' όσον τέμνονται), ανήκουν είτε στο F, είτε στο $F(\sqrt{d})$ με $d > 0$, $d \in F$, $\sqrt{d} \notin F$. Έστω $K_1 : x^2 + y^2 + a_1\, x + b_1\, y + g_1 = 0$, $K_2 : x^2 + y^2 + a_2\, x + b_2\, y + g_2 = 0$ οι εξισώσεις δύο κύκλων του επιπέδου ώστε $a_1, b_1, g_1, a_2, b_2, g_2$ να ανήκουν στο F. Οι δύο κύκλοι τέμνονται αν και μόνο αν το σύστημα των εξισώσεων των K_1, K_2 έχει είτε μία λύση αλγεβρικής πολλαπλότητας δύο, είτε δύο λύσεις. Η απόδειξη του αποτελέσματος ακολουθεί εντελώς ανάλογη λογική με αυτήν της παραγράφου 35 γι' αυτό δίνουμε εδώ ένα σύντομο περίγραμμα.

Πολλαπλασιάζοντας μία εκ' των εξισώσεων K_1, K_2 με -1 και προσθέτοντας στην άλλη προκύπτει ισοδύναμο σύστημα μίας πρωτοβάθμιας και μίας δευτεροβάθμιας εξίσωσης με συντελεστές και των δύο εξισώσεων από το σώμα F, (ως αφαιρέσεις των $a_1, b_1, g_1, a_2, b_2, g_2$ που ανήκουν στο σώμα F). Κατόπιν ακολουθούμε τα βήματα επίλυσης του συστήματος (2) της παραγράφου 35.

37. Θα δείξουμε ότι για κάθε σύνολο S_n, υπάρχει σώμα F_n ώστε $\mathbb{Q} \subseteq F_n \subseteq \mathbb{R}$ και για κάθε $P(a_n, b_n) \in S_n$ τα $a_n, b_n \in F_n$. Εφαρμόζουμε επαγωγή στο n. Για $n = 0$, το $S_0 = \{P(0,0), P(1,0)\}$ και το συμπέρασμα ισχύει για το σώμα $F_0 = \mathbb{Q}$.

Υποθέτουμε ότι για $n-1$, υπάρχει σώμα F_{n-1} ώστε $\mathbb{Q} \subseteq F_{n-1} \subseteq \mathbb{R}$ και για κάθε $P(a_{n-1}, b_{n-1}) \in S_{n-1}$ τα $a_{n-1}, b_{n-1} \in F_{n-1}$. Από την παράγραφο 33 προκύπτει ότι το S_n περιέχει πεπερασμένο άρα, και αριθμήσιμο πλήθος από σημεία του επιπέδου. Μπορούμε να συμβολίσουμε τα σημεία του επιπέδου που ανήκουν στο S_n ως $P(a_{n,i}, b_{n,i})$, $i = 1, 2, \ldots, m_n$, m_n ό πληθάριθμος του συνόλου S_n.

Από την παράγραφο 5, κάθε $P(a_{n,i}, b_{n,i})$ που ανήκει στο S_n είναι κ.κ.δ. από το S_{n-1} σε 1 βήμα. Δηλαδή το $P(a_{n,i}, b_{n,i})$ προσδιορίζεται ως τομή είτε δύο S_{n-1}-ευθειών, είτε μίας S_{n-1}-ευθείας και ενός S_{n-1}-κύκλου, είτε δύο S_{n-1}-κύκλων. Από την υπόθεση της επαγωγής και την παράγραφο 7 προκύπτει ότι οι μεν συντεταγμένες των σημείων που ανήκουν στο S_{n-1} είναι στοιχεία του σώματος F_{n-1}, οι δε S_{n-1}-ευθείες και κύκλοι έχουν εξισώσεις με συντελεστές από το σώμα F_{n-1}. Από τις παραγράφους 34, 35, 36 έπεται ότι οι συντεταγμένες του κάθε $P(a_{n,i}, b_{n,i})$, $i = 1, 2, \ldots, m_n$, (ως σημείων τομής S_{n-1}-ευθειών και κύκλων), ανήκουν είτε στο F_{n-1}, είτε στο $F_{n-1}(\sqrt{d_{i,n-1}})$ με $d_{i,n-1} > 0$, $d_{i,n-1} \in F_{n-1}$, $\sqrt{d_{i,n-1}} \notin F_{n-1}$. Από την παράγραφο 31 προκύπτει ότι κάθε $F_{n-1}(\sqrt{d_{i,n-1}})$ είναι υποσώμα του $\mathbb{R}$, (γιατί τα στοιχεία του $F_{n-1}(\sqrt{d_{i,n-1}})$ ανήκουν στο $\mathbb{R}$), που περιέχει το F_{n-1}. Επαγωγικά αποδεικνύεται ότι το,

$$\left(\left(\left(F_{n-1}(\sqrt{d_{1,n-1}})\right)(\sqrt{d_{2,n-1}})\right)\cdots\right)\left(\sqrt{d_{m_n,n-1}}\right)\ , \tag{6}$$

είναι σώμα, και ισχύει,

$$\mathbb{Q} \subseteq F_{n-1} \subseteq \left(\left(\left(F_{n-1}(\sqrt{d_{1,n-1}})\right)(\sqrt{d_{2,n-1}})\right)\cdots\right)\left(\sqrt{d_{m_n,n-1}}\right) = F_n \subseteq \mathbb{R}.$$

Από την πιο πάνω ανάλυση οι συντεταγμένες των σημείων που ανήκουν στο S_n, (οι $a_{n,i}$, $b_{n,i}$), ανήκουν στο σώμα (6) που πληροί τις απαιτήσεις του συμπεράσμα-

τος που θέλουμε να αποδείξουμε. Το συμπέρασμα ισχύει για n.

38. Έστω η σειρά $S_0 \subset S_1 \subset \cdots \subset S_n$. Από την παράγραφο 33 γνωρίζουμε ότι το κάθε S_i, $i = 1, 2, \ldots, n$, περιέχει πεπερασμένο άρα και αριθμήσιμο πλήθος σημείων του επιπέδου. Έστω ότι ο πληθάριθμος του S_i είναι m_i, $i = 1, 2, \ldots, n$. Μπορούμε να συμβολίζουμε τα σημεία του επιπέδου που ανήκουν στο S_i ως $P(a_{i,j}, b_{i,j})$ με $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, m_i$.

Θα δείξουμε ότι, σε κάθε σειρά $S_0 \subset S_1 \subset \cdots \subset S_n$ αντιστοιχεί μία σειρά σωμάτων $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$ με $\mathbb{Q} \subseteq F_i \subseteq \mathbb{R}$, και $a_{i,j}, b_{i,j} \in F_i$ για κάθε $P(a_{i,j}, b_{i,j}) \in S_i$, $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, m_i$. Θα εφαρμόσουμε επαγωγή στο n. Για $n = 0$, η σειρά συνόλων γίνεται S_0 και το συμπέρασμα ισχύει για τη σειρά σωμάτων $\mathbb{Q} = F_0$, (γιατί στο $S_0 = \{P(0,0), P(1,0)\}$ αντιστοιχεί το σώμα $\mathbb{Q} = F_0$ με $\mathbb{Q} = F_0 \subseteq \mathbb{R}$ και $0, 1 \in F_0$).

Υποθέτουμε ότι το συμπέρασμα ισχύει για $n-1$ δηλαδή, σε κάθε σειρά $S_0 \subset S_1 \subset \cdots \subset S_{n-1}$ αντιστοιχεί μία σειρά σωμάτων $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{n-1}$ με $\mathbb{Q} \subseteq F_i \subseteq \mathbb{R}$, και $a_{i,j}, b_{i,j} \in F_i$ για κάθε $P(a_{i,j}, b_{i,j}) \in S_i$, $i = 1, 2, \ldots, n-1$, $j = 1, 2, \ldots, m_i$. Από την υπόθεση της επαγωγής που μόλις διατυπώσαμε, προκύπτει ότι για το S_{n-1} υπάρχει σώμα F_{n-1} ώστε $\mathbb{Q} \subseteq F_{n-1} \subseteq \mathbb{R}$, και $a_{n-1,j}, b_{n-1,j} \in F_{n-1}$ για κάθε $P(a_{n-1,j}, b_{n-1,j}) \in S_{n-1}$, $j = 1, 2, \ldots, m_{n-1}$. Αυτά τα δεδομένα συγκρότησαν την υπόθεση της επαγωγής κατά την απόδειξη του συμπεράσματος της παραγράφου 37. Ακολουθώντας βήματα ανάλογα αυτών της απόδειξης της παραγράφου 37, (μετά την διατύπωση της υπόθεσης της επαγωγής), αποδεικνύεται ότι υπάρχει σώμα F_n, (αυτό που δίνεται στην (6)), ώστε $F_{n-1} \subseteq F_n$, $\mathbb{Q} \subseteq F_n \subseteq \mathbb{R}$, και $a_{n,j}, b_{n,j} \in F_n$ για κάθε $P(a_{n,j}, b_{n,j}) \in S_n$, $j = 1, 2, \ldots, m_n$. Το συμπέρασμα απεδείχθη για n.

39. Στα επόμενα όταν αναφερόμαστε σε σώματα που ορίζονται όπως στην παράγραφο 31 δεν θα μας απασχολεί η συνθήκη $\sqrt{d} \notin F$. Αυτό γιατί στην περίπτωση που $\sqrt{d} \in F$ τότε, το $F(\sqrt{d}) = F$. Οπότε στα αποτελέσματα και τις αποδείξεις που θα ακολουθήσουν όπου εμφανίζεται κάποιο σώμα της μορφής $F(\sqrt{d})$ με $\sqrt{d} \in F$ απλά αντικαθίσταται με το F απλοποιώντας διατυπώσεις και αποδείξεις.

Επίσης όταν αναφερόμαστε σε σώματα της μορφής $F(\sqrt{d})$ θα παραλείπουμε, (για λόγους συντόμευσης), να αναφέρουμε ότι $d \in F$ είτε όταν $F \subseteq \mathbb{R}$ και d θετικός πραγματικός, είτε όταν $F \subseteq \mathbb{C}$ και d μιγαδικός. Θα θεωρούμε όμως ότι πάντα $d \in F$.

40. Η παρούσα μονογραφία αντικαθιστά την έως τον Ιούλιο 2017 αναρτηθείσα. Η παράγραφος 40 όπως παρουσιαζόταν στην προηγούμενη εκδοχή της παρούσης μονογραφίας ήταν λανθασμένη και παραλείπεται. Το κείμενο στην παρούσα μονογραφία έχει διορθωθεί σε σχέση με την προηγούμενη ανάρτηση.

41. Η παρούσα μονογραφία αντικαθιστά την έως τον Ιούλιο 2017 αναρτηθείσα. Η παράγραφος 41 όπως παρουσιαζόταν στην προηγούμενη εκδοχή της παρούσης μονογραφίας ήταν λανθασμένη και παραλείπεται. Το κείμενο στην παρούσα μονογραφία έχει διορθωθεί σε σχέση με την προηγούμενη ανάρτηση.

42. Έστω $z = a + b\,i$, ένας μιγαδικός αριθμός κ.κ.δ. σε πεπερασμένο πλήθος βημάτων, (έστω n). Από την παράγραφο 10 προκύπτει ότι το σημείο $P(a, b)$ είναι κ.κ.δ. από το S_0 σε n βήματα δηλαδή $P(a, b) \in S_n$. Από την παράγραφο 5 υπάρχει η σειρά συνόλων $S_0 \subset S_1 \subset S_2 \subset \cdots \subset S_n$ που περιέχουν τα κ.κ.δ.

σημεία του επιπέδου από το S_0 σε $1, 2, \ldots, n$ βήματα αντιστοίχως. Από την παράγραφο 38 στην πιο πάνω σειρά συνόλων S_i αντιστοιχεί μία σειρά σωμάτων $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$ με $\mathbb{Q} \subseteq F_j \subseteq \mathbb{R}$, και $g, r \in F_j$ για κάθε $P(g, r) \in S_j$.

Επίσης, από την παράγραφο 38 προκύπτει ότι η μορφή του κάθε F_j είναι,

$$F_j = \left(\left(\left(F_{j-1}(\sqrt{d_{1,j-1}})\right)(\sqrt{d_{2,j-1}})\right)\cdots\right)\left(\sqrt{d_{m_j,j-1}}\right). \tag{14}$$

όπου m_j ο πληθάριθμος του F_j, $d_{i,j-1}$ θετικοί πραγματικοί αριθμοί, (παράγραφος 39). Από τον ορισμό της παραγράφου 31 είναι σαφές ότι,

$$\begin{aligned} F_{j-1} &\subseteq F_{j-1}(\sqrt{d_{1,j-1}}) \subseteq \left(F_{j-1}(\sqrt{d_{1,j-1}})\right)(\sqrt{d_{2,j-1}}) \subseteq \cdots \subseteq \\ &\subseteq \left(\left(\left(F_{j-1}(\sqrt{d_{1,j-1}})\right)(\sqrt{d_{2,j-1}})\right)\cdots\right)\left(\sqrt{d_{m_j,j-1}}\right) \overset{(14)}{=} F_j. \end{aligned}$$

Έτσι, από τη σειρά σωμάτων $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$ δημιουργείται η ευρύτερη σε πλήθος σωμάτων σειρά,

$$\begin{aligned} F_0 &\subseteq F_0(\sqrt{d_{1,0}}) \subseteq \left(F_0(\sqrt{d_{1,0}})\right)(\sqrt{d_{2,0}}) \subseteq \cdots \subseteq \\ &\subseteq \left(\left(\left(F_0(\sqrt{d_{1,0}})\right)(\sqrt{d_{2,0}})\right)\cdots\right)(\sqrt{d_{m_1,0}}) = \\ F_1 &\subseteq F_1(\sqrt{d_{1,1}}) \subseteq \left(F_1(\sqrt{d_{1,1}})\right)(\sqrt{d_{2,1}}) \subseteq \cdots \subseteq \\ &\subseteq \left(\left(\left(F_1(\sqrt{d_{1,1}})\right)(\sqrt{d_{2,1}})\right)\cdots\right)(\sqrt{d_{m_2,1}}) = \\ F_2 &\subseteq \cdots \subseteq \left(\left(\left(F_{n-1}(\sqrt{d_{1,n-1}})\right)(\sqrt{d_{2,n-1}})\right)\cdots\right)\left(\sqrt{d_{m_n,n-1}}\right) = \\ &= F_n. \end{aligned} \tag{15}$$

Η (15) αποδεικνύει ότι, αν ο μιγαδικός $z = a + bi$ είναι κ.κ.δ. σε n βήματα τότε, υπάρχει σειρά σωμάτων, $\mathbb{Q} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_t$ με $\mathbb{Q} \subseteq H_j \subseteq \mathbb{R}$, $H_j = H_{j-1}(\sqrt{d_{j-1}})$ για κάποιο θετικό πραγματικό d_{j-1}, $j = 1, 2, \ldots, t$, και $a, b \in H_t$.

43. Από την παράγραφο 32 προκύπτει ότι κάθε στοιχείο του H_t σε μία σειρά σωμάτων $\mathbb{Q} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_t$ με $\mathbb{Q} \subseteq H_j \subseteq \mathbb{R}$, $H_j = H_{j-1}(\sqrt{d_{j-1}})$ για κάποιο θετικό πραγματικό d_{j-1}, $j = 1, 2, \ldots, t$, είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Άρα και οι μιγαδικοί αριθμοί που δημιουργούνται με πραγματικό και φανταστικό μέρος από το H_t λόγω και της παραγράφου 17 θα είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων.

Από την άλλη, από την παράγραφο 42 προκύπτει ότι αν ένας μιγαδικός αριθμός είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων τότε το πραγματικό και το φανταστικό του μέρος ανήκουν στο H_t μίας σειράς σωμάτων $\mathbb{Q} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_t$ με $\mathbb{Q} \subseteq H_j \subseteq \mathbb{R}$, $H_j = H_{j-1}(\sqrt{d_{j-1}})$ για κάποιο θετικό πραγματικό d_{j-1}, $j = 1, 2, \ldots, t$.

Από τα πιο πάνω προκύπτει ότι ικανή και αναγκαία συνθήκη για να κ.κ.δ. ένας μιγαδικός αριθμός σε πεπερασμένο πλήθος βημάτων είναι η ύπαρξη σειράς σωμάτων $\mathbb{Q} = \mathbf{H_0} \subseteq \mathbf{H_1} \subseteq \cdots \subseteq \mathbf{H_t}$ με $\mathbb{Q} \subseteq \mathbf{H_j} \subseteq \mathbb{R}$, $\mathbf{H_j} = \mathbf{H_{j-1}}(\sqrt{\mathbf{d_{j-1}}})$ για κάποιο θετικό πραγματικό $\mathbf{d_{j-1}}$, $\mathbf{j} = 1, 2, \ldots, \mathbf{t}$ και $\mathbf{Re(z)}, \mathbf{Im(z)} \in \mathbf{H_t}$.

44. Στόχος των επόμενων παραγράφων είναι να καταστήσουν πρακτικώς εφαρμόσιμη και ελέγξιμη την συνθήκη κατασκευασημότητας με κανόνα και διαβήτη που διατυπώθηκε στην παράγραφο 43.

45. Έστω W υποσύνολο του $\mathbb{C}$, F υποσώμα του $\mathbb{C}$. Θα λέμε ότι το W είναι διανυσματικός χώρος επί του F, (και τα στοιχεία του θα καλούνται διανύσματα), αν συμβαίνουν τα κάτωθι,

- $w_1 + w_2 \in W$, $\forall\, w_1, w_2 \in W$.
- $-w \in W$, $\forall\, w \in W - \{0\}$.
- $0 = w + (-w) \in W$, $\forall\, w \in W$.
- $w_1 + w_2 = w_2 + w_1$ $\forall\, w_1, w_2 \in W$.
- $w_1 + (w_2 + w_3) = (w_1 + w_2) + w_3$, $\forall\, w_1, w_2, w_3 \in W$.
  Δηλαδή το σύνολο $(W, +)$ είναι μία μεταθετική, προσθετική ομάδα.
- $f\, w \in W$, $\forall\, f \in F$, $\forall\, w \in W$.
- $1\, w = w$, $\forall\, w \in W$.
- $(f_1\, f_2)\, w = f_1\, (f_2\, w)$, $\forall\, f_1, f_2 \in F$, $\forall\, w \in W$.
- $(f_1 + f_2)\, w = f_1\, w + f_2\, w$, $\forall\, f_1, f_2 \in F$, $\forall\, w \in W$.
- $f\, (w_1 + w_2) = f\, w_1 + f\, w_2$, $\forall\, f \in F$, $\forall\, w_1, w_2 \in W$.

Έστω $w_1, w_2, \ldots, w_n$ διανύσματα του διανυσματικού χώρου W επί του σώματος F. Θα λέμε ότι τα w_i, $i = 1, 2, \ldots, n$ είναι γραμμικώς ανεξάρτητα επί του F αν κάθε γραμμικός συνδυασμός $f_1\, w_1 + f_2\, w_2 + \cdots + f_n\, w_n = 0$ με $f_i \in F$, $i = 1, 2, \ldots, n$ συνεπάγεται $f_1 = f_2 = \cdots = f_n = 0$. Θα λέμε ότι τα w_i, $i = 1, 2, \ldots, n$ είναι μία βάση του W επί του F αν τα w_i είναι γραμμικώς ανεξάρτητα επί του F και επιπλέον, για κάθε $w \in W$ υπάρχουν $f_i \in F$, $i = 1, 2, \ldots, n$ ώστε $w = f_1\, w_1 + f_2\, w_2 + \cdots + f_n\, w_n$. Αποδεικνύεται στην Γραμμική Άλγεβρα ότι, κάθε υποσύνολο στοιχείων του W που περιέχει το μέγιστο πλήθος γραμμικώς ανεξαρτήτων επί του F διανυσμάτων είναι μία βάση του W. Το μέγιστο πλήθος γραμμικώς ανεξαρτήτων επί του F διανυσμάτων δηλαδή, το πλήθος των στοιχείων της κάθε βάσης καλείται διάσταση του W επί του F.

46. Έστω $F \subseteq W$ δύο υποσώματα του $\mathbb{C}$. Θα αποδείξουμε ότι πάντα το σώμα W είναι διανυσματικός χώρος επί του σώματος F. Οι απαιτήσεις 1, 2, 3, 4, 5 της παραγράφου 45 ισχύουν τετριμμένα γιατί το W ως σώμα είναι μεταθετική προσθετική ομάδα. Οι απαιτήσεις 6, 7, 8 της παραγράφου 45 ισχύουν επειδή το $F \subseteq W$ και το W είναι μεταθετική πολλαπλασιαστική ομάδα. Οι απαιτήσεις 9, 10 της παραγράφου 45 ισχύουν επειδή $F \subseteq W$ και ο πολλαπλασιασμός μεταξύ στοιχείων του W είναι επιμεριστικός ως προς την πρόσθεση και την αφαίρεση αφού $W \subseteq \mathbb{C}$.

47. Έστω $F \subseteq E \subseteq K$ τρία υποσώματα του $\mathbb{C}$. Από την παράγραφο 46 προκύπτει ότι το μεν K είναι διανυσματικός χώρος επί του σώματος E με βάση έστω $\{k_1, k_2, \ldots, k_n\}$, το δε E είναι διανυσματικός χώρος επί του σώματος F με

βάση έστω $\{e_1, e_2, \ldots, e_m\}$. Θα αποδείξουμε ότι το K είναι διανυσματικός χώρος επί του σώματος F με βάση,

$$\{e_1, e_2, \ldots, e_m\}\cdot\{k_1, k_2, \ldots, k_n\} = \{r_{i,j} = e_i\, k_j\ ,\ i = 1, \ldots, m\ ,\ j = 1, \ldots, n\}.$$

Η διάσταση του K ως προς το F θα είναι $n\, m$.

Από την παράγραφο 46 προκύπτει ότι το K είναι διανυσματικός χώρος επί του F. Έστω $f_{i,j} \in F$ τέτοια ώστε, $\sum_{i=1}^{m}\sum_{j=1}^{n} f_{i,j}\, r_{i,j} = 0$. Τότε,

$$\begin{aligned}
\sum_{i=1}^{m}\sum_{j=1}^{n} f_{i,j}\, e_i\, k_j = 0 \quad &\Rightarrow \quad \sum_{j=1}^{n}\sum_{i=1}^{m} f_{i,j}\, e_i\, k_j = 0 \Rightarrow \\
\sum_{j=1}^{n}\left(\sum_{i=1}^{m} f_{i,j}\, e_i\right) k_j = 0 \quad &\Rightarrow \quad \left(\text{επειδή } \sum_{i=1}^{m} f_{i,j}\, e_i \in E \text{ και } \{k_1, \ldots, k_n\}\right. \\
&\qquad\qquad \left.\text{βάση του } K \text{ επί του } E\right) \\
\sum_{i=1}^{m} f_{i,j}\, e_i = 0 \quad &\overset{j=1,\ldots,n}{\Longrightarrow} \quad (\text{επειδή } f_{i,j} \in F \text{ και } \{e_1, \ldots, e_m\} \\
&\qquad\qquad \text{βάση του } E \text{ επί του } F) \\
f_{i,j} = 0 \qquad &, \qquad i = 1, 2, \ldots, m\ ,\ j = 1, 2, \ldots, n.
\end{aligned}$$

Αποδείξαμε ότι τα $r_{i,j}$ είναι γραμμικώς ανεξάρτητα επί του F.

Έστω $k \in K$. Επειδή $\{k_1, k_2, \ldots, k_n\}$ είναι βάση του K επί του E υπάρχουν $b_j \in E$, $j = 1, 2 \ldots, n$ ώστε $k = \sum_{j=1}^{n} b_j\, k_j$. Επειδή $\{e_1, e_2, \ldots, e_m\}$ είναι βάση του E επί του F, για κάθε $b_j \in E$ υπάρχουν $f_{i,j} \in F$, $i = 1, 2 \ldots, m$ ώστε $b_j = \sum_{i=1}^{m} f_{i,j}\, e_i$. Άρα, για το $k \in K$ ισχύει $k = \sum_{i=1}^{m}\sum_{j=1}^{n} f_{i,j}\, e_i\, k_j = \sum_{i=1}^{m}\sum_{j=1}^{n} f_{i,j}\, r_{i,j}$. Αποδείξαμε ότι κάθε στοιχείο του K είναι γραμμικός συνδυασμός στοιχείων του F και των γραμμικώς ανεξαρτήτων επί του F στοιχείων του K, $r_{i,j}$. Από την παράγραφο 45 προκύπτει ότι το σύνολο των $r_{i,j}$ είναι μία βάση του διανυσματικού χώρου K επί του F.

48. Έστω F ένα υποσώμα του $\mathbb{R}$, d ένας θετικός πραγματικός αριθμός ώστε $\sqrt{d} \notin F$. Επειδή, $F \subseteq F(\sqrt{d})$ από την παράγραφο 46 προκύπτει ότι το σώμα $F(\sqrt{d})$ είναι διανυσματικός χώρος επί του σώματος F. Θα δείξουμε ότι το υποσύνολο $\{1, \sqrt{d}\}$ του $F(\sqrt{d})$ είναι βάση του προαναφερθέντος διανυσματικού χώρου επί του F. Δηλαδή, ότι ο $F(\sqrt{d})$ είναι διανυσματικός χώρος διάστασης 2 επί του F. Για κάθε $f_1, f_2 \in F$ τέτοια ώστε

$$f_1\, 1 + f_2\, \sqrt{d} = 0, \tag{16}$$

προκύπτει $f_1 = f_2 = 0$ γιατί αλλιώς, αν δηλαδή, $f_1 \neq 0, f_2 = 0$ από την (16) θα παίρναμε $f_1 = 0$ άτοπο, αν $f_1 = 0, f_2 \neq 0$ από την (16) θα παίρναμε $\sqrt{d} = 0 \in F$ άτοπο, αν $f_1 \neq 0, f_2 \neq 0$ από την (16) θα παίρναμε $\sqrt{d} = (-f_1)\, f_2^{-1} \in F$ άτοπο. Επίσης, από την παράγραφο 31 προκύπτει ότι κάθε στοιχείο του $F(\sqrt{d})$ είναι της μορφής $f_1 + f_2\, \sqrt{d}$ με $f_1, f_2 \in F$. Από την παράγραφο 45 προκύπτει ότι το $\{1, \sqrt{d}\}$ είναι βάση του διανυσματικού χώρου $F(\sqrt{d})$ επί του F.

49. Έστω F ένα υποσώμα του $\mathbb{R}$, $d_1, d_2, \ldots, d_n$ θετικοί πραγματικοί αριθμοί

ώστε,

$$\begin{aligned}\sqrt{d_1} &\notin F\\ \sqrt{d_i} &\notin \left(\left(\left(F(\sqrt{d_1})\right)(\sqrt{d_2})\right)\cdots\right)(\sqrt{d_{i-1}}), i=2,3,\ldots,n.\end{aligned}$$

Θα αποδείξουμε ότι το σώμα,

$$\left(\left(\left(F(\sqrt{d_1})\right)(\sqrt{d_2})\right)\cdots\right)(\sqrt{d_n}), \tag{17}$$

είναι διανυσματικός χώρος επί του F με βάση,

$$\left\{1,\sqrt{d_1}\right\}\cdot\left\{1,\sqrt{d_2}\right\}\cdot\ldots\cdot\left\{1,\sqrt{d_{n-1}}\right\}\cdot\left\{1,\sqrt{d_n}\right\}, \tag{18}$$

όπου $\{1,\sqrt{a}\}\cdot\left\{1,\sqrt{b}\right\}=\left\{1,\sqrt{a},\sqrt{b},\sqrt{a}\,\sqrt{b}\right\}$. Η διάσταση του διανυσματικού χώρου (17) είναι 2^n.

Επειδή το σώμα F είναι υποσύνολο του σώματος (17) από την παράγραφο 46 προκύπτει ότι το σώμα (17) είναι διανυσματικός χώρος επί του σώματος F. Επαγωγικώς, από τις παραγράφους 47, 48 προκύπτει ότι το σύνολο (18) είναι μία βάση του διανυσματικού χώρου (17) επί του F.

Με ακριβώς ανάλογο τρόπο προκύπτουν τα ίδια συμπεράσματα και όταν F ένα υποσώμα του $\mathbb{C}$, $d_1,d_2,\ldots,d_n$ μιγαδικοί αριθμοί.

50. Έστω $z=\varepsilon+\zeta\,i$ μιγαδικός αριθμός κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Τότε και η $\pm\sqrt{z}$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Έστω $w=\eta+\theta\,i$ μιγαδικός τέτοιος ώστε $w^2=z$. Από την τελευταία ισότητα παίρνουμε,

$$\eta=\sqrt{\frac{\varepsilon+\sqrt{\varepsilon^2+\zeta^2}}{2}}\quad,\quad \theta=\sqrt{\frac{-\varepsilon+\sqrt{\varepsilon^2+\zeta^2}}{2}}\text{ , όταν }\zeta>0\text{ ή} \tag{19}$$

$$\eta=-\sqrt{\frac{\varepsilon+\sqrt{\varepsilon^2+\zeta^2}}{2}}\quad,\quad \theta=-\sqrt{\frac{-\varepsilon+\sqrt{\varepsilon^2+\zeta^2}}{2}}\text{ , όταν }\zeta>0, \tag{20}$$

$$\eta=\sqrt{\frac{\varepsilon+\sqrt{\varepsilon^2+\zeta^2}}{2}}\quad,\quad \theta=-\sqrt{\frac{-\varepsilon+\sqrt{\varepsilon^2+\zeta^2}}{2}}\text{ , όταν }\zeta<0\text{ ή} \tag{21}$$

$$\eta=-\sqrt{\frac{\varepsilon+\sqrt{\varepsilon^2+\zeta^2}}{2}}\quad,\quad \theta=\sqrt{\frac{-\varepsilon+\sqrt{\varepsilon^2+\zeta^2}}{2}}\text{ , όταν }\zeta<0. \tag{22}$$

Από την παράγραφο 16 προκύπτει ότι οι ε και ζ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Από τις παραγράφους 29, 32 προκύπτει ότι οι πραγματικοί αριθμοί στις (19), (20), (21), (22) είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Από τις παραγράφους 17, 30 προκύπτει ότι οι μιγαδικοί αριθμοί $\pm w=\pm\sqrt{z}$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων.

51. Έστω b,g,d μιγαδικοί αριθμοί κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Θα αποδείξουμε ότι και οι ρίζες της εξίσωσης $b\,x^2+g\,x+d=0$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Επειδή οι ρίζες της προαναφερθείσας δευτεροβάθμιας εξίσωσης είναι οι,

$$x_{1,2}=\frac{-g\pm\sqrt{g^2-4\,b\,d}}{2\,b}\ ,$$

από τις παραγράφους 30, 50 προκύπτει ότι αυτές είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων.

52. Θα αποδείξουμε μια ισοδύναμη έκφραση της ικανής και αναγκαίας συνθήκης για να είναι ένας μιγαδικός αριθμός κ.κ.δ. σε πεπερασμένο πλήθος βημάτων όπως αυτή έχει διατυπωθεί και αποδειχθεί στην παράγραφο 43.

Ένας μιγαδικός αριθμός $\mathbf{z = a + b\,i}$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων αν και μόνο αν υπάρχει σειρά σωμάτων $\mathbb{Q} = \mathbf{H_0} \subseteq \mathbf{H_1} \subseteq \cdots \subseteq \mathbf{H_m}$ με $\mathbb{Q} \subseteq \mathbf{H_j} \subseteq \mathbb{C}$, $\mathbf{H_j = H_{j-1}(\sqrt{d_{j-1}})}$ για κάποιο μιγαδικό $\mathbf{d_{j-1}}$, $\mathbf{j = 1, 2, \ldots, m}$, και $\mathbf{z \in H_m}$.

Από την παράγραφο 43 προκύπτει ότι αν ο $z = a + b\,i$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων τότε υπάρχει σειρά σωμάτων $\mathbb{Q} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_t$ με $\mathbb{Q} \subseteq H_j \subseteq \mathbb{R} \subseteq \mathbb{C}$, $H_j = H_{j-1}(\sqrt{d_{j-1}})$ για κάποιο θετικό πραγματικό, (άρα και μιγαδικό), αριθμό d_{j-1}, $j = 1, 2, \ldots, t$ και $a = Re(z), b = Im(z) \in H_t$. Τότε ο $z \in H_t(\sqrt{-1}) = H_t(i)$ και το συμπέρασμα προκύπτει για την σειρά σωμάτων $\mathbb{Q} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_t \subseteq H_m = H_t(\sqrt{-1})$.

Αντιστρόφως, έστω σειρά σωμάτων $\mathbb{Q} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_m$ με $\mathbb{Q} \subseteq H_j \subseteq \mathbb{C}$, $H_j = H_{j-1}(\sqrt{d_{j-1}})$ για κάποιο μιγαδικό d_{j-1}, $j = 1, 2, \ldots, m$, και $z \in H_m$. Θα αποδείξουμε ότι κάθε στοιχείο του H_m, (άρα και ο z), είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων εφαρμόζοντας επαγωγή στο m. Για $m = 0$ έπεται ότι $H_0 = \mathbb{Q}$ και κάθε ρητός είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων από την παράγραφο 32.

Υποθέτουμε ότι για $m - 1$ κάθε στοιχείο του H_{m-1} είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Επειδή $H_m = H_{m-1}(\sqrt{d_{m-1}})$ κάθε στοιχείο του H_m γράφεται ως $a_{m-1} + b_{m-1}\sqrt{d_{m-1}}$ για κάθε $a_{m-1}, b_{m-1} \in H_{m-1}$. Από την παράγραφο 39 προκύπτει ότι και ο $d_{m-1} \in H_{m-1}$. Από την υπόθεση της επαγωγής έπεται ότι τα $a_{m-1}, b_{m-1}, d_{m-1}$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Από την παράγραφο 50 έπεται ότι και ο $\sqrt{d_{m-1}}$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Τελικώς, τα $a_{m-1}, b_{m-1}, \sqrt{d_{m-1}}$ ανήκουν στο $\mathcal{C}$ που από την παράγραφο 30 γνωρίζουμε ότι είναι σώμα. Άρα και τα $a_{m-1} + b_{m-1}\sqrt{d_{m-1}}$ ως αποτελέσματα πράξεων μεταξύ στοιχείων του σώματος $\mathcal{C}$, ανήκουν στο $\mathcal{C}$. Το συμπέρασμα απεδείχθη για m.

53. Έστω z μιγαδικός αριθμός με $z \notin \mathbb{Q}$. Έστω ότι ο z είναι ρίζα κάποιου, (μη μηδενικού), πολυωνύμου με ρητούς συντελεστές. Έστω επίσης $\mathbb{Q}[x]$ το σύνολο όλων των πολυωνύμων με ρητούς συντελεστές, (γνωστό από την Γραμμική Άλγεβρα ότι είναι δακτύλιος). Θα αποδείξουμε ότι το σύνολο,

$$\mathbb{Q}(z) = \left\{ \sum_{i=0}^{n} a_i\, z^i \ : \ \forall \sum_{i=0}^{n} a_i\, x^i \in \mathbb{Q}[x] \right\} = \{ f(z) \ : \ \forall\, f(x) \in \mathbb{Q}[x] \}, \qquad (23)$$

είναι υποσώμα του $\mathbb{C}$. Θα συμβολίσουμε με $Q[x]$ το υποσύνολο του $\mathbb{Q}[x]$ που περιέχει τα πολυώνυμα με ρητούς συντελεστές που έχουν το z ως ρίζα. Από την υπόθεση, το $Q[x]$ δεν είναι κενό. Αυτό σημαίνει ότι ανάμεσα στα στοιχεία του $Q[x]$ υπάρχουν κάποια πολυώνυμα με τον ελάχιστο δυνατό βαθμό έστω m. Αν $f(x), g(x)$ είναι δύο πολυώνυμα του $Q[x]$ ελαχίστου βαθμού m, από την Ευκλείδεια διαίρεσή τους προκύπτει ότι $f(x) = g(x)\,\pi(x) + \upsilon(x)$, με $\pi(x), \upsilon(x) \in \mathbb{Q}[x]$, $\upsilon(x) = 0$ ή $deg[\upsilon(x)] < deg[g(x)] = m$, (με $deg[a(x)]$ να συμβολίζει τον βαθμό του πολυωνύμου $a(x)$). Επειδή για τα $f(x), g(x)$ ορίζεται βαθμός καταλαβαίνουμε

ότι αυτά δεν είναι τα μηδενικά πολυώνυμα.

Έστω ότι $deg[\upsilon(x)] < deg[g(x)] = m$. Επειδή $f(z) = g(z) = 0$, από την ταυτότητα της Ευκλείδειας διαίρεσης των $f(x), g(x)$ έπεται ότι $f(z) = g(z)\,\pi(z) + \upsilon(z)$ δηλαδή, $0 = 0\,\pi(z) + \upsilon(z)$ άρα $\upsilon(z) = 0$. Σε αυτή την περίπτωση, το $\upsilon(x)$ είναι στοιχείο του $Q[x]$ βαθμού μικρότερου του m άτοπο. Άρα, $\upsilon(x) = 0$ και από την ταυτότητα της Ευκλείδειας διαίρεσης των $f(x), g(x)$ έπεται ότι $f(x) = g(x)\,\pi(x)$. Όμως, $deg[f(x)] = deg[g(x)] = m$ και όπως είναι γνωστό, $deg[f(x)] = deg[g(x)] + deg[\pi(x)]$. Από τα τελευταία προκύπτει ότι $deg[\pi(x)] = 0$ και το $\pi(x) = c \in \mathbb{Q} - \{0\}$, (δηλαδή, είναι σταθερό μη μηδενικό πολυώνυμο του $\mathbb{Q}[x]$). Άρα, μπορούμε να επιλέξουμε ένα τυχαίο ελαχίστου βαθμού πολυώνυμο $f(x)$ του $Q[x]$ και γνωρίζουμε ότι κάθε άλλο ελαχίστου βαθμού πολυώνυμο του $Q[x]$ θα είναι το $c\,f(x)$ για $c \in \mathbb{Q} - \{0\}$.

Έστω $f(x)$ ένα τυχαίο ελαχίστου βαθμού πολυώνυμο του $Q[x]$. Αυτό είναι ανάγωγο επί του $\mathbb{Q}[x]$ δηλαδή, δεν παραγοντοποιείται σε γινόμενο δύο πολυωνύμων του $\mathbb{Q}[x]$ βαθμού έκαστο μεγαλύτερου ή ίσου του 1 και μικρότερου του $deg[f(x)]$. Έστω ότι $g(x), h(x) \in \mathbb{Q}[x]$ με $1 \leq deg[g(x)], deg[h(x)] < deg[f(x)]$. Αν $f(x) = g(x)\,h(x)$ τότε $0 = g(z)\,h(z)$ και είτε $g(z) = 0$ είτε $h(z) = 0$. Το τελευταίο συνεπάγεται ότι είτε $g(x) \in Q[x]$ είτε $h(x) \in Q[x]$ με βαθμό έκαστο μικρότερο του βαθμού του $f(x)$ αντιβαίνοντας την υπόθεση ότι το $f(x)$ είναι ελαχίστου βαθμού πολυώνυμο του $Q[x]$. Άρα, το $f(x)$ είναι ανάγωγο επί του $\mathbb{Q}[x]$.

Έστω $g(x) \in \mathbb{Q}[x]$, τέτοιο ώστε $g(z) \neq 0$. Έστω $f(x)$ ένα ελαχίστου βαθμού πολυώνυμο του $Q[x]$. Αν $g(x) = f(x)\,h(x)$ για κάποιο $h(x) \in \mathbb{Q}[x]$ τότε, $g(z) = f(z)\,h(z) = 0$ άτοπο. Άρα, το $f(x)$ δεν είναι διαιρέτης του $g(x)$. Έστω $d(x) \in \mathbb{Q}[x]$ ένας κοινός διαιρέτης των $g(x), f(x)$. Επειδή $d(x) \neq f(x)$ και επειδή το $f(x)$ είναι ανάγωγο επί του $\mathbb{Q}[x]$ έπεται ότι $d(x) = c \in \mathbb{Q} - \{0\}$. Το τελευταίο συνεπάγεται ότι τα $g(x), f(x)$ είναι σχετικώς πρώτα μεταξύ τους δηλαδή, ο μέγιστος κοινός διαιρέτης τους επί του $\mathbb{Q}[x]$ είναι το σταθερό πολυώνυμο 1. Ως επακόλουθο, υπάρχουν $a(x), b(x) \in \mathbb{Q}[x]$ ώστε $a(x)\,g(x) + b(x)\,f(x) = 1$ και $a(z)\,g(z) + b(z)\,f(z) = 1$ δηλαδή, $a(z)\,g(z) = 1$. Άρα, κάθε στοιχείο $\sum_{i=1}^{n} a_i\,z^i \neq 0$ του $\mathbb{Q}(z)$ είναι αντιστρέψιμο.

Οι υπόλοιπες προϋποθέσεις για να είναι το σύνολο (23) σώμα, (όπως αυτές παρατίθενται στην αρχή της παραγράφου 7), είναι άμεσο να επαληθευτούν. Ουσιαστικά προκύπτουν από το γεγονός ότι τα στοιχεία του $\mathbb{Q}[x]$, (ως γνωστόν από την Γραμμική Άλγεβρα), ικανοποιούν όλες τις προϋποθέσεις που ικανοποιούν τα στοιχεία ενός σώματος εκτός από αυτή της αντιστρεψιμότητας. Έτσι αρκεί σε κάθε μία από τις προϋποθέσεις του σώματος που ικανοποιούν τα στοιχεία του $\mathbb{Q}[x]$ να αντικαταστήσουμε το x με z. Η αντιστρεψιμότητα των μη μηδενικών στοιχείων του $\mathbb{Q}(z)$ απεδείχθη πιο πάνω. Αποδείξαμε ότι το σύνολο (23) είναι σώμα και σαν υποσύνολο του $\mathbb{C}$ είναι και υποσώμα του $\mathbb{C}$.

54. Έστω $z = a + b\,i$ μιγαδικός αριθμός κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Θα αποδείξουμε ότι υπάρχει πολυώνυμο με ρητούς συντελεστές που έχει το z ως ρίζα. Θα αποδείξουμε ότι το σώμα $\mathbb{Q}(z)$ είναι διανυσματικός χώρος επί του $\mathbb{Q}$. Το ελαχίστου βαθμού πολυώνυμο ανάμεσα στα πολυώνυμα που έχουν το z ως ρίζα προσδιορίζει με τον βαθμό του την διάσταση του $\mathbb{Q}(z)$ επί του $\mathbb{Q}$.

Επειδή ο $z = a + b\,i$, είναι μιγαδικός αριθμός κ.κ.δ. σε πεπερασμένο πλήθος βημάτων, από την παράγραφο 52 προκύπτει ότι υπάρχει σειρά σωμάτων $\mathbb{Q} =$

$H_0 \subseteq H_1 \subseteq \cdots \subseteq H_m$ με $\mathbb{Q} \subseteq H_j \subseteq \mathbb{C}$, $H_j = H_{j-1}(\sqrt{d_{j-1}})$ για κάποιο μιγαδικό d_{j-1}, $j = 1, 2, \ldots, m$ και $z \in H_m$. Από την παράγραφο 46 προκύπτει ότι το H_m είναι διανυσματικός χώρος επί του $\mathbb{Q}$. Επίσης, από τη δομή της προαναφερθείσης σειράς σωμάτων έπεται ότι,

$$H_m = \left(\left(\left(\mathbb{Q}(\sqrt{d_0})\right)(\sqrt{d_1})\right)\cdots\right)(\sqrt{d_{m-1}}), \tag{24}$$

και από την παράγραφο 49 προκύπτει ότι η διάσταση του διανυσματικού χώρου (24) επί του $\mathbb{Q}$ είναι 2^m. Από την παράγραφο 45 έπεται ότι το μέγιστο πλήθος γραμμικώς ανεξάρτητων στοιχείων του H_m επί του $\mathbb{Q}$ είναι 2^m. Τα $1, z, z^2, \ldots, z^{2^m}$ που είναι $2^m + 1$ το πλήθος στοιχεία του H_m είναι γραμμικώς εξαρτημένα επί του $\mathbb{Q}$ δηλαδή, υπάρχουν $a_i \in \mathbb{Q}$ όχι όλα μηδενικά ώστε,

$$\sum_{i=0}^{2^m} a_i\, z^i = 0.$$

Είναι προφανές ότι ο z είναι ρίζα του πολυωνύμου $\sum_{i=0}^{2^m} a_i\, x^i$ του $\mathbb{Q}[x]$ και το πρώτο ζητούμενο απεδείχθη.

Από την παράγραφο 53 προκύπτει ότι το $\mathbb{Q}(z)$ είναι σώμα. Επίσης, το $\mathbb{Q} \subseteq H_m$, το $z \in H_m$ και το H_m είναι σώμα. Αυτό σημαίνει ότι, $\mathbb{Q} \subseteq \mathbb{Q}(z) \subseteq H_m$ και κάθε ένα από τα σύνολα αυτά είναι σώμα, (υποσώμα του $\mathbb{C}$). Από την παράγραφο 46 προκύπτει ότι το H_m είναι διανυσματικός χώρος επί του $\mathbb{Q}(z)$ και το $\mathbb{Q}(z)$ είναι διανυσματικός χώρος επί του $\mathbb{Q}$. Ήδη έχουμε επισημάνει ότι το H_m είναι διανυσματικός χώρος και επί του $\mathbb{Q}$ με διάσταση 2^m. Από την παράγραφο 47 προκύπτει ότι η διάσταση του $\mathbb{Q}(z)$ επί του $\mathbb{Q}$ είναι διαιρέτης της διάστασης του H_m επί του $\mathbb{Q}$. Άρα και η διάσταση του $\mathbb{Q}(z)$ επί του $\mathbb{Q}$ είναι δύναμη του 2.

Έστω ότι η διάσταση του $\mathbb{Q}(z)$ επί του $\mathbb{Q}$ είναι 2^s, $s \in \mathbb{N}$, $s \leq m$. Έστω επίσης ότι k είναι ο ελάχιστος βαθμός πολυωνύμου του $\mathbb{Q}[x]$ που έχει το z ως ρίζα. Θα αποδείξουμε ότι τα $1, z, z^2, \ldots, z^{k-1}$ είναι μία βάση του διανυσματικού χώρου $\mathbb{Q}(z)$ επί του $\mathbb{Q}$. Τα $1, z, z^2, \ldots, z^{k-1}$ ανήκουν στο $\mathbb{Q}(z)$ γιατί το $z \in \mathbb{Q}(z)$ και το $\mathbb{Q}(z)$ ως σώμα περιέχει το 1 και όλα τα αποτελέσματα των πολλαπλασιασμών των στοιχείων του $\mathbb{Q}(z)$ μεταξύ τους.

Αν τα $1, z, z^2, \ldots, z^{k-1}$ είναι γραμμικώς εξαρτημένα επί του $\mathbb{Q}$ τότε, υπάρχουν $b_i \in \mathbb{Q}$ όχι όλα μηδενικά ώστε,

$$\sum_{i=0}^{k-1} b_i\, z^i = 0.$$

Τότε ο z θα είναι ρίζα του πολυωνύμου $\sum_{i=0}^{k-1} b_i\, x^i \in \mathbb{Q}[x]$ βαθμού $k-1$ αντιβαίνοντας την υπόθεση ότι ο ελάχιστος βαθμός πολυωνύμου του $\mathbb{Q}[x]$ που έχει το z ως ρίζα είναι k. Άρα, τα $1, z, z^2, \ldots, z^{k-1}$ είναι γραμμικώς ανεξάρτητα επί του $\mathbb{Q}$. Έστω,

$$\sum_{i=0}^{n} r_i\, z^i, \tag{25}$$

ένα μη μηδενικό στοιχείο του $\mathbb{Q}(z)$. Έστω επίσης $g(x)$ ένα ελαχίστου βαθμού πολυώνυμο του $\mathbb{Q}[x]$ που έχει το z ως ρίζα. Η ταυτότητα της Ευκλείδειας διαίρεσης για τα πολυώνυμα $f(x) = \sum_{i=0}^{n} r_i\, x^i$ και $g(x)$ δίνει, $f(x) = g(x)\,\pi(x) + \upsilon(x)$

με $\pi(x), \upsilon(x) \in \mathbb{Q}[x]$, $\upsilon(x) = 0$ ή $deg[\upsilon(x)] < deg[g(x)] = k$ οπότε $\upsilon(x) = \sum_{i=0}^{\ell} \theta_i\, x^i$, $\ell \leq k-1$.

Αν $\upsilon(x) = 0$ η ταυτότητα της Ευκλείδειας διαίρεσης για τα $f(x)$, $g(x)$ δίνει $f(x) = g(x)\,\pi(x)$ από όπου έπεται $f(z) = g(z)\,\pi(z) = 0$ και σε αυτή την περίπτωση το (25) είναι το μηδενικό στοιχείο του $\mathbb{Q}(z)$ αντιβαίνοντας την υπόθεση. Άρα, $\upsilon(x) \neq 0$ και τότε από την ταυτότητα της Ευκλείδειας διαίρεσης για τα $f(x)$, $g(x)$ λαμβάνουμε $f(z) = g(z)\,\pi(z) + \upsilon(z)$ από όπου έπεται $f(z) = \upsilon(z) = \sum_{i=0}^{\ell} \theta_i\, z^i$ με $\ell \leq k-1$. Το τελευταίο αποδεικνύει ότι όλα τα μη μηδενικά στοιχεία του $\mathbb{Q}(z)$ προκύπτουν ως γραμμικοί συνδυασμοί επί του $\mathbb{Q}$ των $1, z, z^2, \ldots, z^{k-1}$. Το 0 προφανώς προκύπτει ως, (μηδενικός), γραμμικός συνδυασμός επί του $\mathbb{Q}$ των $1, z, z^2, \ldots, z^{k-1}$. Από την παράγραφο 45 προκύπτει ότι τα k το πλήθος στοιχεία $1, z, z^2, \ldots, z^{k-1}$ είναι μία βάση του διανυσματικού χώρου $\mathbb{Q}(z)$ επί του $\mathbb{Q}$. Άρα, $k = 2^s$ και το δεύτερο συμπέρασμα απεδείχθη.

55. Έστω $z = a + b\,i$ ένας μιγαδικός αριθμός. Από την παράγραφο 54 προκύπτει μία πολύ πρακτική αναγκαία συνθήκη για την κ.κ.δ. των στοιχείων του $\mathbb{C}$.

Αν ο z είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων τότε υπάρχει ελαχίστου βαθμού πολυώνυμο με ρητούς συντελεστές που έχει ως ρίζα του τον z και ο βαθμός του είναι 2^s, για κάποιο $s \in \mathbb{N}$.

Η πρακτικότητα της συνθήκης έγκειται στο γεγονός ότι μας επιτρέπει να προσδιορίσουμε αμέσως πιοί μιγαδικοί αριθμοί δεν είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων.

Δεν είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων όσοι μιγαδικοί αριθμοί δεν είναι ρίζες πολυωνύμων με ρητούς συντελεστές βαθμού 2^s, για κάποιο $s \in \mathbb{N}$.

Προσοχή. Η αρχική συνθήκη είναι αναγκαία και όχι ικανή. Δηλαδή, υπάρχουν ρίζες πολυωνύμων με ρητούς συντελεστές βαθμού 2^s, για κάποιο $s \in \mathbb{N}$, που δεν είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Ως παράδειγμα αναφέρουμε το πολυώνυμο,

$$x^4 - 4\,x + 2,$$

του οποίου κάποια από τις ρίζες είναι μιγαδικός που δεν κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Η απόδειξη του τελευταίου ισχυρισμού παραλείπεται διότι απαιτείται εκτεταμένη χρήση των συμπερασμάτων της θεωρίας Galois παρεκκλίνοντας από τους σκοπούς του παρόντος κειμένου. Ο ενδιαφερόμενος μπορεί να βρει την σχετική απόδειξη στο [10] της βιβλιογραφίας την οποία παραθέτουμε στο τέλος του κειμένου.

56. Έστω $f(x) \in \mathbb{Q}[x]$. Το $f(x)$ μπορεί να γραφεί ως,

$$f(x) = \sum_{i=0}^{n} \frac{q_{i,1}}{q_{i,2}}\, x^i\ ,\ q_{i,1} \in \mathbb{Z},\ q_{n,1}, q_{i,2} \in \mathbb{Z} - \{0\}. \tag{26}$$

Αν συμβολίσουμε με $LCM(q_{0,2}, q_{1,2}, \ldots, q_{n,2})$ το ελάχιστο κοινό πολλαπλάσιο των $q_{0,2}, q_{1,2}, \ldots, q_{n,2}$, το $f(x)$ ισοδυνάμως γράφεται ως,

$$f(x) = \frac{1}{LCM(q_{0,2}, q_{1,2}, \ldots, q_{n,2})} \sum_{i=0}^{n} b_i\, x^i\ ,\ b_i \in \mathbb{Z},\ b_n \in \mathbb{Z} - \{0\}. \tag{27}$$

Είναι σαφές ότι κάθε ρίζα του (26) είναι ρίζα και του (27) και αντιστρόφως.

57. Από την παράγραφο 56 προκύπτει ότι η αναγκαία συνθήκη της παραγράφου 55 μπορεί ισοδυνάμως να διατυπωθεί ως,

Αν ο z είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων τότε υπάρχει ελαχίστου βαθμού πολυώνυμο με ακέραιους συντελεστές που έχει ως ρίζα του τον z και ο βαθμός του είναι $2^{\mathbf{s}}$, για κάποιο $\mathbf{s} \in \mathbb{N}$.

59. Δοθέντος ενός κύβου ακμής a, το πρόβλημα του διπλασιασμού του κύβου με κανόνα και διαβήτη συνίσταται στην κ.κ.δ. σε πεπερασμένο πλήθος βημάτων ακμής b νέου κύβου με όγκο διπλάσιο του όγκου του δοθέντος.

Ο όγκος του δοθέντος κύβου είναι a^3 και του ζητούμενου $b^3 = 2\,a^3$. Οπότε, για να είναι δυνατή αυτή η κατασκευή θα πρέπει ο αριθμός $b = \sqrt[3]{2}\,a$ να μπορεί να κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Εννοείται ότι για να έχει νόημα το πρόβλημα πρέπει η ακμή a του δοθέντος κύβου να είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων.

Έστω ότι η ακμή b του ζητούμενου κύβου είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Από την παράγραφο 29 γνωρίζουμε ότι οι πραγματικοί αριθμοί που είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων συγκροτούν το σώμα $\mathcal{K}$. Από τις ιδιότητες του σώματος, το αποτέλεσμα της διαίρεσης δύο μη μηδενικών στοιχείων του $\mathcal{K}$ ανήκουν στο σώμα $\mathcal{K}$. Άρα, και ο πραγματικός αριθμός $a/b = \sqrt[3]{2}$ ανήκει στο $\mathcal{K}$ και είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Από την παράγραφο 57 προκύπτει ότι το ελαχίστου βαθμού πολυώνυμο που έχει τη $\sqrt[3]{2}$ ως ρίζα πρέπει να έχει βαθμό 2^s, $\mathbf{s} \in \mathbb{N}$. Όμως το ελαχίστου βαθμού πολυώνυμο με ακέραιους συντελεστές που έχει ως ρίζα του τον αριθμό $\sqrt[3]{2}$ είναι προφανώς το $x^3 - 2$.

Αποδείξαμε ότι ο διπλασιασμός με κανόνα και διαβήτη ενός δοθέντος κύβου είναι αδύνατος.

60. Έστω μιγαδικός αριθμός z, και $p(x)$ ένα ελαχίστου βαθμού πολυώνυμο του $\mathbb{Q}[x]$ που έχει τον z ως ρίζα. Έστω επίσης, $f(x)$ ένα άλλο πολυώνυμο του $\mathbb{Q}[x]$ που έχει τον z ως ρίζα. Η ταυτότητα της Ευκλείδειας διαίρεσης των $f(x), p(x)$ δίνει, $f(x) = p(x)\,\pi(x) + \upsilon(x)$ με $\pi(x), \upsilon(x) \in \mathbb{Q}[x]$, $\upsilon(x) = 0$ ή $deg[\upsilon(x)] < deg[p(x)]$.

Αν $deg[\upsilon(x)] < deg[p(x)]$ τότε, από την ισότητα $f(z) = p(z)\,\pi(z) + \upsilon(z)$ προκύπτει $\upsilon(z) = 0$ αντιβαίνοντας τη υπόθεση ότι το $p(x)$ είναι ελαχίστου βαθμού πολυώνυμο του $\mathbb{Q}[x]$ που έχει τον z ως ρίζα. Άρα, $\upsilon(x) = 0$ και $f(x) = p(x)\,\pi(x)$.

Αποδείξαμε ότι κάθε ελαχίστου βαθμού πολυώνυμο του $\mathbb{Q}[x]$ που έχει τον z ως ρίζα είναι διαιρέτης κάθε άλλου πολυωνύμου του $\mathbb{Q}[x]$ που έχει τον z ως ρίζα.

61. Έστω $p(x)$ πολυώνυμο του $\mathbb{Q}[x]$. Θα λέμε ότι το $p(x)$ είναι ανάγωγο επί του $\mathbb{Q}[x]$ αν δεν υπάρχουν πολυώνυμα $a(x), b(x) \in \mathbb{Q}[x]$ με $1 \leq deg[a(x)], deg[b(x)] < deg[p(x)]$ ώστε $p(x) = a(x)\,b(x)$.

62. Θα αποδείξουμε ότι το πολυώνυμο $p(x) = x^3 - 3\,x - 1$ είναι ανάγωγο επί του $\mathbb{Q}[x]$. Έστω ότι υπάρχουν πολυώνυμα $a(x), b(x) \in \mathbb{Q}[x]$ με $1 \leq deg[a(x)], deg[b(x)] < deg[p(x)]$ ώστε $p(x) = a(x)\,b(x)$. Τότε είτε $deg[a(x)] = 1$ και $deg[b(x)] = 2$ είτε $deg[a(x)] = 2$ και $deg[b(x)] = 1$. Δηλαδή, σε κάθε περίπτωση θα υπάρχει πρωτοβάθμιο πολυώνυμο του $\mathbb{Q}[x]$ που θα είναι διαιρέτης του $p(x)$. Έστω $\gamma\,x + \delta$, $\gamma \in \mathbb{Q} - \{0\}$, $\delta \in \mathbb{Q}$ το πολυώνυμο αυτό. Τότε, ο ρητός

αριθμός $-\delta/\gamma$ θα είναι ρίζα του $p(x)$. Οι μόνοι ρητοί που μπορεί να είναι ρίζες του $p(x)$ είναι οι ± 1. Όμως $p(\pm 1) \neq 0$. Οπότε, το $p(x)$ είναι ανάγωγο επί του $\mathbb{Q}[x]$.

63. Θα αποδείξουμε ότι ο αριθμός $2\,\text{συν}\,\frac{\pi}{9}$ δεν κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Από την τριγωνομετρική ταυτότητα $\text{συν}(3\,\theta) = 4\,\text{συν}^3(\theta) - 3\,\text{συν}(\theta)$ για $\theta = \pi/9$ παίρνουμε,

$$\begin{aligned} \text{συν}\,\frac{\pi}{3} = 4\,\text{συν}^3\,\frac{\pi}{9} - 3\,\text{συν}\,\frac{\pi}{9} \quad &\Rightarrow \quad 8\,\text{συν}^3\,\frac{\pi}{9} - 6\,\text{συν}\,\frac{\pi}{9} - 1 = 0 \\ &\Rightarrow \quad p\left(2\,\text{συν}\,\frac{\pi}{9}\right) = 0, \end{aligned}$$

όπου $p(x) = x^3 - 3\,x - 1$. Θα δείξουμε ότι το $p(x)$ είναι ένα ελαχίστου βαθμού πολυώνυμο του $\mathbb{Q}[x]$ που έχει τον $2\,\text{συν}\,\frac{\pi}{9}$ ως ρίζα.

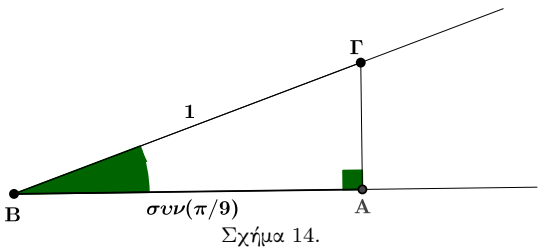
Έστω ότι ο ελάχιστος βαθμός πολυωνύμου του $\mathbb{Q}[x]$ που έχει τον $2\,\text{συν}\,\frac{\pi}{9}$ ως ρίζα είναι 2. Δηλαδή, υπάρχει $a(x) \in \mathbb{Q}[x]$ τέτοιο ώστε $a\left(2\,\text{συν}\,\frac{\pi}{9}\right) = 0$ και $deg[a(x)] = 2$ ο ελάχιστος βαθμός πολυωνύμου του $\mathbb{Q}[x]$ που έχει το $2\,\text{συν}\,\frac{\pi}{9}$ ως ρίζα. Τότε από την παράγραφο 60 προκύπτει ότι το $a(x)$ είναι διαιρέτης του $p(x)$ και άρα υπάρχει πρωτοβάθμιο πολυώνυμο $b(x) \in \mathbb{Q}[x]$ ώστε $p(x) = a(x)\,b(x)$ αντιβαίνοντας το συμπέρασμα της παραγράφου 62 ότι το $p(x)$ είναι ανάγωγο επί του $\mathbb{Q}[x]$.

Αποδείξαμε ότι το $p(x)$ είναι ένα ελαχίστου βαθμού πολυώνυμο του $\mathbb{Q}[x]$ που έχει τον $2\,\text{συν}\,\frac{\pi}{9}$ ως ρίζα. Το $p(x)$ είναι και ένα ελαχίστου βαθμού πολυώνυμο με ακέραιους συντελεστές που έχει το $2\,\text{συν}\,\frac{\pi}{9}$ ως ρίζα, (γιατί τα πολυώνυμα με ακέραιους συντελεστές περιέχονται στο $\mathbb{Q}[x]$). Όμως το $p(x)$ δεν είναι βαθμού 2^s, για κάποιο $s \in \mathbb{N}$. Από την παράγραφο 57 προκύπτει ότι ο αριθμός $2\,\text{συν}\,\frac{\pi}{9}$ δεν κ.κ.δ. σε πεπερασμένο πλήθος βημάτων.

64. Αν ο αριθμός $\text{συν}\,\frac{\pi}{9}$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων τότε, από την παράγραφο 29 προκύπτει ότι και ο $2\,\text{συν}\,\frac{\pi}{9}$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων αντιβαίνοντας το συμπέρασμα της παραγράφου 63.

Αποδείξαμε ότι ο αριθμός $\text{συν}\,\frac{\pi}{9}$ δεν είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων

65. Έστω ότι η γωνία των $\pi/3$ ακτινίων τριχοτομείται με κανόνα και διαβήτη. Αυτό σημαίνει ότι η γωνία των $\pi/9$ ακτινίων κατασκευάζεται με κανόνα και διαβήτη, (Σχήμα 14).



Σχήμα 14.

Είναι προφανές ότι και το ορθογώνιο τρίγωνο $AB\Gamma$ του σχήματος 14 κατασκευάζεται με κανόνα και διαβήτη εφ΄ όσον το κάθετο ευθύγραμμο τμήμα από το σημείο Γ, $(B\Gamma = 1)$, προς την ημιευθεία BA είναι κατασκευάσιμο με κανόνα και διαβήτη. Άρα και το ευθύγραμμο τμήμα $BA = \text{συν}\,\frac{\pi}{9}$ είναι κατασκευάσιμο με κανόνα και διαβήτη αντιβαίνοντας το συμπέρασμα της παραγράφου 64.

Αποδείξαμε ότι η γωνία των $\pi/3$ ακτινίων δεν τριχοτομείται με κανόνα και διαβήτη. Άρα, γενικώς μία γωνία δεν τριχοτομείται με κανόνα και διαβήτη παρά μόνο σε ειδικές περιπτώσεις όπως για παράδειγμα η γωνία των $\pi/2$ ακτινίων η οποία τριχοτομείται με κανόνα και διαβήτη.

66. Το περίφημο από την αρχαιότητα πρόβλημα του τετραγωνισμού του κύκλου συνίσταται στην κατασκευή με κανόνα και διαβήτη της πλευράς a τετραγώνου εμβαδού ίσου προς το εμβαδόν δοθέντος κύκλου ακτίνας r, (η ακτίνα r θεωρείται κ.κ.δ. σε πεπερασμένο πλήθος βημάτων).

Αν το πρόβλημα αυτό επιδέχεται λύσης τότε για τα εμβαδά τετραγώνου και κύκλου ισχύει $a^2 = \pi\, r^2$ ή $\pi = a^2/r^2$. Από την υπόθεση η ακτίνα r είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Αν και η πλευρά a του τετραγώνου είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων τότε από την παράγραφο 29 προκύπτει ότι και ο αριθμός $(a/r)^2$ είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων οπότε και ο αριθμός π είναι κ.κ.δ. σε πεπερασμένο πλήθος βημάτων. Από την παράγραφο 57 έπεται ότι το ελαχίστου βαθμού πολυώνυμο με ακέραιους συντελεστές που έχει το π ως ρίζα είναι βαθμού 2^s, για κάποιο $s \in \mathbb{N}$.

Αποδεικνύεται όμως ότι δεν υπάρχει πολυώνυμο με ακέραιους συντελεστές οιουδήποτε βαθμού που να έχει τον π ως ρίζα. Άρα, η αναγκαία συνθήκη της παραγράφου 57 δεν ισχύει στην περίπτωση του π και το πρόβλημα του τετραγωνισμού του κύκλου δεν επιδέχεται λύσης υπό τον περιορισμό η κατασκευή να γίνει αποκλειστικά με κανόνα και διαβήτη. Στις επόμενες παραγράφους θα παρουσιάσουμε την απόδειξη της υπερβατικότητας του π επί του $\mathbb{Z}$ δηλαδή, ότι δεν υπάρχει πολυώνυμο με ακέραιους συντελεστές οιουδήποτε βαθμού που να έχει τον π ως ρίζα. Αυτό ουσιαστικά συνεπάγεται ότι δεν υπάρχει πολυώνυμο με ρητούς συντελεστές οιουδήποτε βαθμού που να έχει τον π ως ρίζα, γιατί αν υπήρχε πολυώνυμο $f(x) \in \mathbb{Q}[x]$, $f(x) = \sum_{i=0}^{n} \frac{q_{i,1}}{q_{i,2}}\, x^i$, $q_{i,1} \in \mathbb{Z}$, $q_{n,1}, q_{i,2} \in \mathbb{Z} - \{0\}$ ώστε $f(\pi) = 0$ τότε, από την παράγραφο 56 και το πολυώνυμο $LCM(q_{0,2}, q_{1,2}, \ldots, q_{n,2})\, f(x)$ που έχει ακέραιους συντελεστές θα είχε τον π ως ρίζα, άτοπο.

67. Έστω R υποσύνολο του $\mathbb{C}$. Θα λέμε ότι το R είναι ένας μεταθετικός δακτύλιος με μονάδα, (υποδακτύλιος του $\mathbb{C}$), αν έχει όλες της ιδιότητες του σώματος εκτός από την ιδιότητα της αντιστρεψιμότητας των μη μηδενικών του στοιχείων. Για λόγους συντομίας στα επόμενα θα λέμε δακτύλιος αντί για μεταθετικός δακτύλιος με μονάδα. Ως παράδειγμα υποδακτυλίου του $\mathbb{C}$ αναφέρουμε το σύνολο $\mathbb{Z}$ των ακεραίων αριθμών.

68. Έστω R υποδακτύλιος του $\mathbb{C}$. Θα συμβολίζουμε με $R[x_1, x_2, \ldots, x_n]$ το σύνολο των πολυωνύμων στις n το πλήθος μεταβλητές $x_1, x_2, \ldots, x_n$ με συντελεστές από το R δηλαδή, των πολυωνύμων,

$$f(x_1, x_2, \ldots, x_n) = \sum_{i_1=0}^{m_1} \sum_{i_2=0}^{m_2} \cdots \sum_{i_n=0}^{m_n} a_{i_1,i_2,\ldots,i_n}\, x_1^{i_1}\, x_2^{i_2}\, \cdots\, x_n^{i_n},$$

με $a_{i_1,i_2,\ldots,i_n} \in R$. Είναι γνωστό από την θεωρία σωμάτων και δακτυλίων ότι το $R[x_1, x_2, \ldots, x_n]$ είναι δακτύλιος.

69. Έστω R υποδακτύλιος του $\mathbb{C}$. Ένα πολυώνυμο $f(x_1, x_2, \ldots, x_n) \in R[x_1, x_2, \ldots, x_n]$ θα λέγεται συμμετρικό πολυώνυμο αν παραμένει αμετάβλητο σε κάθε μετάθεση των μεταβλητών $x_1, x_2, \ldots, x_n$. Ως παράδειγμα αναφέρουμε το πολυώνυ-

μο $f(x_1,x_2,x_3)=x_1^2\,x_2\,x_3+x_1\,x_2^2\,x_3+x_1\,x_2\,x_3^2$ του $\mathbb{Z}[x_1,x_2,x_3]$. Αυτό είναι συμμετρικό πολυώνυμο αφού,

$$\begin{aligned} f(x_1,x_2,x_3) &= f(x_2,x_1,x_3)=f(x_2,x_3,x_1)=f(x_1,x_3,x_2)= \\ &= f(x_3,x_1,x_2)=f(x_3,x_2,x_1). \end{aligned}$$

70. Έστω R υποδακτύλιος του $\mathbb{C}$. Τα πολυώνυμα του $R[x_1,x_2,\ldots,x_n]$,

$$\begin{aligned} e_1(x_1,x_2,\ldots,x_n) &= \sum_{i=1}^{n} x_i, \\ e_2(x_1,x_2,\ldots,x_n) &= \sum_{1\le i_1<i_2\le n} x_{i_1}\,x_{i_2}, \\ &\vdots \\ e_k(x_1,x_2,\ldots,x_n) &= \sum_{1\le i_1<i_2<\cdots<i_k\le n} x_{i_1}\,x_{i_2}\,\cdots\,x_{i_k}, \\ &\vdots \\ e_n(x_1,x_2,\ldots,x_n) &= x_1\,x_2\,\cdots\,x_n, \end{aligned}$$

είναι συμμετρικά πολυώνυμα και λέγονται στοιχειώδη συμμετρικά πολυώνυμα του $R[x_1,x_2,\ldots,x_n]$. Μία πολύ σημαντική ιδιότητα των στοιχειωδών συμμετρικών πολυωνύμων είναι η ακόλουθη.

Έστω $f(x)$ πολυώνυμο βαθμού m με συντελεστές από το R και ρίζες $\rho_1,\rho_2,\ldots,\rho_m\in\mathbb{C}$. Αν $f(x)=\sum_{i=0}^{m} a_i\,x_i$, $a_m\neq 0$ έπεται ότι $f(x)=a_m\,(x-\rho_1)\,(x-\rho_2)\,\cdots\,(x-\rho_m)$ και,

$$\begin{aligned} -\frac{a_{m-1}}{a_m} &= \sum_{i=1}^{m}\rho_i = e_1(\rho_1,\rho_2,\ldots,\rho_m), \\ \frac{a_{m-2}}{a_m} &= \sum_{1\le i_1<i_2\le m}\rho_{i_1}\,\rho_{i_2} = e_2(\rho_1,\rho_2,\ldots,\rho_m), \\ &\vdots \\ (-1)^k\,\frac{a_{m-k}}{a_m} &= \sum_{1\le i_1<i_2<\cdots<i_k\le m}\rho_{i_1}\,\rho_{i_2}\,\cdots\,\rho_{i_k} = e_k(\rho_1,\rho_2,\ldots,\rho_m), \\ &\vdots \\ (-1)^m\,\frac{a_0}{a_m} &= \rho_1\,\rho_2\,\cdots\,\rho_m = e_m(\rho_1,\rho_2,\ldots,\rho_m). \end{aligned}$$

Οι πιο πάνω ισότητες είναι οι τύποι του Viète στη γενική περίπτωση.

71. Έστω R υποδακτύλιος του $\mathbb{C}$. Οι αλγεβρικές παραστάσεις $a\,x_1^{i_1}\,x_2^{i_2}\,\cdots\,x_n^{i_n}$, $i_1,i_2,\ldots,i_n\in\mathbb{N}$, οι οποίες είναι πολυώνυμα του $R[x_1,x_2,\ldots,x_n]$ με ένα όρο, θα λέγονται μονώνυμα και το άθροισμα των εκθετών τους θα λέγεται βαθμός του μονωνύμου.

72. Έστω R υποδακτύλιος του $\mathbb{C}$. $x_1^{i_1}\,x_2^{i_2}\,\cdots\,x_n^{i_n}$, $x_1^{j_1}\,x_2^{j_2}\,\cdots\,x_n^{j_n}$ δύο μονώνυμα του $R[x_1,x_2,\ldots,x_n]$. Ορίζουμε μία σχέση διάταξης μεταξύ των μονωνύμων του $R[x_1,x_2,\ldots,x_n]$ ως εξής,

$$x_1^{i_1}\,x_2^{i_2}\,\cdots\,x_n^{i_n} > x_1^{j_1}\,x_2^{j_2}\,\cdots\,x_n^{j_n},$$

αν είτε,

$$\sum_{\ell=1}^{n} i_\ell > \sum_{\ell=1}^{n} j_\ell \tag{28}$$

είτε,

$$\sum_{\ell=1}^{n} i_\ell = \sum_{\ell=1}^{n} j_\ell \quad \text{και}$$
$$i_1 = j_1,\ i_2 = j_2,\ \ldots,\ i_k = j_k,\ i_{k+1} > j_{k+1},\ \text{με}\ k \in \{0, 1, \ldots, n-2\}. \tag{29}$$

Στην περίπτωση $k = 0$ εννοείτε $i_1 > j_1$. Ως παράδειγμα αναφέρουμε τα μονώνυμα του $R[x_1, x_2, x_3]$,

$$x_1\, x_2\, x_3^3 > x_1\, x_2^2\, x_3 > x_1\, x_2\, x_3^2.$$

Παρατηρούμε ότι με την πιο πάνω ορισθείσα διάταξη μονωνύμων, το μεγαλύτερο μονώνυμο ενός πολυωνύμου του $R[x_1, x_2, \ldots, x_n]$, (ως προς την διάταξη αυτή), ταυτίζεται με το μεγιστοβάθμιο μονώνυμο του πολυωνύμου αυτού. Βέβαια, το ίδιο δεν συμβαίνει με τα μονώνυμα μικρότερου βαθμού του πολυωνύμου αυτού. Δεν ταυτίζονται υποχρεωτικά με τα μονώνυμα του πολυωνύμου που έπονται με βάση την ορισθείσα πιο πάνω διάταξη.

73. Έστω R υποδακτύλιος του $\mathbb{C}$. Θεωρούμε το στοιχειώδες συμμετρικό πολυώνυμο του $R[x_1, x_2, \ldots, x_n]$,

$$e_k(x_1, x_2, \ldots, x_n) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1}\, x_{i_2} \cdots x_{i_k}.$$

Από την δομή του $e_k(x_1, x_2, \ldots, x_n)$ προκύπτει ότι κάθε μονώνυμό του είναι βαθμού k δηλαδή, όλα τα μονώνυμα του $e_k(x_1, x_2, \ldots, x_n)$ είναι ισοβάθμια. Αν θέλουμε να διατάξουμε τα μονώνυμα του $e_k(x_1, x_2, \ldots, x_n)$ με βάση τη διάταξη της παραγράφου 72 θα πρέπει να χρησιμοποιήσουμε το κριτήριο διάταξης (29). Κάθε μονώνυμο του $e_k(x_1, x_2, \ldots, x_n)$ μπορεί να γραφεί ως,

$$x_1^{j_1}\, x_2^{j_2} \cdots x_n^{j_n},$$

με $j_m = 0$ ή 1, $m = 1, 2, \ldots, n$. Θεωρούμε το μονώνυμο του $e_k(x_1, x_2, \ldots, x_n)$,

$$x_1\, x_2 \cdots x_k = x_1\, x_2 \cdots x_k\, x_{k+1}^0 \cdots x_n^0, \tag{30}$$

και ένα τυχαίο από τα υπόλοιπα μονώνυμα του $e_k(x_1, x_2, \ldots, x_n)$, το,

$$x_1^{j_1}\, x_2^{j_2} \cdots x_n^{j_n}, \tag{31}$$

με $j_m = 0$ ή 1, $m = 1, 2, \ldots, n$. Επειδή όλα τα πολυώνυμα έχουν προκύψει από αναγωγή ομοίων όρων, στο $e_k(x_1, x_2, \ldots, x_n)$ δεν υπάρχουν όμοια μονώνυμα και άρα δεν υπάρχουν δύο ταυτόσημες διατάξεις εκθετών $(j_1, j_2, \ldots, j_n)$. Η διάταξη εκθετών για το μονώνυμο (30) είναι,

$$(\underbrace{1, 1, \ldots, 1, 1}_{k \text{ το πλήθος}},\ \underbrace{0, 0, \ldots, 0}_{n-k \text{ το πλήθος}}), \tag{32}$$

Η διάταξη εκθετών για το μονώνυμο (31) περιέχει και αυτή k το πλήθος 1 αλλά όχι ακριβώς στις ίδιες θέσεις με την διάταξη εκθετών (32), (αλλιώς τα μονώνυμα (30), (31) θα ήταν όμοια). Αυτό σημαίνει ότι,

$$(j_1, j_2, \ldots, j_n) = (\underbrace{1, \ldots, 1}_{\ell \text{ το πλήθος}}, 0, j_{\ell+1}, \ldots, j_n),$$

με $0 \leq \ell \leq k-1$, $j_m = 0$ ή 1, $m = \ell+1, \ell+2, \ldots, n$. Είναι σαφές από το κριτήριο διάταξης μονωνύμων (29) ότι, το μεγαλύτερο ως προς την διάταξη της παραγράφου 72 μονώνυμο του $e_k(x_1, x_2, \ldots, x_n)$ είναι το $x_1\, x_2 \cdots x_k$.

74. Έστω R υποδακτύλιος του $\mathbb{C}$. $f_1(x)$, $f_2(x)$ πολυώνυμα του $R[x_1, x_2, \ldots, x_n]$. Διατάσουμε τα μονώνυμα των $f_1(x)$, $f_2(x)$ σύμφωνα με την διάταξη της παραγράφου 72. Έστω,

$$a_{i_1,i_2,\ldots,i_n}\, x_1^{i_1}\, x_2^{i_2} \cdots x_n^{i_n} \ ,\ b_{j_1,j_2,\ldots,j_n}\, x_1^{j_1}\, x_2^{j_2} \cdots x_n^{j_n},$$

δύο μονώνυμα των πολυωνύμων $f_1(x)$, $f_2(x)$ αντιστοίχως. Το γινόμενο $f_1(x)\, f_2(x)$ είναι το πολυώνυμο που προκύπτει αν πολλαπλασιάσουμε επιμεριστκώς τα $f_1(x)$, $f_2(x)$. Αυτό σημαίνει πως κάθε μονώνυμο του $f_1(x)$ πολλαπλασιάζεται με όλα τα μονώνυμα του $f_2(x)$ και προκύπτουν μονώνυμα της μορφής,

$$(a_{i_1,i_2,\ldots,i_n}\, b_{j_1,j_2,\ldots,j_n})\, x_1^{i_1+j_1}\, x_2^{i_2+j_2} \cdots x_n^{i_n+j_n}.$$

Έστω,

$$\gamma_{i_1,i_2,\ldots,i_n}\, x_1^{k_1}\, x_2^{k_2} \cdots x_n^{k_n} \ ,\ \delta_{j_1,j_2,\ldots,j_n}\, x_1^{h_1}\, x_2^{h_2} \cdots x_n^{h_n},$$

τα μεγαλύτερα, (ως προς τη διάταξη της παραγράφου 72), μονώνυμα των πολυωνύμων $f_1(x)$, $f_2(x)$ αντιστοίχως. Από τα κριτήρια (28), (29) προκύπτει ότι

- είτε,
$$\sum_{m=1}^{n} k_m > \sum_{m=1}^{n} i_m \text{ και } \sum_{m=1}^{n} h_m > \sum_{m=1}^{n} j_m,$$
οπότε και
$$\sum_{m=1}^{n} (k_m + h_m) > \sum_{m=1}^{n} (i_m + j_m),$$

- είτε,
$$\sum_{m=1}^{n} k_m > \sum_{m=1}^{n} i_m \text{ και } \sum_{m=1}^{n} h_m = \sum_{m=1}^{n} j_m \quad \text{με} \quad ,$$
$$h_1 = j_1,\ h_2 = j_2,\ \ldots,\ h_\ell = j_\ell,\ h_{\ell+1} > j_{\ell+1}, \quad \text{και} \quad \ell \in \{0, 1, \ldots, n-2\},$$
οπότε και
$$\sum_{m=1}^{n} (k_m + h_m) > \sum_{m=1}^{n} (i_m + j_m),$$

- είτε,
$$\sum_{m=1}^{n} k_m = \sum_{m=1}^{n} i_m \text{ και } \sum_{m=1}^{n} h_m > \sum_{m=1}^{n} j_m \quad \text{με} \quad ,$$
$$k_1 = i_1,\ k_2 = i_2,\ \ldots,\ k_\ell = i_\ell,\ k_{\ell+1} > i_{\ell+1}, \quad \text{και} \quad \ell \in \{0, 1, \ldots, n-2\},$$

οπότε και

$$\sum_{m=1}^{n}(k_m+h_m) > \sum_{m=1}^{n}(i_m+j_m),$$

- είτε,

$$\sum_{m=1}^{n} k_m = \sum_{m=1}^{n} i_m \text{ και } \sum_{m=1}^{n} h_m = \sum_{m=1}^{n} j_m \quad \text{με} \quad ,$$
$$k_1=i_1,\ k_2=i_2,\ \ldots,\ k_\ell=i_\ell,\ k_{\ell+1}>i_{\ell+1}, \quad \text{και} \quad \ell\in\{0,1,\ldots,n-2\},$$
$$h_1=j_1,\ h_2=j_2,\ \ldots,\ h_\theta=j_\theta,\ h_{\theta+1}>j_{\theta+1}, \quad \text{και} \quad \theta\in\{0,1,\ldots,n-2\},$$

οπότε, αν $\rho=\min\{\ell,\theta\}$,

$$\textstyle\sum_{m=1}^{n}(k_m+h_m)=\sum_{m=1}^{n}(i_m+j_m),$$
$$k_1+h_1=i_1+j_1,\ k_2+h_2=i_2+j_2,\ \ldots,\ k_\rho+h_\rho=i_\rho+j_\rho,$$
$$k_{\rho+1}+h_{\rho+1}>i_{\rho+1}+j_{\rho+1},\ \text{και}\ \rho\in\{0,1,\ldots,n-2\}.$$

Από τα πιο πάνω προκύπτει ότι το γινόμενο,

$$(\gamma_{i_1,i_2,\ldots,i_n}\,\delta_{j_1,j_2,\ldots,j_n})\,x_1^{k_1+h_1}\,x_2^{k_2+h_2}\,\cdots\,x_n^{k_n+h_n},$$

των μεγαλυτέρων, (ως προς τη διάταξη της παραγράφου 72), μονωνύμων των πολυωνύμων $f_1(x)$, $f_2(x)$ είναι το μεγαλύτερο, (ως προς τη διάταξη της παραγράφου 72), μονώνυμο του γινομένου $f_1(x)\,f_2(x)$.

75. Έστω R υποδακτύλιος του $\mathbb{C}$, $e_k(x_1,x_2,\ldots,x_n)$, $k=1,2,\ldots,n$ τα στοιχειώδη συμμετρικά πολυώνυμα του $R[x_1,x_2,\ldots,x_n]$. Από τις παραγράφους 73, 74 προκύπτει ότι το μεγαλύτερο μονώνυμο, (ως προς τη διάταξη της παραγράφου 72), του πολυωνύμου,

$$e_1^{\delta_1}(x_1,x_2,\ldots,x_n)\,e_2^{\delta_2}(x_1,x_2,\ldots,x_n)\,\cdots\,e_n^{\delta_n}(x_1,x_2,\ldots,x_n),$$

με $\delta_i\in\mathbb{N}$, $i=1,2,\ldots,n$ είναι το,

$$x_1^{\delta_1}\,(x_1\,x_2)^{\delta_2}\,\cdots\,(x_1\,x_2\,\cdots\,x_n)^{\delta_n}=x_1^{\sum_{i=1}^{n}\delta_i}\,x_2^{\sum_{i=2}^{n}\delta_i}\,\cdots\,x_n^{\delta_n}.$$

76. Έστω R υποδακτύλιος του $\mathbb{C}$, $f(x_1,x_2,\ldots,x_n)$ συμμετρικό πολυώνυμο του $R[x_1,x_2,\ldots,x_n]$. Θα αποδείξουμε ότι,

$$\begin{aligned} f(x_1,x_2,\ldots,x_n) \;=\; & \sum_{i_1=0}^{m_1}\sum_{i_2=0}^{m_2}\cdots\sum_{i_n=0}^{m_n}\Big(a_{i_1,i_2,\ldots,i_n}\,e_1^{i_1}(x_1,x_2,\ldots,x_n)\\ & e_2^{i_2}(x_1,x_2,\ldots,x_n)\,\cdots\,e_n^{i_n}(x_1,x_2,\ldots,x_n)\Big), \end{aligned}$$

με $a_{i_1,i_2,\ldots,i_n}\in R$, $e_k(x_1,x_2,\ldots,x_n)$, $k=1,2,\ldots,n$ τα στοιχειώδη συμμετρικά πολυώνυμα του $R[x_1,x_2,\ldots,x_n]$.

Κάθε συμμετρικό πολυώνυμο $f(x_1,x_2,\ldots,x_n)$ του $R[x_1,x_2,\ldots,x_n]$ που αποτελείται μόνο από ένα μονώνυμο, (ως προς τη διάταξη της παραγράφου 72),

επειδή ακριβώς είναι συμμετρικό ως προς τις μεταθέσεις των $x_1, x_2, \ldots, x_n$ θα γράφεται ως,

$$f(x_1, x_2, \ldots, x_n) = a\, x_1^p\, x_2^p \cdots x_n^p = a\, e_n^p(x_1, x_2, \ldots, x_n),\ a \in R,\ p \in \mathbb{N}.$$

Αποδείξαμε το συμπέρασμα για όλα τα συμμετρικά πολυώνυμα του $R[x_1, x_2, \ldots, x_n]$ που αποτελούνται μόνο από ένα μονώνυμο.

Υποθέτουμε ότι το προς απόδειξη συμπέρασμα ισχύει για όλα τα συμμετρικά πολυώνυμα του $R[x_1, x_2, \ldots, x_n]$ που αποτελούνται από $m-1$ μονώνυμα ως προς τη διάταξη της παραγράφου 72. Έστω τώρα τυχαίο πολυώνυμο του $R[x_1, x_2, \ldots, x_n]$, το $f(x_1, x_2, \ldots, x_n)$, που αποτελείται από m μονώνυμα. Διατάσουμε τα μονώνυμα του $f(x_1, x_2, \ldots, x_n)$ σύμφωνα με τη διάταξη της παραγράφου 72. Οπότε,

$$f(x_1, x_2, \ldots, x_n) = a_{j_1, j_2, \ldots, j_n}\, x_1^{j_1}\, x_2^{j_2} \cdots x_n^{j_n} + (\text{ Τα μικρότερα μονώνυμα}),$$

με $a_{j_1, j_2, \ldots, j_n}\, x_1^{j_1}\, x_2^{j_2} \cdots x_n^{j_n}$ το μεγαλύτερο μονώνυμο. Το $f(x_1, x_2, \ldots, x_n)$ είναι συμμετρικό ως προς τις μεταθέσεις των $x_1, x_2, \ldots, x_n$. Αυτό σημαίνει ότι το $f(x_1, x_2, \ldots, x_n)$ περιέχει όλα τα μονώνυμα που προκύπτουν από το $a_{j_1, j_2, \ldots, j_n}\, x_1^{j_1}\, x_2^{j_2} \cdots x_n^{j_n}$ αν εφαρμόσουμε σε αυτό όλες τις μεταθέσεις των $x_1, x_2, \ldots, x_n$. Άρα, για το μεγαλύτερο μονώνυμο του $f(x_1, x_2, \ldots, x_n)$ ισχύει $j_1 \geq j_2 \geq \cdots \geq j_n$, (γιατί ανάμεσα σε όλες τις μεταθέσεις των $j_1, j_2, \ldots, j_n$, εκείνη που ικανοποιεί τα κριτήρια (28), (29) της παραγράφου 72 είναι η έχουσα $j_1 \geq j_2 \geq \cdots \geq j_n$). Οπότε ξαναγράφουμε,

$$\begin{aligned} f(x_1, x_2, \ldots, x_n) &= a_{j_1, j_2, \ldots, j_n}\, x_1^{j_1}\, x_2^{j_2} \cdots x_n^{j_n} + (\text{ Τα μικρότερα μονώνυμα}), \\ &\text{με} \quad j_1 \geq j_2 \geq \cdots \geq j_n. \end{aligned}$$

Θεωρούμε το πολυώνυμο του $R[x_1, x_2, \ldots, x_n]$,

$$\begin{aligned} g(e_1, e_2, \ldots, e_n) &= e_1^{j_1 - j_2}(x_1, x_2, \ldots, x_n)\, e_2^{j_2 - j_3}(x_1, x_2, \ldots, x_n) \cdots \\ &\quad e_{n-1}^{j_{n-1} - j_n}(x_1, x_2, \ldots, x_n)\, e_n^{j_n}(x_1, x_2, \ldots, x_n). \end{aligned}$$

Από την παράγραφο 75 προκύπτει ότι το μεγαλύτερο μονώνυμο του $g(e_1, e_2, \ldots, e_n)$ είναι το,

$$x_1^{j_1}\, x_2^{j_2} \cdots x_n^{j_n}.$$

Το πολυώνυμο του $R[x_1, x_2, \ldots, x_n]$,

$$f(x_1, x_2, \ldots, x_n) - a_{j_1, j_2, \ldots, j_n}\, g(e_1, e_2, \ldots, e_n), \tag{33}$$

είναι συμμετρικό ως όλες τις μεταθέσεις των $x_1, x_2, \ldots, x_n$, και έχει $m-1$ μονώνυμα, (ως προς τη διάταξη της παραγράφου 72), αφού τα $f(x_1, x_2, \ldots, x_n)$ και $a_{j_1, j_2, \ldots, j_n}\, g(e_1, e_2, \ldots, e_n)$ έχουν το ίδιο μεγαλύτερο μονώνυμο. Από την υπόθεση της επαγωγής το,

$$\begin{aligned} &f(x_1, x_2, \ldots, x_n) - a_{j_1, j_2, \ldots, j_n}\, g(e_1, e_2, \ldots, e_n) = \\ &= \sum_{i_1=0}^{m_1} \sum_{i_2=0}^{m_2} \cdots \sum_{i_n=0}^{m_n} \Big(a_{i_1, i_2, \ldots, i_n}\, e_1^{i_1}(x_1, x_2, \ldots, x_n)\, e_2^{i_2}(x_1, x_2, \ldots, x_n) \end{aligned}$$

$$\cdots e_n^{i_n}(x_1,x_2,\ldots,x_n)\big) \Rightarrow$$
$$f(x_1,x_2,\ldots,x_n) =$$
$$= \; a_{j_1,j_2,\ldots,j_n}\, g(e_1,e_2,\ldots,e_n) + \sum_{i_1=0}^{m_1}\sum_{i_2=0}^{m_2}\cdots\sum_{i_n=0}^{m_n}\left(a_{i_1,i_2,\ldots,i_n}\, e_1^{i_1}\, e_2^{i_2}\,\cdots\, e_n^{i_n}\right).$$

με $e_k \equiv e_k(x_1,x_2,\ldots,x_n)$, $k=1,2,\ldots,n$. Το συμπέρασμα απεδείχθη για όλα όλα τα συμμετρικά πολυώνυμα του $R[x_1,x_2,\ldots,x_n]$ που αποτελούνται από m μονώνυμα ως προς τη διάταξη της παραγράφου 72.

77. Έστω F ένα υποσώμα του $\mathbb{C}$, $g(x)\in F[x]$, (πολυώνυμο με συντελεστές από το F), με ρίζες του αριθμούς $r_1,r_2,\ldots,r_n$. Αν $f(x_1,x_2,\ldots,x_n)$ είναι ένα συμμετρικό πολυώνυμο του $F[x_1,x_2,\ldots,x_n]$ θα αποδείξουμε ότι $f(r_1,r_2,\ldots,r_n)\in F$.

Επειδή, κάθε σώμα είναι και δακτύλιος όλα τα αποτελέσματα των προηγούμενων παραγράφων που αναφέρονται στο $R[x_1,x_2,\ldots,x_n]$ για κάποιο υποδακτύλιο R του $\mathbb{C}$ ισχύουν ομοίως και για το $F[x_1,x_2,\ldots,x_n]$ για κάποιο υποσώμα F του $\mathbb{C}$. Έστω $g(x)=\sum_{i=0}^{n} a_i\, x_i$, $a_n\neq 0$. Τότε και $g(x)=a_n\,(x-r_1)\,(x-r_2)\,\cdots\,(x-r_n)$. Έστω και $f(x_1,x_2,\ldots,x_n)$ ένα συμμετρικό πολυώνυμο του $F[x_1,x_2,\ldots,x_n]$. Από την παράγραφο 76 προκύπτει ότι,

$$\begin{aligned} f(x_1,x_2,\ldots,x_n) \;=\; & \sum_{i_1=0}^{m_1}\sum_{i_2=0}^{m_2}\cdots\sum_{i_n=0}^{m_n}\Big(a_{i_1,i_2,\ldots,i_n}\, e_1^{i_1}(x_1,x_2,\ldots,x_n) \\ & e_2^{i_2}(x_1,x_2,\ldots,x_n)\,\cdots\, e_n^{i_n}(x_1,x_2,\ldots,x_n)\Big), \end{aligned}$$

με $a_{i_1,i_2,\ldots,i_n}\in F$, $e_k(x_1,x_2,\ldots,x_n)$, $k=1,2,\ldots,n$ τα στοιχειώδη συμμετρικά πολυώνυμα του $F[x_1,x_2,\ldots,x_n]$. Άρα,

$$\begin{aligned} f(r_1,r_2,\ldots,r_n) \;=\; & \sum_{i_1=0}^{m_1}\sum_{i_2=0}^{m_2}\cdots\sum_{i_n=0}^{m_n}\Big(a_{i_1,i_2,\ldots,i_n}\, e_1^{i_1}(r_1,r_2,\ldots,r_n) \\ & e_2^{i_2}(r_1,r_2,\ldots,r_n)\,\cdots\, e_n^{i_n}(r_1,r_2,\ldots,r_n)\Big). \end{aligned}$$

Από την παράγραφο 70 προκύπτει ότι,

$$f(r_1,r_2,\ldots,r_n) =$$
$$= \sum_{i_1=0}^{m_1}\sum_{i_2=0}^{m_2}\cdots\sum_{i_n=0}^{m_n} a_{i_1,i_2,\ldots,i_n}\left(-\frac{a_{n-1}}{a_n}\right)^{i_1}\left(\frac{a_{n-2}}{a_n}\right)^{i_2}\cdots\left((-1)^n\,\frac{a_0}{a_n}\right)^{i_n}\in F,$$

ως αποτέλεσμα πράξεων μεταξύ αριθμών που ανήκουν στο σώμα F.

78. Έστω $a,n,k\in\mathbb{N}$, $k\leq n$. Ορίζουμε ως,

$$a! = 1\cdot 2\cdot 3\cdot\ldots\cdot(a-1)\cdot a,\;\; 0!=1,$$
$$\binom{n}{0}=1\,,\binom{n}{k}=\frac{n!}{k!\,(n-k)!}\,,0<k\leq n \quad .$$

Θα αποδείξουμε ότι τα $\binom{n}{k}$ έτσι όπως ορίσθηκαν είναι πάντα φυσικοί αριθμοί. Θα εφαρμόσουμε επαγωγή στο n. Για κάθε $n\in\mathbb{N}$ και $k=0$ το συμπέρασμα προφανώς ισχύει, (από τον πιο πάνω ορισμό). Για κάθε $n\in\mathbb{N}-\{0\}$ και $k=1$,

$\binom{n}{k} = \frac{n!}{(n-1)!} = n$ και το συμπέρασμα ισχύει. Υποθέτουμε ότι το συμπέρασμα ισχύει για κάθε $n \in \mathbb{N} - \{0\}$ και κάθε k με $0 < k \leq n$. Τότε από την ταυτότητα,

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1},$$

και την υπόθεση της επαγωγής προκύπτει το προς απόδειξη συμπέρασμα για $n+1$ και $0 < k \leq n$. Τέλος, για $k = n+1$, $\binom{n+1}{n+1} = 1$ και το συμπέρασμα ισχύει για $n+1$ και $0 < k \leq n+1$.

Επίσης, θα αποδείξουμε ότι το γινόμενο p το πλήθος διαδοχικών μη μηδενικών φυσικών αριθμών διαιρείται με το $p!$. Από τα προηγούμενα μπορούμε να γράψουμε για το γινόμενο $(m+1)(m+2)\cdots(m+p)$, p το πλήθος μη μηδενικών φυσικών αριθμών,

$$(m+1)(m+2)\cdots(m+p) = p!\,\frac{(m+p)!}{p!\,m!} = p!\binom{m+p}{p},$$

και το συμπέρασμα προκύπτει επειδή το $\binom{m+p}{p}$ είναι φυσικός αριθμός.

79. Έστω οι μιγαδικοί αριθμοί $r_1, r_2, \ldots, r_n$ και $\ell \in \{1, 2, \ldots, n\}$. Επιλέγουμε ℓ το πλήθος διακεκριμένους αριθμούς από το $\{r_1, r_2, \ldots, r_n\}$, π.χ. τους $r_{j_1}, r_{j_2}, \ldots, r_{j_\ell}$ και τους αθρίζουμε. Συμβολίζουμε το άθροισμα αυτό με,

$$s_{j_1, j_2, \ldots, j_\ell} = r_{j_1} + r_{j_2} + \cdots + r_{j_\ell}.$$

Μπορούμε να σχηματίσουμε $\binom{n}{\ell}$ το πλήθος από τέτοια αθροίσματα γιατί ο αριθμός $\binom{n}{\ell}$, (ως γνωστόν από την Συνδυαστική), εκφράζει το πλήθος των διαφορετικών επιλογών ℓ διακεκριμένων στοιχείων από ένα σύνολο n στοιχείων.

80. Έστω F ένα υποσώμα του $\mathbb{C}$, $\ell \in \{1, 2, \ldots, n\}$, $p\left(x_1, x_2, \ldots, x_{\binom{n}{\ell}}\right)$ ένα συμμετρικό πολυώνυμο του $F\left[x_1, x_2, \ldots, x_{\binom{n}{\ell}}\right]$. Θεωρούμε το πολυώνυμο,

$$\begin{aligned} f(y_1, y_2, \ldots, y_n) \;=\; & p\left((y_1 + y_2 + \cdots + y_\ell), \ldots, (y_{j_1} + y_{j_2} + \ldots + y_{j_\ell}),\right. \\ & \left. \ldots, (y_{n-\ell+1} + y_{n-\ell+2} + \cdots + y_n)\right), \end{aligned}$$

δηλαδή, αντικαθιστούμε στην θέση του κάθε x_i, $i = 1, 2, \ldots, \binom{n}{\ell}$ κάθε ένα από τα $\binom{n}{\ell}$ το πλήθος διαφορετικά αθροίσματα που δημιουργούνται αν από τις μεταβλητές $y_1, y_2, \ldots, y_n$ επιλέξουμε όλες τις δυνατές ℓ-άδες διακεκριμένων y_γ, $\gamma = 1, 2, \ldots, n$.

Θα αποδείξουμε ότι το $f(y_1, y_2, \ldots, y_n)$ είναι ένα συμμετρικό πολυώνυμο του $F[y_1, y_2, \ldots, y_n]$. Έστω ότι στη n-άδα $y_1, y_2, \ldots, y_n$ αντιμεταθέτουμε δύο τυχαία στοιχεία π.χ. τα y_τ, y_ν. Τότε τα αθροίσματα $y_{j_1} + y_{j_2} + \ldots + y_{j_\ell}$ που περιέχουν και τα δύο τα y_τ, y_ν καθώς και τα αθροίσματα $y_{j_1} + y_{j_2} + \ldots + y_{j_\ell}$ που περιέχουν κανένα από τα y_τ, y_ν μένουν αμετάβλητα ενώ τα υπόλοιπα αθροίσματα $y_{j_1} + y_{j_2} + \ldots + y_{j_\ell}$ που περιέχουν ακριβώς το y_τ αντιμετατίθενται με τα αθροίσματα $y_{j_1} + y_{j_2} + \ldots + y_{j_\ell}$ που περιέχουν ακριβώς το y_ν. Οι αντιμεταθέσεις των διαφόρων αθροισμάτων $y_{j_1} + y_{j_2} + \ldots + y_{j_\ell}$ στο πολυώνυμο,

$$\begin{aligned} & p\left((y_1 + y_2 + \cdots + y_\ell), \ldots, (y_{j_1} + y_{j_2} + \ldots + y_{j_\ell}),\right. \\ & \left. \ldots, (y_{n-\ell+1} + y_{n-\ell+2} + \cdots + y_n)\right), \end{aligned}$$

αντιστοιχούν σε αντιμεταθέσεις των μεταβλητών x_i, (στις θέσεις των οποίων τοποθετήσαμε τα αθροίσματα $y_{j_1}+y_{j_2}+\ldots+y_{j_\ell}$), στο πολυώνυμο $p\left(x_1,x_2,\ldots,x_{\binom{n}{\ell}}\right)$. Από την συμμετρικότητα του πολυωνύμου αυτού ως προς τις μεταβλητές $x_1,x_2,\ldots,x_{\binom{n}{\ell}}$ προκύπτει ότι και το πολυώνυμο,

$$p\left((y_1+y_2+\cdots+y_\ell),\ldots,(y_{j_1}+y_{j_2}+\ldots+y_{j_\ell}),\right.$$
$$\left.\ldots,(y_{n-\ell+1}+y_{n-\ell+2}+\cdots+y_n)\right),$$

είναι συμμετρικό ως προς τις αντιμεταθέσεις των $y_1,y_2,\ldots,y_n$. Επειδή, κάθε μετάθεση των $y_1,y_2,\ldots,y_n$ προκύπτει από μία σειρά αντιμεταθέσεων των $y_1,y_2,\ldots,y_n$ προκύπτει ότι το πολυώνυμο,

$$p\left((y_1+y_2+\cdots+y_\ell),\ldots,(y_{j_1}+y_{j_2}+\ldots+y_{j_\ell}),\right.$$
$$\left.\ldots,(y_{n-\ell+1}+y_{n-\ell+2}+\cdots+y_n)\right),$$

είναι συμμετρικό ως προς τις μεταθέσεις των $y_1,y_2,\ldots,y_n$.

81. Έστω F ένα υποσώμα του $\mathbb{C}$, $g(x)\in F[x]$ με ρίζες $r_1,r_2,\ldots,r_n$, $\ell\in\{1,2,\ldots,n\}$, $s_{j_1,j_2,\ldots,j_\ell}$ τα αθροίσματα που ορίσθηκαν στην παράγραφο 79. Θα αποδείξουμε ότι υπάρχει πολυώνυμο $h_\ell(x)\in F[x]$ τέτοιο ώστε οι ρίζες του να είναι τα $\binom{n}{\ell}$ το πλήθος αθροίσματα $s_{j_1,j_2,\ldots,j_\ell}$. Θέτουμε,

$$h_\ell(x)=\prod_{1\le j_1<j_2<\cdots<j_\ell\le n}(x-s_{j_1,j_2,\ldots,j_\ell}).$$

Τονίζουμε ότι το πλήθος των επιλογών για τα $j_1,j_2,\ldots,j_\ell$ ώστε να ισχύει $1\le j_1<j_2<\cdots<j_\ell\le n$ είναι $\binom{n}{\ell}$. Άρα το γινόμενο που δημιουργεί το πολυώνυμο $h_\ell(x)$ περιέχει $\binom{n}{\ell}$ το πλήθος παράγοντες. Το $h_\ell(x)$ έχει τις επιθυμητές ρίζες. Αρκεί να αποδείξουμε ότι αυτό ανήκει στο $F[x]$ δηλαδή, ότι οι συντελεστές των μονωνύμων του είναι στοιχεία του σώματος F. Αναπτύσσοντας το $h_\ell(x)$ προκύπτει,

$$h_\ell(x)=\prod_{1\le j_1<j_2<\cdots<j_\ell\le n}(x-s_{j_1,j_2,\ldots,j_\ell})=\sum_{i=0}^{\binom{n}{\ell}}a_i\,x^i\ ,\ a_{\binom{n}{\ell}}=1.$$

Από την παράγραφο 70 προκύπτει ότι,

$$\begin{aligned}
-a_{\binom{n}{\ell}-1} &= e_1(s_{1,2,\ldots,\ell},\ldots,s_{j_1,j_2,\ldots,j_\ell},\ldots,s_{n-\ell+1,n-\ell+2,\ldots,n}),\\
a_{\binom{n}{\ell}-2} &= e_2(s_{1,2,\ldots,\ell},\ldots,s_{j_1,j_2,\ldots,j_\ell},\ldots,s_{n-\ell+1,n-\ell+2,\ldots,n}),\\
&\vdots\\
(-1)^k\,a_{\binom{n}{\ell}-k} &= e_k(s_{1,2,\ldots,\ell},\ldots,s_{j_1,j_2,\ldots,j_\ell},\ldots,s_{n-\ell+1,n-\ell+2,\ldots,n}),\qquad (34)\\
&\vdots\\
(-1)^{\binom{n}{\ell}}\,a_0 &= e_{\binom{n}{\ell}}(s_{1,2,\ldots,\ell},\ldots,s_{j_1,j_2,\ldots,j_\ell},\ldots,s_{n-\ell+1,n-\ell+2,\ldots,n}),
\end{aligned}$$

όπου $e_k\left(x_1,x_2,\ldots,x_{\binom{n}{\ell}}\right)$ τα στοιχειώδη συμμετρικά πολυώνυμα του $F\left[x_1,\right.$

$x_2, \ldots, x_{\binom{n}{\ell}}\Big]$. Όμως,

$$e_k(s_{1,2,\ldots,\ell}, \ldots, s_{j_1,j_2,\ldots,j_\ell}, \ldots, s_{n-\ell+1,n-\ell+2,\ldots,n}) = e_k\left((r_1 + r_2 + \cdots + r_\ell), \ldots, (r_{j_1} + r_{j_2} + \ldots + r_{j_\ell}), \ldots, (r_{n-\ell+1} + r_{n-\ell+2} + \cdots + r_n)\right).$$

Από τις παραγράφους 77, 80, (για $p = e_k$, $y_1 = r_1$, $y_2 = r_2$, ..., $y_n = r_n$), προκύπτει ότι το,

$$f(r_1, r_2, \ldots, r_n) = e_k(s_{1,2,\ldots,\ell}, \ldots, s_{j_1,j_2,\ldots,j_\ell}, \ldots, s_{n-\ell+1,n-\ell+2,\ldots,n}) \in F,$$

για $k = 1, 2, \ldots, \binom{n}{\ell}$. Τότε από τις ισότητες (34) και τα $(-1)^k\, a_{\binom{n}{\ell}-k} \in F$ για $k = 1, 2, \ldots, \binom{n}{\ell}$. Επειδή το F είναι σώμα και τα $a_{\binom{n}{\ell}-k} \in F$ για $k = 1, 2, \ldots, \binom{n}{\ell}$. Οι συντελεστές του $h_\ell(x)$ ανήκουν στο F και το συμπέρασμα απεδείχθη.

82. Έστω $a \in \mathbb{R}$. Ορίζουμε ως ακέραιο μέρος του a τον μεγαλύτερο ακέραιο b που είναι μικρότερος ή και ίσος του a δηλαδή, $b \leq a < b + 1$. Θα συμβολίζουμε $b = \lfloor a \rfloor$.

83. Έστω $z = a + b\, i$ μιγαδικός αριθμός. Από την Μιγαδική Ανάλυση είναι γνωστό ότι $e^z = e^a\, (\sigma\upsilon\nu(b) + i\ \eta\mu(b))$. Αν $z = \pi\, i$ προκύπτει ότι, $e^{\pi\, i} = -1$.

84. Έστω $r_1, r_2, \ldots, r_n$ μιγαδικοί αριθμοί, $u_1 = e^{r_1}$, $u_2 = e^{r_2}$, ..., $u_n = e^{r_n}$. Αναπτύσσοντας το πιο κάτω γινόμενο παίρνουμε,

$$\begin{aligned}
(x + u_1)\,(x + u_2) \cdots (x + u_n) &= x^n + \sum_{\ell=1}^{n} e_\ell(u_1, u_2, \ldots, u_n)\, x^{n-\ell} \Rightarrow \\
(1 + e^{r_1})\,(1 + e^{r_2}) \cdots (1 + e^{r_n}) &= 1 + \sum_{\ell=1}^{n} e_\ell(e^{r_1}, e^{r_2}, \ldots, e^{r_n}) = \\
&= 1 + \sum_{\ell=1}^{n} \left(\sum_{1 \leq j_1 < j_2 < \cdots < j_\ell \leq n} e^{r_{j_1} + r_{j_2} + \cdots + r_{j_\ell}} \right),
\end{aligned}$$

όπου e_ℓ τα στοιχειώδη συμμετρικά πολυώνυμα του $\mathbb{C}[x_1, x_2, \ldots, x_n]$.

85. Έστω ότι υπάρχει πολυώνυμο, (όχι ταυτοτικά μηδέν), $f(x) = \sum_{j=0}^{m} a_j\, x^j$ του $\mathbb{Z}[x]$ ώστε ο π να είναι ρίζα του. Τότε,

$$\begin{aligned}
\sum_{j=0}^{m} a_j\, \pi^j = 0 \Rightarrow \sum_{j=0}^{m} a_j\, (\pi\, i)^j\, (-i)^j = 0 \quad &\Rightarrow \\
\sum_{k=0}^{\lfloor m/2 \rfloor} (-1)^k\, a_{2\,k}\, (\pi\, i)^{2\,k} + i \sum_{k=0}^{\lfloor (m-1)/2 \rfloor} (-1)^{k+1}\, a_{2\,k+1}\, (\pi\, i)^{2\,k+1} = 0 \quad &\Rightarrow \\
\sum_{k=0}^{\lfloor m/2 \rfloor} (-1)^k\, a_{2\,k}\, (\pi\, i)^{2\,k} = i \sum_{k=0}^{\lfloor (m-1)/2 \rfloor} (-1)^k\, a_{2\,k+1}\, (\pi\, i)^{2\,k+1} \quad &\Rightarrow \\
\left[\sum_{k=0}^{\lfloor m/2 \rfloor} (-1)^k\, a_{2\,k}\, (\pi\, i)^{2\,k} \right]^2 = - \left[\sum_{k=0}^{\lfloor (m-1)/2 \rfloor} (-1)^k\, a_{2\,k+1}\, (\pi\, i)^{2\,k+1} \right]^2 \quad &\Rightarrow
\end{aligned}$$

$$\left[\sum_{k=0}^{\lfloor m/2\rfloor}(-1)^k\,a_{2\,k}\,(\pi\,i)^{2\,k}\right]^2+\left[\sum_{k=0}^{\lfloor (m-1)/2\rfloor}(-1)^k\,a_{2\,k+1}\,(\pi\,i)^{2\,k+1}\right]^2=0\quad,\ (35)$$

από όπου προκύπτει ότι και ο $\pi\,i$ είναι ρίζα πολυωνύμου του $\mathbb{Z}[x]$. Το πολυώνυμο (35) είναι βαθμού το πολύ $2\,m$ και δεν είναι ταυτοτικά το μηδενικό πολυώνυμο, (γιατί αν ήταν τότε όλοι οι συντελεστές του θα ήταν μηδέν. Όπως μπορούμε να διαπιστώσουμε αναπτύσσοντας τα τετράγωνα στο πολυώνυμο (35), εμφανίζονται προσθεταίοι της μορφής $a_{2\,k}^2(\pi\,i)^{4\,k}$ και $a_{2\,k+1}^2(\pi\,i)^{4\,k+2}$ για $k=1,2,\ldots,\lfloor m/2\rfloor$, $k=1,2,\ldots,\lfloor (m-1)/2\rfloor$ αντιστοίχως.

Αν λοιπόν το πολυώνυμο (35) ήταν ταυτοτικά το μηδενικό πολυώνυμο τότε και $a_{2\,k}^2=0$, $a_{2\,k+1}^2=0$ για $k=1,2,\ldots,\lfloor m/2\rfloor$, $k=1,2,\ldots,\lfloor (m-1)/2\rfloor$ αντιστοίχως. Ως επακόλουθο, $a_{2\,k}=0$, $a_{2\,k+1}=0$ για $k=1,2,\ldots,\lfloor m/2\rfloor$, $k=1,2,\ldots,\lfloor (m-1)/2\rfloor$ αντιστοίχως. Όμως τα $a_{2\,k}$, $a_{2\,k+1}$ για $k=1,2,\ldots,\lfloor m/2\rfloor$, $k=1,2,\ldots,\lfloor (m-1)/2\rfloor$ αντιστοίχως, είναι όλοι οι συντελεστές του, (μη ταυτοτικά μηδενικού), πολυωνύμου $f(x)$ που υποθέσαμε στην αρχή ότι έχει τον π ως ρίζα. Τουλάχιστον ένα από τα $a_{2\,k}$, $a_{2\,k+1}$ δεν είναι μηδέν οδηγώντας σε άτοπο την υπόθεση ότι το πολυώνυμο (35) είναι ταυτοτικά το μηδενικό πολυώνυμο).

86. Από την παράγραφο 85 προκύπτει ότι, αν υπάρχει πολυώνυμο με ακέραιους συντελεστές όχι ταυτοτικά μηδέν που να έχει το π ως ρίζα τότε, υπάρχει πολυώνυμο με ακέραιους συντελεστές όχι ταυτοτικά μηδέν που να έχει το $\pi\,i$ ως ρίζα.

Έστω n ο βαθμός του πολυωνύμου $g(x)\in\mathbb{Z}[x]$ που έχει το $r_1=\pi\,i$ ως ρίζα και $r_2,\ldots,r_n$ οι υπόλοιπες ρίζες του. Από τις παραγράφους 83, 84 προκύπτει ότι,

$$\begin{aligned}0&=(1+e^{r_1})\,(1+e^{r_2})\cdots(1+e^{r_n})=\\&=1+\sum_{\ell=1}^{n}\left(\sum_{1\le j_1<j_2<\cdots<j_\ell\le n}e^{r_{j_1}+r_{j_2}+\cdots+r_{j_\ell}}\right)=\\&=1+\sum_{\ell=1}^{n}\left(\sum_{1\le j_1<j_2<\cdots<j_\ell\le n}e^{s_{j_1,j_2,\ldots,j_\ell}}\right),\end{aligned}\qquad(36)$$

με $s_{j_1,j_2,\ldots,j_\ell}$ όπως ορίσθηκαν στην παράγραφο 79. Επειδή $\mathbb{Z}[x]\subset\mathbb{Q}[x]$ έπεται ότι $g(x)\in\mathbb{Q}[x]$. Από την παράγραφο 81, (με $F=\mathbb{Q}$), προκύπτει ότι για κάθε $\ell\in\{1,2,\ldots,n\}$ υπάρχει πολυώνυμο $h_\ell(x)\in\mathbb{Q}[x]$ που να έχει ως ρίζες ακριβώς τα $s_{j_1,j_2,\ldots,j_\ell}$ για όλα τα $1\le j_1<j_2<\cdots<j_\ell\le n$.

Το πολυώνυμο $b(x)=\prod_{\ell=1}^{n}h_\ell(x)\in\mathbb{Q}[x]$ έχει ως ρίζες ακριβώς τα $s_{j_1,j_2,\ldots,j_\ell}$ για όλα τα $1\le j_1<j_2<\cdots<j_\ell\le n$ και όλα τα $\ell=1,2,\ldots,n$. Αν υπάρχουν δ το πλήθος αριθμοί $s_{j_1,j_2,\ldots,j_\ell}$ ίσοι με μηδέν τότε, το πολυώνυμο,

$$t(x)=LCM(\text{των παρονομαστών των συντελεστών του } b(x))\,\frac{b(x)}{x^\delta},$$

ανήκει στο $\mathbb{Z}[x]$ και έχει ως ρίζες ακριβώς τα μη μηδενικά $s_{j_1,j_2,\ldots,j_\ell}$ για όλα τα $1\le j_1<j_2<\cdots<j_\ell\le n$ και όλα τα $\ell=1,2,\ldots,n$. Ας συμβολίσουμε με $q_1,q_2,\ldots,q_m$ τα μη μηδενικά $s_{j_1,j_2,\ldots,j_\ell}$ για όλα τα $1\le j_1<j_2<\cdots<j_\ell\le n$ και όλα τα $\ell=1,2,\ldots,n$. Άρα, $t(x)=\sum_{\zeta=0}^{m}a_\zeta\,x^\zeta$ με ρίζες $q_1,q_2,\ldots,q_m$. Επίσης,

από την (36) αν αθροίσουμε τις μονάδες που προκύπτουν ως αποτελέσματα των δυνάμεων $e^{s_{j_1,j_2,\ldots,j_\ell}}$ για τα δ το πλήθος μηδενικά $s_{j_1,j_2,\ldots,j_\ell}$ προκύπτει,

$$0 = (\delta + 1) + e^{q_1} + e^{q_2} + \cdots + e^{q_m}. \tag{37}$$

Έστω p ένας πρώτος αριθμός, $\sigma = m\,p - 1$. Θεωρούμε το πολυώνυμο,

$$u(x) = \frac{a_m^\sigma\, x^{p-1}\,[t(x)]^p}{(p-1)!} \in \mathbb{Q}[x].$$

Ο βαθμός του $u(x)$ είναι $\sigma + p$. Επίσης, θεωρούμε το πολυώνυμο,

$$U(x) = u(x) + u^{(1)}(x) + u^{(2)}(x) + \cdots + u^{(\sigma+p)}(x) \in \mathbb{Q}[x],$$

όπου $\theta^{(\nu)}(x)$ συμβολίζει την ν τάξης παράγωγο μίας συνάρτησης θ με τύπο $\theta(x)$. Θεωρούμε και την συνάρτηση $\phi : \mathbb{C} \mapsto \mathbb{C}$ με τύπο, $\phi(w) = e^{-x\,w}\,U(x\,w)$.

$$\begin{aligned}\phi'(w) &= \frac{\partial\phi(w)}{\partial w} = \frac{\partial(e^{-x\,w}\,U(x\,w))}{\partial w} = \\ &= -x\,e^{-x\,w}\,U(x\,w) + x\,e^{-x\,w}\,(u^{(1)}(x\,w) + \cdots + u^{(\sigma+p+1)}(x\,w)).\end{aligned}$$

Όμως το πολυώνυμο $u(x\,w)$ είναι βαθμού $\sigma + p$. Η παράγωγος $u^{(\sigma+p+1)}(x\,w)$ είναι ταυτοτικά το μηδενικό πολυώνυμο και,

$$\phi'(w) = -x\,e^{-x\,w}\,u(x\,w). \tag{38}$$

Από το Θεμελιώδες Θεώρημα του Ολοκληρωτικού Λογισμού για την (38) έπεται,

$$\begin{aligned}\phi(1) - \phi(0) &= \int_0^1 -x\,e^{-x\,w}\,u(x\,w)\,dw \Rightarrow \\ U(x) - e^x\,U(0) &= \int_0^1 -x\,e^{x\,(1-w)}\,u(x\,w)\,dw.\end{aligned} \tag{39}$$

Αθροίζοντας τις ισότητες (39) διαδοχικά για $x = q_1, q_2, \ldots, q_m$ και λαμβάνοντας υπ΄ όψιν την (37) παίρνουμε,

$$\sum_{\mu=1}^{m} U(q_\mu) + (\delta + 1)\,U(0) = -\sum_{\mu=1}^{m} \int_0^1 q_\mu\,e^{q_\mu\,(1-w)}\,u(q_\mu\,w)\,dw. \tag{40}$$

Στόχος μας είναι να αποδείξουμε ότι για κάθε ε θετικό πραγματικό αριθμό, ο πρώτος p, (όπως εμφανίζεται στον ορισμό του $u(x)$), μπορεί να επιλεγεί με τέτοιο τρόπο ώστε το αριστερό σκέλος της (40) να είναι ένας μη μηδενικός ακέραιος ενώ το δεξί σκέλος της (40) μικρότερο του ε.

87. Με τις υποθέσεις και τους συμβολισμούς της παραγράφου 86 θα αποδείξουμε ότι ο $\sum_{\mu=1}^{m} U(q_\mu)$ είναι ακέραιος διαιρετός από τον p.

Από τον ορισμό του $U(x)$ προκύπτει ότι,

$$\sum_{\mu=1}^{m} U(q_\mu) = \sum_{\mu=1}^{m}\sum_{\tau=0}^{\sigma+p} u^{(\tau)}(q_\mu) = \sum_{\tau=0}^{\sigma+p}\sum_{\mu=1}^{m} u^{(\tau)}(q_\mu).$$

Από τον κανόνα παραγώγισης γινομένου του Leibniz προκύπτει ότι,

$$u^{(\tau)}(x) = \frac{a_m^\sigma}{(p-1)!} \sum_{\xi=0}^{\tau} \binom{\tau}{\xi} \left(x^{p-1}\right)^{(\tau-\xi)} \, [t^p(x)]^{(\xi)}.$$

Έστω $0 \leq \xi \leq p-1$. Θα αποδείξουμε, εφαρμόζοντας επαγωγή στο ξ ότι, $[t^p(x)]^{(\xi)} = t^{p-\xi}(x)\,\psi(x)$ με $\psi(x)$ κάποιο πολυώνυμο του $\mathbb{Q}[x]$. Για $\xi = 0$ το συμπέρασμα ισχύει τετριμμένα για $\psi(x) = 1$ επειδή $[t^p(x)]^{(0)} = t^p(x)$. Υποθέτουμε το συμπέρασμα για $\xi = p-2$ δηλαδή, $[t^p(x)]^{(p-2)} = t^2(x)\,\psi(x)$ με $\psi(x)$ κάποιο πολυώνυμο του $\mathbb{Q}[x]$. Τότε,

$$[t^p(x)]^{(p-1)} = \Big([t^p(x)]^{(p-2)}\Big)' = \big(t^2(x)\,\psi(x)\big)' = t(x)\,(2\,t'(x)\,\psi(x) + t(x)\,\psi'(x)).$$

και το συμπέρασμα απεδείχθη για $\xi = p-1$. Από το προηγούμενο προκύπτει ότι, αν $\tau \leq p-1$,

$$u^{(\tau)}(x) = \frac{a_m^\sigma}{(p-1)!} \sum_{\xi=0}^{\tau} \binom{\tau}{\xi} \left(x^{p-1}\right)^{(\tau-\xi)} \, t^{p-\xi}(x)\,\psi(x) \Rightarrow u^{(\tau)}(q_\mu) \;\; =$$

$$= \frac{a_m^\sigma}{(p-1)!} \sum_{\xi=0}^{\tau} \binom{\tau}{\xi} \frac{(p-1)!}{(p-1-\tau+\xi)!}\, q_\mu^{p-1-\tau+\xi}\, t^{p-\xi}(q_\mu)\,\psi(q_\mu) \;\; = \;\; 0,$$

επειδή, q_μ είναι ρίζα του $t(x)$ και $t^{p-\xi}(q_\mu) = 0$ για $0 \leq \xi \leq p-1$. Οπότε,

$$\sum_{\mu=1}^{m} U(q_\mu) \;\; = \;\; \sum_{\tau=0}^{\sigma+p} \sum_{\mu=1}^{m} u^{(\tau)}(q_\mu) = \sum_{\tau=0}^{p-1} \sum_{\mu=1}^{m} u^{(\tau)}(q_\mu) + \sum_{\tau=p}^{\sigma+p} \sum_{\mu=1}^{m} u^{(\tau)}(q_\mu) \Rightarrow$$

$$\sum_{\mu=1}^{m} U(q_\mu) \;\; = \;\; \sum_{\tau=p}^{\sigma+p} \sum_{\mu=1}^{m} u^{(\tau)}(q_\mu). \tag{41}$$

Γνωρίζουμε ότι, το $u(x)$ είναι πολυώνυμο βαθμού $\sigma + p$. Μπορούμε λοιπόν να γράψουμε, $u(x) = \frac{a_m^\sigma}{(p-1)!} \sum_{\nu=0}^{\sigma+p} \eta_\nu\, x^\nu$ με $\eta_\nu \in \mathbb{Z}$, $\eta_{\sigma+p} \neq 0$. Για $p \leq \tau \leq \sigma + p$ έπεται,

$$u^{(\tau)}(x) = \frac{a_m^\sigma}{(p-1)!} \sum_{\nu=\tau}^{\sigma+p} \nu\,(\nu-1)\,\cdots\,(\nu-\tau+1)\,\eta_\nu\, x^{\nu-\tau},$$

γιατί τα μονώνυμα του $u(x)$ βαθμού μικρότερου του τ γίνονται μηδέν μετά από τ το πλήθος διαδοχικές παραγωγίσεις. Βλέπουμε ότι, για $p \leq \tau \leq \sigma + p$, οι συντελεστές του πολυωνύμου $a_m^{-\sigma}\,(p-1)!\,u^{(\tau)}(x)$ είναι ακέραιοι που περιέχουν το γινόμενο τ, (άρα και p), το πλήθος διαδοχικών φυσικών αριθμών. Όσοι από τους συντελεστές αυτούς είναι 0 προφανώς διαιρούνται με το $p!$. Όσοι δεν είναι 0 διαιρούνται με το $p!$ γιατί πληρούνται οι προϋποθέσεις της παραγράφου 78. Άρα,

$$u^{(\tau)}(x) = \frac{a_m^\sigma\, p!}{(p-1)!} \sum_{\nu=\tau}^{\sigma+p} v_\nu\, x^{\nu-\tau} = a_m^\sigma\, p \sum_{\nu=\tau}^{\sigma+p} v_\nu\, x^{\nu-\tau} = a_m^\sigma\, p\, \omega(x), \tag{42}$$

με $v_\nu \in \mathbb{Z}$, $v_{\sigma+p} \neq 0$, τα πηλίκα της διαίρεσης των $\nu\,(\nu-1)\,\cdots\,(\nu-\tau+1)\,\eta_\nu$ με τον $p!$, $\omega(x) \in \mathbb{Z}[x]$. Θεωρούμε το πολυώνυμο του $\mathbb{Z}[x_1, x_2, \ldots, x_m]$,

$$\Pi(x_1, x_2, \ldots, x_m) = \sum_{\mu=1}^{m} \omega(x_\mu).$$

Οποιαδήποτε μετάθεση των $x_1, x_2, \ldots, x_m$ αφήνει το $\Pi(x_1, x_2, \ldots, x_m)$ αμετάβλητο. Άρα, το $\Pi(x_1, x_2, \ldots, x_m)$ είναι ένα συμμετρικό πολυώνυμο του $\mathbb{Z}[x_1, x_2, \ldots, x_m]$. Από την παράγραφο 76 προκύπτει ότι,

$$\begin{aligned}\Pi(x_1, x_2, \ldots, x_m) &= \sum_{i_1=0}^{c_1}\sum_{i_2=0}^{c_2}\cdots\sum_{i_m=0}^{c_m}\Big(\gamma_{i_1,i_2,\ldots,i_m}\, e_1^{i_1}(x_1, x_2, \ldots, x_m)\\ &\quad e_2^{i_2}(x_1, x_2, \ldots, x_m)\cdots e_m^{i_m}(x_1, x_2, \ldots, x_m)\Big),\end{aligned}$$

με $\gamma_{i_1,i_2,\ldots,i_m} \in \mathbb{Z}$, $e_k(x_1, x_2, \ldots, x_m)$, $k = 1, 2, \ldots, m$ τα στοιχειώδη συμμετρικά πολυώνυμα του $\mathbb{Z}[x_1, x_2, \ldots, x_m]$. Επειδή, $p \le \tau \le \sigma + p$ έπεται ότι, ο βαθμός $\sigma + p - \tau$ του $\Pi(x_1, x_2, \ldots, x_m)$ είναι μικρότερος ή ίσος του σ. Αν συμβολίσουμε με $deg[\Pi]$ τον βαθμό του $\Pi(x_1, x_2, \ldots, x_m)$ έχουμε, $deg[\Pi] \le \sigma$.

Από την παράγραφο 70 προκύπτει ότι η τιμή του κάθε $e_k(x_1, x_2, \ldots, x_m)$ στις ρίζες $q_1, q_2, \ldots, q_m$ ισούται με $(-1)^k \frac{a_{m-k}}{a_m}$ όπου a_{m-k} οι ακέραιοι συντελεστές του $t(x)$ όπως ορίσθηκαν στην παράγραφο 86. Έτσι, για $p \le \tau \le \sigma + p$ έπεται,

$$\begin{aligned}\sum_{\mu=1}^{m}\omega(q_\mu) &= \Pi(q_1, q_2, \ldots, q_m) =\\ &= \sum_{i_1=0}^{c_1}\sum_{i_2=0}^{c_2}\cdots\sum_{i_m=0}^{c_m}\Big(\gamma_{i_1,i_2,\ldots,i_m}\, e_1^{i_1}(q_1, q_2, \ldots, q_m)\\ &\quad e_2^{i_2}(q_1, q_2, \ldots, q_m)\cdots e_m^{i_m}(q_1, q_2, \ldots, q_m)\Big) =\\ &= \sum_{i_1=0}^{c_1}\sum_{i_2=0}^{c_2}\cdots\sum_{i_m=0}^{c_m}\left(\gamma_{i_1,i_2,\ldots,i_m}\prod_{k=1}^{m}\left((-1)^k\frac{a_{m-k}}{a_m}\right)^{i_k}\right) =\\ &= \frac{1}{a_m^{deg[\Pi]}}A,\end{aligned}$$

όπου $A \in \mathbb{Z}$. Από το τελευταίο αποτέλεσμα και την (42) προκύπτει ότι,

$$\begin{aligned}\sum_{\mu=1}^{m}u^{(\tau)}(q_\mu) &= a_m^\sigma\, p\sum_{\mu=1}^{m}\sum_{\nu=\tau}^{\sigma+p}v_\nu\, q_\mu^{\nu-\tau} \Rightarrow \sum_{\mu=1}^{m}u^{(\tau)}(q_\mu) = a_m^\sigma\, p\sum_{\mu=1}^{m}\omega(q_\mu) \Rightarrow\\ \sum_{\mu=1}^{m}u^{(\tau)}(q_\mu) &= a_m^\sigma\, p\,\frac{1}{a_m^{deg[\Pi]}}A \Rightarrow \sum_{\mu=1}^{m}u^{(\tau)}(q_\mu) = p\, a_m^{\sigma-deg[\Pi]}A = p\, a_m^{\tau-p}A,\end{aligned}$$

όπου, $deg[\Pi] \le \sigma$, p πρώτος, a_m θετικός φυσικός, A ακέραιος. Από το τελευταίο συμπέρασμα και την (41) προκύπτει ότι,

$$\sum_{\mu=1}^{m}U(q_\mu) = \sum_{\tau=p}^{\sigma+p}\sum_{\mu=1}^{m}u^{(\tau)}(q_\mu) = p\,A\sum_{\tau=p}^{\sigma+p}a_m^{\tau-p} = \begin{cases} p\,A\,\frac{a_m^{\sigma+1}-1}{a_m-1} & , \text{ αν } a_m \ne 1,\\ p\,A\,(\sigma+1) & , \text{ αν } a_m = 1.\end{cases}$$

Σε κάθε περίπτωση ο $\sum_{\mu=1}^{m}U(q_\mu)$ είναι ακέραιος διαιρούμενος από τον p.

88. Με τις υποθέσεις και τους συμβολισμούς της παραγράφου 86 θα αποδείξουμε ότι ο $(\delta+1)U(0)$ είναι ακέραιος που δεν διαιρείται από τον p για κατάλληλη επιλογή

του p. Από τον ορισμό του $U(x)$ προκύπτει ότι,

$$\begin{aligned} U(0) &= u(0)+u^{(1)}(0)+u^{(2)}(0)+\cdots+u^{(p-2)}(0)+ \\ &\quad +u^{(p-1)}(0)+ \\ &\quad +u^{(p)}(0)+u^{(p+1)}(0)+\cdots+u^{(\sigma+p)}(0). \end{aligned}$$

Από τον κανόνα παραγώγισης γινομένου του Leibniz προκύπτει ότι,

$$u^{(\tau)}(x)=\frac{a_m^\sigma}{(p-1)!}\sum_{\xi=0}^{\tau}\binom{\tau}{\xi}\left(x^{p-1}\right)^{(\tau-\xi)}\,[t^p(x)]^{(\xi)}. \tag{43}$$

Έστω $0\le c\le p-2$. Θα αποδείξουμε, εφαρμόζοντας επαγωγή στο c ότι,

$$\left(x^{p-1}\right)^{(c)}=\beta\,x^{p-1-c}, \tag{44}$$

με β κάποιο μη μηδενικό φυσικό αριθμό. Για $p=2$ έπεται $c=0$ και το συμπέρασμα ισχύει τετριμμένα για $\beta=1$ επειδή $\left(x^{p-1}\right)^{(0)}=x^{p-1}$.

Για $p\ge 3$, και $c=0$ ισχύει ότι και προηγουμένως. Υποθέτουμε το συμπέρασμα για $c=p-3$ δηλαδή, $\left(x^{p-1}\right)^{(p-3)}=\beta\,x^2$ με β κάποιο μη μηδενικό φυσικό αριθμό. Τότε,

$$\left(x^{p-1}\right)^{(p-2)}=\left(\left(x^{p-1}\right)^{(p-3)}\right)'=(\beta\,x^2)'=2\,\beta\,x,$$

και το συμπέρασμα ισχύει για $\xi=p-2$. Για $0\le\tau\le p-2$ οι (43) και (44) δίνουν,

$$\begin{aligned} u^{(\tau)}(x) &= \frac{a_m^\sigma}{(p-1)!}\sum_{\xi=0}^{\tau}\binom{\tau}{\xi}\left(\beta\,x^{p-1+\xi-\tau}\right)\,[t^p(x)]^{(\xi)}\Rightarrow \\ u^{(\tau)}(0) &= \frac{a_m^\sigma}{(p-1)!}\sum_{\xi=0}^{\tau}\binom{\tau}{\xi}\left(\beta\,0^{p-1+\xi-\tau}\right)\,[t^p(0)]^{(\xi)}=0, \end{aligned} \tag{45}$$

γιατί, $1\le p-1-\tau\le p-1+\xi-\tau\le p-1$ όταν $0\le\tau\le p-2$. Για $\tau=p-1$ από την (43) παίρνουμε,

$$\begin{aligned} u^{(p-1)}(x) &= \frac{a_m^\sigma}{(p-1)!}\sum_{\xi=0}^{p-1}\binom{p-1}{\xi}\left(x^{p-1}\right)^{(p-1-\xi)}\,[t^p(x)]^{(\xi)}\Rightarrow \\ u^{(p-1)}(x) &= \frac{a_m^\sigma}{(p-1)!}\left[\left(x^{p-1}\right)^{(p-1)}\,t^p(x)+\right. \\ &\quad \left.+\sum_{\xi=1}^{p-1}\binom{p-1}{\xi}\left(x^{p-1}\right)^{(p-1-\xi)}\,[t^p(x)]^{(\xi)}\right]\overset{\xi=\gamma+1}{=\!=\!\Rightarrow} \\ u^{(p-1)}(x) &= \frac{a_m^\sigma}{(p-1)!}\left[(p-1)!\,t^p(x)+\right. \\ &\quad \left.+\sum_{\gamma=0}^{p-2}\binom{p-1}{\gamma+1}\left(x^{p-1}\right)^{(p-2-\gamma)}\,[t^p(x)]^{(\gamma+1)}\right]\overset{(44)}{\Rightarrow} \end{aligned}$$

$$\begin{aligned} u^{(p-1)}(x) &= \frac{a_m^\sigma}{(p-1)!}\left[(p-1)!\,t^p(x) + \right. \\ &\quad \left. + \sum_{\gamma=0}^{p-2}\binom{p-1}{\gamma+1}\left(\beta\, x^{\gamma+1}\right)\,\left[t^p(x)\right]^{(\gamma+1)}\right] \Rightarrow \\ u^{(p-1)}(0) &= \frac{a_m^\sigma}{(p-1)!}\left[(p-1)!\,t^p(0) + \right. \\ &\quad \left. + \sum_{\gamma=0}^{p-2}\binom{p-1}{\gamma+1}\left(\beta\, 0^{\gamma+1}\right)\,\left[t^p(0)\right]^{(\gamma+1)}\right] \Rightarrow \\ u^{(p-1)}(0) &= a_m^\sigma\, t^p(0) = a_m^\sigma\, a_0^p, \end{aligned} \tag{46}$$

επειδή $t(0) = a_0$ από τον ορισμό του $t(x)$ στην παράγραφο 86. Για $p \le \tau \le \sigma + p$, στην (42) δείξαμε ότι, $u^{(\tau)}(x) = a_m^\sigma\, p\, \omega(x)$ με $\omega(x) \in \mathbb{Z}[x]$. Οπότε,

$$u^{(\tau)}(0) = a_m^\sigma\, p\, \omega(0), \tag{47}$$

με $\omega(0) \in \mathbb{Z}$. Οι (45), (46), (47) δίνουν,

$$\begin{aligned} (\delta+1)\,U(0) &= (\delta+1)\,\left[\left(\sum_{\tau=0}^{p-2} 0\right) + a_m^\sigma\, a_0^p + \left(\sum_{\tau=p}^{\sigma+p} a_m^\sigma\, p\,\omega(0)\right)\right] = \\ &= (\delta+1)\,a_m^\sigma\, a_0^p + (\delta+1)\,a_m^\sigma\, p\, v_\tau. \end{aligned}$$

Αν επιλέξουμε τον πρώτο p να είναι μεγαλύτερος από τους $(\delta+1)$, a_m, a_0 τότε, ο p δεν διαιρεί το γινόμενο $(\delta+1)\,U(0)$ και το συμπέρασμα απεδείχθη.

89. Με τις υποθέσεις και τους συμβολισμούς της παραγράφου 86 θα αποδείξουμε ότι για κατάλληλη επιλογή του πρώτου p το δεξί μέλος της (40) γίνεται μικρότερο από την απόλυτη τιμή οιουδήποτε μη μηδενικού ακέραιου.

$$\begin{aligned} &\left|-\sum_{\mu=1}^{m}\int_0^1 q_\mu\, e^{q_\mu\,(1-w)}\, u(q_\mu\, w)\, dw\right| = \\ &= \left|\int_0^1 \sum_{\mu=1}^{m} q_\mu\, e^{q_\mu\,(1-w)}\,\frac{a_m^\sigma\,(q_\mu\, w)^{p-1}\,[t(q_\mu\, w)]^p}{(p-1)!}\, dw\right| \le \\ &\le \int_0^1 \sum_{\mu=1}^{m}\left|\frac{[a_m^m\,(q_\mu\, w)\, t(q_\mu\, w)]^{p-1}}{(p-1)!}\, q_\mu\, e^{q_\mu\,(1-w)}\, a_m^{m-1}\, t(q_\mu\, w)\right| dw, \end{aligned} \tag{48}$$

όπου χρησιμοποιήσαμε τον ορισμό του σ από την παράγραφο 86 και τις ισότητες,

$$a_m^\sigma = a_m^{m\,p-1} = a_m^{m\,p-m+m-1} = (a_m^m)^{p-1}\, a_m^{m-1}.$$

Η συνάρτηση $T_\mu : \mathbb{C} \to \mathbb{C}$ με τύπο $T_\mu(w) = |a_m^m\,(q_\mu\, w)\, t(q_\mu\, w)|$ είναι συνεχής άρα και φραγμένη στο διάστημα $[0,1]$. Έστω B_μ θετικός πραγματικός, το ελάχιστο ανάμεσα στα φράγματα της T_μ. Θέτουμε $B = \max\limits_{\mu=1,2,\ldots,m}\{B_\mu\}$. Έπεται ότι,

$$|a_m^m\,(q_\mu\, w)\, t(q_\mu\, w)| \le B, \text{ για κάθε } \mu = 1, 2, \ldots, m. \tag{49}$$

Η συνάρτηση $K : \mathbb{C} \to \mathbb{C}$ με τύπο $K(w) = \sum_{\mu=1}^{m} |q_\mu \, e^{q_\mu \, (1-w)} \, a_m^{m-1} \, t(q_\mu \, w)|$ είναι συνεχής άρα και φραγμένη στο διάστημα $[0, 1]$. Έστω Y θετικός πραγματικός ώστε,

$$\sum_{\mu=1}^{m} |q_\mu \, e^{q_\mu \, (1-w)} \, a_m^{m-1} \, t(q_\mu \, w)| \leq Y. \tag{50}$$

Από τις (48), (49), (50) προκύπτει ότι,

$$\left| -\sum_{\mu=1}^{m} \int_0^1 q_\mu \, e^{q_\mu \, (1-w)} \, u(q_\mu \, w) \, dw \right| \leq Y \, \frac{B^{p-1}}{(p-1)!} \, . \tag{51}$$

Όμως, από την Πραγματική Ανάλυση γνωρίζουμε ότι, $Y \, e^B = \sum_{k=0}^{+\infty} Y \, \frac{B^k}{k!}$. Αν θεωρήσουμε την ακολουθία πραγματικών αριθμών $S_n = \sum_{k=0}^{n} Y \, \frac{B^k}{k!}$ προκύπτουν τα,

$$\begin{aligned} \lim_{n \to +\infty} S_n &= Y \, e^B, \\ Y \, \frac{B^{n-1}}{(n-1)!} &= S_{n-1} - S_{n-2}, \\ \lim_{n \to +\infty} Y \, \frac{B^{n-1}}{(n-1)!} &= \lim_{n \to +\infty} (S_{n-1} - S_{n-2}) = Y \, e^B - Y \, e^B = 0. \end{aligned}$$

Άρα, για κάθε $\varepsilon > 0$, υπάρχει $n_0 \in \mathbb{N}$ ώστε για κάθε $n > n_0$ να έπεται $\left| Y \, \frac{B^{n-1}}{(n-1)!} \right| < \varepsilon$. Για $\varepsilon = 1/2$ προκύπτει ότι υπάρχει $n_0 \in \mathbb{N}$ ώστε για κάθε $n > n_0$ να έπεται $\left| Y \, \frac{B^{n-1}}{(n-1)!} \right| < \frac{1}{2}$. Επιλέγουμε τον πρώτο p να είναι μεγαλύτερος από τον n_0. Τότε, $\left| Y \, \frac{B^{p-1}}{(p-1)!} \right| < \frac{1}{2}$. Από την (51) ο $Y \, \frac{B^{p-1}}{(p-1)!}$ είναι θετικός οπότε, $0 \leq Y \, \frac{B^{p-1}}{(p-1)!} < \frac{1}{2}$. Αποδείξαμε ότι υπάρχει κατάλληλος πρώτος p ώστε,

$$\left| -\sum_{\mu=1}^{m} \int_0^1 q_\mu \, e^{q_\mu \, (1-w)} \, u(q_\mu \, w) \, dw \right| \leq Y \, \frac{B^{p-1}}{(p-1)!} < \frac{1}{2} \, . \tag{52}$$

Από την (52) προκύπτει ότι υπάρχει κατάλληλη επιλογή του πρώτου p ώστε το δεξί μέλος της (40) να γίνεται μικρότερο από την απόλυτη τιμή οιουδήποτε μη μηδενικού ακέραιου.

90. Στην παράγραφο 86 υποθέσαμε ότι υπάρχει πολυώνυμο με ακέραιους συντελεστές που έχει τον π ως ρίζα του. Οδηγηθήκαμε έτσι στην ισχύ της ισότητας (40). Όμως, όπως αποδείξαμε στις παραγράφους 87, 88, το αριστερό μέλος της (40) είναι άθροισμα ενός ακέραιου που διαιρείται με τον p και ενός ακέραιου που δεν διαιρείται με το p. Άρα, το άθροισμα των δύο αυτών ακέραιων δεν διαιρείται με το p. Αυτό σημαίνει ότι το αριστερό μέλος της (40) είναι ένας μη μηδενικός ακέραιος διότι, αν ήταν μηδέν ο p θα το διαιρούσε.

Στην παράγραφο 89 αποδείξαμε ότι το δεξί μέλος της (40) είναι αριθμός μεταξύ του $-1/2$ και του $1/2$. Άρα, αν είναι ακέραιος είναι ο 0. Αυτό οδηγεί στην αντίφαση ότι ένας μη μηδενικός ακέραιος ισούται με το 0. Αν το δεξί μέλος της (40) δεν είναι ακέραιος οδηγούμαστε στην αντίφαση ότι ένας ακέραιος ισούται

με έναν πραγματικό μεταξύ του $-1/2$ και του $1/2$. Άρα, η υπόθεση ότι υπάρχει πολυώνυμο με ακέραιους συντελεστές που έχει τον π ως ρίζα του είναι εσφαλμένη και το συμπέρασμα της παραγράφου 66 απεδείχθη.

91. Οι επόμενες παράγραφοι αναφέρονται στην απόδειξη της ικανής και αναγκαίας συνθήκης που πρέπει να ικανοποιεί ένας φυσικός αριθμός n ώστε κανονικό πολύγωνο με n το πλήθος πλευρές να κατασκευάζεται με κανόνα και διαβήτη.

92. Έστω R υποδακτύλιος του $\mathbb{C}$. Στην παράγραφο 53 ανεφέρθη για πρώτη φορά η έννοια του ανάγωγου πολυωνύμου επί ενός δακτυλίου πολυωνύμων δηλαδή, αν $f(x) \in R[x]$ το $f(x)$ είναι ανάγωγο επί του $R[x]$ αν δεν υπάρχουν πολυώνυμα $g(x), h(x) \in R[x]$ με $1 \leq deg[g(x)], deg[h(x)] < deg[f(x)]$ και $f(x) = g(x)\, h(x)$, για κάθε $x \in \mathbb{C}$. Θα αποδείξουμε ότι το $f(x) \in R[x]$ είναι ανάγωγο επί του $R[x]$ αν και μόνο αν το $f(x+1)$ είναι ανάγωγο επί του $R[x]$.

Έστω ότι το $f(x) \in R[x]$ είναι είναι ανάγωγο επί του $R[x]$ ενώ το $f(x+1)$ δεν είναι ανάγωγο επί του $R[x]$. Τότε, υπάρχουν πολυώνυμα $g(x), h(x) \in R[x]$ με $1 \leq deg[g(x)], deg[h(x)] < deg[f(x+1)]$ και $f(x+1) = g(x)\, h(x)$, για κάθε $x \in \mathbb{C}$. Σημειώνουμε ότι $deg[f(x)] = deg[f(x+1)]$, $deg[g(x)] = deg[g(x-1)]$, $deg[h(x)] = deg[h(x-1)]$. Για $x = u - 1$ παίρνουμε $f(u) = g(u-1)\, h(u-1)$ ή ισοδυνάμως $f(x) = g(x-1)\, h(x-1)$, με $g(x-1), h(x-1) \in R[x]$, $1 \leq deg[g(x-1)], deg[h(x-1)] < deg[f(x)]$ που αντιβαίνει την υπόθεση ότι το $f(x)$ είναι ανάγωγο επί του $R[x]$.

Έστω ότι το το $f(x+1)$ είναι ανάγωγο επί του $R[x]$ ενώ το $f(x)$ δεν είναι. Τότε, υπάρχουν πολυώνυμα $g(x), h(x) \in R[x]$ με $1 \leq deg[g(x)], deg[h(x)] < deg[f(x)]$ και $f(x) = g(x)\, h(x)$, για κάθε $x \in \mathbb{C}$. Σημειώνουμε ότι $deg[f(x)] = deg[f(x+1)]$, $deg[g(x)] = deg[g(x+1)]$, $deg[h(x)] = deg[h(x+1)]$. Για $x = u+1$ παίρνουμε $f(u+1) = g(u+1)\, h(u+1)$ ή ισοδυνάμως $f(x+1) = g(x+1)\, h(x+1)$, με $g(x+1), h(x+1) \in R[x]$, $1 \leq deg[g(x+1)], deg[h(x+1)] < deg[f(x+1)]$ που αντιβαίνει την υπόθεση ότι το $f(x+1)$ είναι ανάγωγο επί του $R[x]$. Το συμπέρασμα απεδείχθη.

93. Έστω p ένας πρώτος αριθμός. Θα αποδείξουμε ότι ο p διαιρεί τον $\binom{p}{k}$ για κάθε $k = 1, 2, \ldots, p-1$. Από την παράγραφο 78 γνωρίζουμε ότι ο $\binom{p}{k}$ είναι φυσικός αριθμός. Μπορούμε να γράψουμε,

$$\binom{p}{k} = \frac{p\,(p-1)!}{k!\,(p-k)!} \Rightarrow (k!\,(p-k)!)\binom{p}{k} = p\,(p-1)!. \tag{53}$$

Επειδή $k = 1, 2, \ldots, p-1$ έπεται ότι $k < p$ και $p - k < p$. Στα γινόμενα $k!$, $(p-k)!$ κάθε παράγοντας είναι μικρότερος του p άρα σχετικώς πρώτος με τον p. Ο p διαιρώντας το γινόμενο (53) διαιρεί υποχρεωτικά τον $\binom{p}{k}$.

94. Έστω $f(x) \in \mathbb{Z}[x]$ με συντελεστές πρώτους μεταξύ τους ώστε $f(x) = g(x)\, h(x)$ με $g(x), h(x) \in \mathbb{Q}[x]$. Θα αποδείξουμε ότι υπάρχουν $k(x), \ell(x) \in \mathbb{Z}[x]$ ώστε $f(x) = k(x)\, \ell(x)$.

Έστω $g(x) = \sum_{i=0}^{n} \frac{a_{i1}}{a_{i2}}\, x^i$, $h(x) = \sum_{j=0}^{m} \frac{b_{j1}}{b_{j2}}\, x^j$ με $a_{i1}, b_{j1} \in \mathbb{Z}$, a_{n1}, b_{m1}, a_{i2}, $b_{j2} \in \mathbb{Z} - \{0\}$. Επίσης θέτουμε, $a = \prod_{i=0}^{n} a_{i2}$, $b = \prod_{j=0}^{m} b_{j2}$. Σημειώνουμε ότι $a\, \frac{a_{i1}}{a_{i2}} \in \mathbb{Z}$, $b\, \frac{b_{j1}}{b_{j2}} \in \mathbb{Z}$. Αν GCD συμβολίζει τον μέγιστο κοινό διαιρέτη κάποιων

ακέραιων θέτουμε,

$$\begin{aligned} d_a &= GCD\left(\frac{a\,a_{01}}{a_{02}}, \frac{a\,a_{11}}{a_{12}}, \ldots, \frac{a\,a_{n1}}{a_{n2}}\right), \\ d_b &= GCD\left(\frac{b\,b_{01}}{b_{02}}, \frac{b\,b_{11}}{b_{12}}, \ldots, \frac{b\,b_{n1}}{b_{n2}}\right). \end{aligned}$$

Θέτουμε $k(x) = \frac{a\,g(x)}{d_a} \in \mathbb{Z}[x]$, $\ell(x) = \frac{b\,h(x)}{d_b} \in \mathbb{Z}[x]$. Τα $k(x), \ell(x)$ από την κατασκευή τους έχουν συντελεστές πρώτους μεταξύ τους. Επίσης ισχύει,

$$(a\,b)\,f(x) = (d_a\,d_b)\left(\frac{a\,g(x)}{d_a}\right)\left(\frac{b\,h(x)}{d_b}\right) \in \mathbb{Z}[x].$$

Ο $(d_a\,d_b)$ διαιρεί τους συντελεστές του $(a\,b)\,f(x)$. Αφού οι συντελεστές του $f(x)$ είναι πρώτοι μεταξύ τους προκύπτει ότι ο $(d_a\,d_b)$ διαιρεί τον $(a\,b)$. Έστω $q = (a\,b)/(d_a\,d_b) \in \mathbb{Z}$. Αν $q \neq \pm 1$ τότε υπάρχει πρώτος p που διαιρεί τον q και,

$$q\,f(x) = \left(\frac{a\,g(x)}{d_a}\right)\left(\frac{b\,h(x)}{d_b}\right) = \sum_{i=0}^{n} A_i\,x^i \sum_{j=0}^{m} B_j\,x^j = k(x)\,\ell(x). \tag{54}$$

Ο p δεν διαιρεί όλα τα A_i γιατί αυτά, (από την κατασκευή τους), είναι πρώτοι μεταξύ τους. Έστω $i_0 \geq 0$ ο μικρότερος δείκτης ώστε ο p να μην διαιρεί τον A_{i_0}.

Ομοίως, ο p δεν διαιρεί όλα τα B_j γιατί αυτά, (από την κατασκευή τους), είναι πρώτοι μεταξύ τους. Έστω $j_0 \geq 0$ ο μικρότερος δείκτης ώστε ο p να μην διαιρεί τον B_{i_0}. Ο συντελεστής του $x^{i_0+j_0}$ στο $q\,f(x)$ της (54) διαιρείται με τον p, (γιατί είναι πολλαπλάσιο του q). Ο συντελεστής του $x^{i_0+j_0}$ στο δεξί μέλος της (54) ισούται με,

$$\left(\sum_{r=0}^{i_0-1} A_r\,B_{i_0+j_0-r}\right) + A_{i_0}\,B_{j_0} + \left(\sum_{r=i_0+1}^{i_0+j_0} A_r\,B_{i_0+j_0-r}\right). \tag{55}$$

Από την επιλογή των i_0, j_0 προκύπτει ότι, ο p διαιρεί τους A_r για $r = 0, 1, \ldots, i_0 - 1$ και τους $B_{i_0+j_0-r}$ για $r = i_0+1, i_0+2, \ldots, i_0+j_0$ ενώ δεν διαιρεί το $A_{i_0}\,B_{j_0}$. Όμως ο συντελεστής του $x^{i_0+j_0}$ στο δεξί μέλος της (54) ισούται με τον συντελεστή του $x^{i_0+j_0}$ στο $q\,f(x)$ ο οποίος δείξαμε ότι διαιρείται με τον p. Άρα, ο αριθμός στην (55) διαιρείται με το p και επειδή οι δύο από τους τρεις προσθεταίους του διαιρούνται με το p και ο τρίτος $A_{i_0}\,B_{j_0}$ διαιρείται με το p άτοπο. Άρα, $q = \pm 1$ και το συμπέρασμα απεδείχθη.

Το συμπέρασμα που αποδείξαμε στην παρούσα παράγραφο είναι γνωστό ως λήμμα του Gauss.

95. Έστω $f(x) \in \mathbb{Z}[x]$ τέτοιο ώστε $f(x) = g(x)\,h(x)$ με $g(x), h(x) \in \mathbb{Q}[x]$. Αν d είναι ο μέγιστος κοινός διαιρέτης των συντελεστών του μπορούμε να γράψουμε $f(x) = d\,u(x)$. Οπότε, από την παράγραφο 94 προκύπτει ότι, $u(x) = (1/d)\,f(x) = ((1/d)\,g(x))\,h(x) = k(x)\,\ell(x)$ με $k(x), \ell(x) \in \mathbb{Z}[x]$ γιατί οι συντελεστές του $u(x)$ είναι πρώτοι μεταξύ τους. Άρα, $f(x) = (d\,k(x))\,\ell(x)$ με $s(x) = (d\,k(x)), \ell(x) \in \mathbb{Z}[x]$ και το συμπέρασμα της παραγράφου 94 ισχύει και όταν οι συντελεστές του $f(x)$ δεν είναι πρώτοι μεταξύ τους.

96. Έστω $f(x) = \sum_{i=0}^{n} a_i\,x^i \in \mathbb{Z}[x]$. Αν υπάρχει πρώτος αριθμός p ώστε,

- ο p να διαιρεί τους $a_0, a_1, \ldots, a_{n-1}$,
- ο p δεν διαιρεί τον a_n,
- ο p^2 δεν διαιρεί τον a_0,

θα αποδείξουμε ότι το $f(x)$ είναι ανάγωγο επί του $\mathbb{Q}[x]$. Το συμπέρασμα αυτό είναι γνωστό ως κριτήριο αναγωγιμότητας του Eisenstein.

Έστω ότι το $f(x)$ δεν είναι ανάγωγο επί του $\mathbb{Q}[x]$. Τότε υπάρχουν $g(x), h(x) \in \mathbb{Q}[x]$ ώστε, $f(x) = g(x)\,h(x)$. Από την παράγραφο 95 προκύπτει ότι $f(x) = s(x)\,\ell(x)$ για κάποια $s(x), \ell(x) \in \mathbb{Z}[x]$. Έστω $s(x) = \sum_{i=0}^{\nu} b_i\,x^i$, $\ell(x) = \sum_{j=0}^{m} c_j\,x^j$. Τότε, $a_n = b_\nu\,c_m$ και επειδή ο p δεν διαιρεί τον a_n έπεται ότι δεν διαιρεί και τους b_ν, c_m. $a_0 = b_0\,c_0$. Αν ο p διαιρεί τον b_0 και τον c_0 τότε ο p^2 διαιρεί τον a_0 άτοπο. Άρα, επειδή ο p διαιρεί τον a_0 έπεται ότι διαιρεί μόνο έναν από τους b_0, c_0. Έστω χωρίς βλάβη της γενικότητας ότι ο p διαιρεί μόνο τον b_0. Επειδή ο p δεν διαιρεί τον b_ν έπεται ότι υπάρχει $1 \leq j_0 \leq \nu$, j_0 ο μικρότερος δυνατός δείκτης ώστε ο p δεν διαιρεί τον b_{j_0}. Από την ισότητα $f(x) = s(x)\,\ell(x)$ παίρνουμε,

$$\begin{aligned}\sum_{i=0}^{n} a_i\,x^i &= \sum_{i=0}^{\nu} b_i\,x^i \sum_{j=0}^{m} c_j\,x^j = \sum_{i=0}^{\nu+m}\left(\sum_{r=0}^{i} b_r\,c_{i-r}\right)x^i \Rightarrow \\ a_{j_0} &= \sum_{r=0}^{j_0} b_r\,c_{j_0-r} = \left(\sum_{r=0}^{j_0-1} b_r\,c_{j_0-r}\right) + b_{j_0}\,c_0. \qquad (56)\end{aligned}$$

Επειδή $1 \leq j_0 \leq \nu < n$ έπεται ότι ο p διαιρεί τον a_{j_0} άρα και τον αριθμό στο δεξί μέλος της (56). Επίσης, από την επιλογή του j_0 προκύπτει ότι ο p διαιρεί τους b_r για κάθε $r = 0, 1, \ldots, j_0 - 1$ άρα και τον πρώτο προσθεταίο στο δεξί μέλος της (56). Ο p διαιρεί το άθροισμα και τον ένα από τους δύο προσθεταίους του δευτέρου μέλους της (56). Αυτό σημαίνει ότι ο p διαιρεί και τον προσθεταίο $b_{j_0}\,c_0$ άτοπο. Άρα, το $f(x)$ είναι ανάγωγο επί του $\mathbb{Q}[x]$ και κατ΄ επέκταση και επί του $\mathbb{Z}[x]$ αφού $\mathbb{Z}[x] \subset \mathbb{Q}[x]$.

97. Έστω p πρώτος αριθμός. Θα αποδείξουμε ότι το πολυώνυμο $f(x) = \sum_{k=0}^{p-1} x^k$ είναι ανάγωγο επί του $\mathbb{Q}[x]$.

Μπορούμε να γράψουμε $f(x) = \frac{x^p-1}{x-1}$. Από την παράγραφο 92 προκύπτει ότι αρκεί να αποδείξουμε ότι το πολυώνυμο $f(x+1)$ είναι ανάγωγο επί του $\mathbb{Q}[x]$.

$$\begin{aligned}f(x+1) &= \frac{(x+1)^p - 1}{x} = \frac{1}{x}\sum_{i=0}^{p-1}\binom{p}{i}x^{p-i} = \sum_{i=0}^{p-1}\binom{p}{i}x^{p-i-1} = \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \ldots + \binom{p}{p-2}x + \binom{p}{p-1}. \qquad (57)\end{aligned}$$

Από την παράγραφο 93 προκύπτει ότι, ο p διαιρεί τους συντελεστές $\binom{p}{i}$ για $i = 1, 2, \ldots, p-1$ ενώ, δεν διαιρεί τον συντελεστή του μεγιστοβάθμιου όρου του πολυωνύμου $f(x+1)$ στην (57). Επίσης, ο σταθερός όρος του $f(x+1)$ στην (57), ο $\binom{p}{p-1} = p$ και δεν διαιρείται με τον p^2. Για το $f(x+1)$ ισχύουν οι προϋποθέσεις της παραγράφου 96. Άρα, το $f(x+1)$ και κατ΄ επέκταση και το $f(x)$ είναι ανάγωγα επί του $\mathbb{Q}[x]$.

98. Είναι γνωστό από την Μιγαδική Ανάλυση ότι οι διακεκριμένοι μιγαδικοί αριθμοί $\zeta_k = e^{2\,k\,\pi\,i/n}$ για $k = 0, 1, \ldots, n-1$ είναι οι n το πλήθος n-οστές ρίζες της μονάδας. Θα λέμε ότι ο μιγαδικός αριθμός ζ_k, $k = 0, 1, \ldots, n-1$ είναι μία πρωταρχική n-οστή ρίζα της μονάδας αν, $\zeta_k^n = 1$ ενώ $\zeta_k^m \neq 1$ για κάθε $m = 1, 2, \ldots, n-1$.

Παράδειγμα πρωταρχικής n-οστής ρίζας της μονάδας είναι ο $\zeta_1 = e^{2\,\pi\,i/n} =$ συν$\frac{2\,\pi}{n} + i$ ημ$\frac{2\,\pi}{n}$. Παρατηρούμε ότι κάθε n-οστή ρίζα της μονάδας μπορεί να γραφεί ως $\zeta_k = \zeta_1^k$, $k = 0, 1, \ldots, n-1$. Δηλαδή, η πρωταρχική n-οστή ρίζα της μονάδας ζ_1 παράγει πολλαπλασιαστικά όλες τις n-οστές ρίζες της μονάδας. Θα αποδείξουμε πως αυτό συμβαίνει με όλες τις πρωταρχικές n-οστές ρίζες της μονάδας.

Έστω ζ_t μία πρωταρχική n-οστή ρίζα της μονάδας. ζ_t^μ με $\mu = 0, 1, \ldots, n-1$ είναι n-οστές ρίζες τις μονάδας γιατί $(\zeta_t^\mu)^n = (\zeta_t^n)^\mu = 1^\mu = 1$ ενώ αν $\zeta_t^a = \zeta_t^b$ για $a, b = 1, 2, \ldots, n-1$, $a > b$ τότε, $\zeta_t^{a-b} = 1$ για $a - b < n$ αντιβαίνοντας στην ιδιότητα της ζ_t ως πρωταρχικής n-οστής ρίζας της μονάδας. Άρα, οι ζ_t^μ με $\mu = 0, 1, \ldots, n-1$ είναι n το πλήθος διακεκριμένες n-οστές ρίζες τις μονάδας. Αλλά και οι ζ_k με $k = 0, 1, \ldots, n-1$ είναι n το πλήθος διακεκριμένες n-οστές ρίζες τις μονάδας. Αυτό σημαίνει ότι τα σύνολα $\{\zeta_k \,:\, k = 0, 1, \ldots, n-1\}$ και $\{\zeta_t^\mu \,:\, \mu = 0, 1, \ldots, n-1\}$ είναι ίσα. Άρα, για κάθε ζ_k υπάρχει $\mu = 0, 1, \ldots, n-1$ ώστε $\zeta_k = \zeta_t^\mu$ και το συμπέρασμα απεδείχθη.

Επίσης, θα αποδείξουμε ότι αν ζ_t είναι μία πρωταρχική n-οστή ρίζα της μονάδας τότε, η ζ_t^μ, $\mu \in \mathbb{N} - \{0\}$ είναι και αυτή μία πρωταρχική n-οστή ρίζα της μονάδας αν και μόνο αν οι n, μ είναι πρώτοι μεταξύ τους.

Έστω ότι η ζ_t^μ είναι και αυτή μία n-οστή πρωταρχική ρίζα της μονάδας. Αν οι n και μ έχουν κοινό πρώτο διαιρέτη p τότε, οι n/p και μ/p είναι φυσικοί και $(\zeta_t^\mu)^{n/p} = (\zeta_t^n)^{\mu/p} = 1^{\mu/p} = 1$. Δηλαδή, για την ζ_t^μ ισχύει $(\zeta_t^\mu)^{n/p} = 1$ για τον φυσικό $n/p < n$ αντιβαίνοντας στην ιδιότητα της ζ_t^μ ως n-οστής πρωταρχικής ρίζας της μονάδας. Άρα, οι n και μ είναι πρώτοι μεταξύ τους.

Έστω ότι οι n και μ είναι πρώτοι μεταξύ τους. Προφανώς $(\zeta_t^\mu)^n = (\zeta_t^n)^\mu = 1^\mu = 1$ και η ζ_t^μ είναι μία n-οστή ρίζα της μονάδας. Αν υπάρχει $1 \leq r < n$ ώστε $(\zeta_t^\mu)^r = 1$ τότε, $\zeta_t^{\mu\,r} = 1$ και επειδή η ζ_t είναι μία πρωταρχική n-οστή ρίζα της μονάδας δεν μπορεί $\mu\,r < n$. Άρα, $\mu\,r \geq n$ και η Ευκλείδεια διαίρεσή τους δίνει $\mu\,r = n\,b + \upsilon$ με $0 \leq \upsilon < n$. Αν $\upsilon \neq 0$ τότε, $1 = \zeta_t^{\mu\,r} = (\zeta_t^n)^b\,\zeta_t^\upsilon = \zeta_t^\upsilon$ αντιβαίνοντας την ιδιότητα της ζ_t ως πρωταρχικής n-οστής ρίζας της μονάδας. Άρα, $\upsilon = 0$ και $\mu\,r = n\,b$ με $1 \leq r < n$. Όμως τα n, μ είναι πρώτοι μεταξύ τους άρα ο n πρέπει να διαιρεί τον r άτοπο γιατί αυτός είναι μικρότερος του n και το συμπέρασμα απεδείχθη.

Έστω $\phi : \mathbb{N} - \{0\} \mapsto \mathbb{N} - \{0\}$ με $\phi(n) =$ το πλήθος των μη μηδενικών φυσικών μικρότερων ή και ίσων του n που είναι σχετικώς πρώτοι με το n. Η συνάρτηση αυτή είναι γνωστή ως η ϕ συνάρτηση του Euler. Θα αποδείξουμε ότι το πλήθος των πρωταρχικών n-οστών ριζών της μονάδας είναι $\phi(n)$.

Έχουμε ήδη αποδείξει ότι κάθε n-οστή ρίζα της μονάδας γράφεται στη μορφή ζ_1^k με $k = 0, 1, \ldots, n-1$. Όλες οι πρωταρχικές n-οστές ρίζες της μονάδας περιλαμβάνονται στο σύνολο $\{\zeta_1^0, \zeta_1^1, \ldots, \zeta_1^{n-1}\}$ των n-οστών ριζών της μονάδας, (ως n-οστές ρίζες που είναι και αυτές). Άρα, και αυτές γράφονται στην μορφή ζ_1^k για κάποιο $k \in \{1, 2, \ldots, n-1\}$. Επειδή, η ζ_1 είναι πρωταρχική n-οστή ρίζα της μονάδας, από τα πιο πάνω προκύπτει πως οι μόνες δυνάμεις της μορφής ζ_1^k για κάποιο $k \in \{1, 2, \ldots, n-1\}$ που μπορεί να αντιστοιχούν σε πρωταρχικές n-οστές

ρίζες της μονάδας είναι αυτές που το k είναι σχετικώς πρώτο με τον n. Αυτές είναι $\phi(n)$ το πλήθος και το συμπέρασμα απεδείχθη.

99. Έστω p πρώτος αριθμός. Θα αποδείξουμε ότι $\phi(p) = p-1$ και $\phi(p^2) = p\,(p-1)$.

Το πρώτο συμπέρασμα προκύπτει από το γεγονός ότι, κάθε $k \in \{1, 2, \ldots, p-1\}$ είναι σχετικώς πρώτο με το p. Για το δεύτερο συμπέρασμα γράφουμε τους μη μηδενικούς φυσικούς μικρότερους ή ίσους του p^2,

$$1, 2, \ldots, p, (p+1), \ldots, 2\,p, (2\,p+1), \ldots, (p-1)\,p, (p-1)\,p+1, \ldots, p^2. \quad (58)$$

Είναι άμεσο να ελέγξουμε ότι από αυτούς εκείνοι που έχουν κοινό διαιρέτη με το p^2 διάφορο του 1 είναι οι,

$$p,\ 2\,p\,,3\,p,\ \ldots,\ (p-1)\,p,\ p^2,$$

οι οποίοι είναι p το πλήθος. Οι υπόλοιποι αριθμοί της (58) είναι σχετικώς πρώτοι με τον p^2 και το πλήθος τους είναι $\phi(p^2) = p^2 - p = p\,(p-1)$.

100. Έστω p πρώτος αριθμός. Θα αποδείξουμε ότι το πολυώνυμο $f(x) = \sum_{\ell=1}^{p} x^{[p\,(p-\ell)]}$ είναι ανάγωγο επί του $\mathbb{Q}[x]$.

Από την παράγραφο 92 προκύπτει ότι αρκεί να αποδείξουμε ότι το πολυώνυμο $f(x+1)$ είναι ανάγωγο επί του $\mathbb{Q}[x]$. Από την παράγραφο 93 προκύπτει ότι ο p διαιρεί τους φυσικούς αριθμούς $\binom{p}{k}$ για κάθε $k = 1, 2, \ldots, p-1$. Συμβολίζουμε με q_k το πηλίκο της διαίρεσης αυτής. Επίσης γράφουμε,

$$\begin{aligned}
f(x+1) &= \sum_{\ell=1}^{p}[(x+1)^p]^{(p-\ell)} = \sum_{\ell=1}^{p}\left[\sum_{k=0}^{p}\binom{p}{k}x^{p-k}\right]^{p-\ell} = \\
&= \sum_{\ell=1}^{p}\left[(x^p+1) + p\sum_{k=1}^{p-1} q_k x^{p-k}\right]^{p-\ell} = \sum_{\ell=1}^{p}\left[(x^p+1) + p\,g(x)\right]^{p-\ell} = \\
&= \sum_{\ell=1}^{p}\left[\sum_{t=0}^{p-\ell}\binom{p-\ell}{t}(x^p+1)^{(p-\ell)-t}\,p^t\,g^t(x)\right] = \\
&= \sum_{\ell=1}^{p}\left[(x^p+1)^{(p-\ell)} + p\sum_{t=1}^{p-\ell}\binom{p-\ell}{t}(x^p+1)^{(p-\ell)-t}\,p^{t-1}\,g^t(x)\right] = \\
&= \sum_{\ell=1}^{p}\left[(x^p+1)^{(p-\ell)} + p\,h_\ell(x)\right] =, \quad (\text{με } deg[h_\ell(x)] = p^2 - \ell\,p - 1) \\
&= \sum_{\ell=1}^{p}(x^p+1)^{(p-\ell)} + p\sum_{\ell=1}^{p}h_\ell(x) = \frac{(x^p+1)^p - 1}{x^p} + p\,H(x) =, \\
&\quad (\text{με } deg[H(x)] = p^2 - p - 1) \\
&= \left[\frac{-1}{x^p} + \sum_{i=0}^{p}\binom{p}{i}x^{p\,(p-i-1)}\right] + p\,H(x) = \\
&= \left[x^{p\,(p-1)} + \sum_{i=1}^{p-1}\binom{p}{i}x^{p\,(p-i-1)}\right] + p\,H(x) = \\
&= x^{p\,(p-1)} + p\,G(x),
\end{aligned}$$

όπου $G(x)$ πολυώνυμο του $\mathbb{Z}[x]$ βαθμού p^2-p-1. Παρατηρούμε ότι, ο συντελεστής του μεγιστοβάθμιου όρου του $f(x+1)$ είναι 1 και δεν διαιρείται με τον p. Οι συντελεστές των υπόλοιπων όρων του $f(x+1)$ διαιρούνται με τον p. Ο σταθερός όρος του $f(x+1)$ είναι ο $f(1)=p$ και δεν διαιρείται με τον p^2. Από την παράγραφο 96 προκύπτει ότι το $f(x+1)$ είναι ανάγωγο επί του $\mathbb{Q}[x]$ και το συμπέρασμα απεδείχθη.

101. Έστω p πρώτος αριθμός. Θα αποδείξουμε ότι ένα ελαχίστου βαθμού πολυώνυμο του $\mathbb{Q}[x]$ που έχει ως ρίζες του τις μιγαδικές p-οστές ρίζες της μονάδας είναι το $f(x)=\sum_{k=0}^{p-1}x^k$. Επίσης, θα αποδείξουμε ότι ένα ελαχίστου βαθμού πολυώνυμο του $\mathbb{Q}[x]$ που έχει ως ρίζες του τις πρωταρχικές p^2-οστές ρίζες της μονάδας είναι το $g(x)=\sum_{\ell=1}^{p}x^{[p\,(p-\ell)]}$.

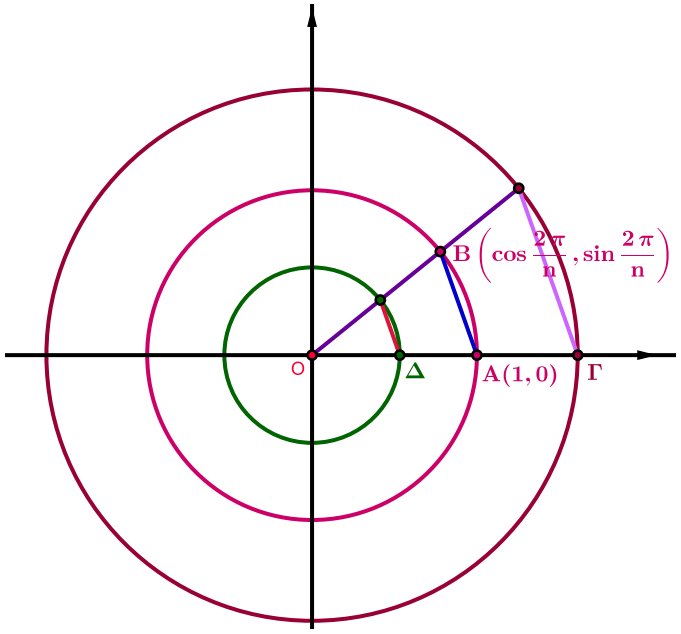
Για την πρώτη περίπτωση, παρατηρούμε ότι οι p-οστές ρίζες της μονάδας είναι ρίζες του πολυωνύμου x^p-1 το οποίο παραγοντοποιείται ως $x^p-1=(x-1)\,f(x)$. Άρα, οι μιγαδικές p-οστές ρίζες της μονάδας, (δηλαδή, όλες εκτός του 1), είναι ρίζες του $f(x)$. Έστω $h(x)\in\mathbb{Q}[x]$ με $deg[h(x)]<deg[f(x)]$ ένα ελαχίστου βαθμού πολυώνυμο που να έχει ως ρίζα του μία από τις μιγαδικές p-οστές ρίζες της μονάδας π.χ. την ζ_{i_0} με $i_0\in\{1,2,\ldots,p-1\}$. Η Ευκλείδεια διαίρεση των $f(x)$, $h(x)$ δίνει $f(x)=h(x)\,a(x)+r(x)$ με $a(x),r(x)\in\mathbb{Q}[x]$, $r(x)=0$ ή $0\le deg[r(x)]<deg[h(x)]$.

Αν $r(x)=0$ τότε, $f(x)=h(x)\,a(x)$ αντιβαίνοντας το συμπέρασμα της παραγράφου 97 ότι το $f(x)$ είναι ανάγωγο επί του $\mathbb{Q}[x]$. Άρα, $0\le deg[r(x)]<deg[h(x)]$. Όμως τότε, $f(\zeta_{i_0})=h(\zeta_{i_0})\,a(\zeta_{i_0})+r(\zeta_{i_0})$ συνεπάγεται ότι, $r(\zeta_{i_0})=0$. Οπότε, υπάρχει πολυώνυμο του $\mathbb{Q}[x]$, (το $r(x)$), που έχει ως ρίζα του την ζ_{i_0} και βαθμό μικρότερο του ελαχίστου βαθμού που μπορεί να έχει ένα πολυώνυμο του $\mathbb{Q}[x]$ με ρίζα την ζ_{i_0}, άτοπο. Άρα, το $h(x)$ δεν υπάρχει και το συμπέρασμα απεδείχθη.

Για την δεύτερη περίπτωση, παρατηρούμε ότι οι p^2-οστές ρίζες της μονάδας είναι ρίζες του πολυωνύμου $x^{p^2}-1$ το οποίο παραγοντοποιείται ως $x^{p^2}-1=(x^p-1)\,g(x)$. Αν μία πρωταρχική p^2-οστή ρίζα της μονάδας π.χ. η ζ είναι ρίζα του x^p-1 τότε, $\zeta^p=1$ αντιβαίνοντας το γεγονός ότι για την ζ ισχύει $\zeta^m\neq 1$ για κάθε $m\in\{1,2,\ldots,p^2-1\}$. Άρα, οι πρωταρχικές p^2-στές ρίζες της μονάδας είναι ρίζες του πολυωνύμου $g(x)$. Η απόδειξη ότι το $g(x)$ είναι και ελαχίστου βαθμού πολυώνυμο του $\mathbb{Q}[x]$ προκύπτει ομοίως με την αντίστοιχη απόδειξη για το $f(x)$ και στηρίζεται στο συμπέρασμα της παραγράφου 100 ότι το $g(x)$ είναι ανάγωγο επί του $\mathbb{Q}[x]$.

102. Από την Ευκλείδεια Γεωμετρία γνωρίζουμε ότι κάθε κανονικό n-γωνο είναι εγγράψιμο σε κύκλο διαιρώντας έτσι τον κύκλο σε n ίσα τόξα. Ως εκ' τούτου, το πρόβλημα της κατασκευής κανονικού n-γώνου με κανόνα και διαβήτη ανάγεται στο πρόβλημα της διαίρεσης με κανόνα και διαβήτη της περιφέρειας δοθέντος κύκλου σε n ίσα τόξα.

Ας υποθέσουμε κατ' αρχήν, ότι ο δοθείς κύκλος έχει ακτίνα 1, (Σχήμα 15). Διαίρεση με κανόνα και διαβήτη της περιφέρειας του κύκλου αυτού σε n ίσα τόξα ισοδυναμεί με διαίρεση με κανόνα και διαβήτη της αντίστοιχης της περιφέρειας του κύκλου επίκεντρης γωνίας των $2\,\pi$ ακτινίων σε n ίσες επίκεντρες γωνίες των $2\,\pi/n$ ακτινίων. Έστω το σημείο $A(1,0)$ του κύκλου. Η κατασκευή με κανόνα και διαβήτη μίας επίκεντρης γωνίας $\widehat{AOB}$ μέτρου $2\,\pi/n$ αντιστοιχεί στον προσδιορι-



Σχήμα 15.

σμό με κανόνα και διαβήτη του σημείου B του κύκλου με συντεταγμένες $\left(\text{συν}\,\frac{2\pi}{n}, \text{ημ}\,\frac{2\pi}{n}\right)$. Το σημείο αυτό, όπως προκύπτει από την παράγραφο 83 είναι η εικόνα στο επίπεδο του μιγαδικού αριθμού $e^{2\pi i/n}$ ο οποίος με τη σειρά του είναι μία πρωταρχική n-οστή ρίζα της μονάδας. Τελικά, η κατασκευή με κανόνα και διαβήτη κανονικού n-γώνου εγγεγραμμένου σε κύκλο ακτίνας 1 ανάγεται στην κατασκευή με κανόνα και διαβήτη της πρωταρχικής n-οστής ρίζα της μονάδας $e^{2\pi i/n}$.

Αν επιθυμούμε την κατασκευή με κανόνα και διαβήτη κανονικού n-γώνου εγγεγραμμένου σε κύκλο ακτίνας $r > 1$ ή $r < 1$ τότε όπως φαίνεται στο Σχήμα 15, κατασκευάζουμε την πρωταρχική n-οστή ρίζα της μονάδας $e^{2\pi i/n}$ η οποία αντιστοιχεί σε σημείο B του μοναδιαίου κύκλου και φέροντας την ημιευθεία $\overrightarrow{OB}$ τέμνουμε τον ομόκεντρο του μοναδιαίου, κύκλο ακτίνας $r > 1$ ή $r < 1$ σε σημείο που προσδιορίζει το ζητούμενο $1/n$ της περιφέρειας τόξο.

Οι επόμενες παράγραφοι αναφέρονται στην διατύπωση και απόδειξη της αναγκαίας και ικανής συνθήκης που πρέπει να πληροί ο n ώστε ένα κανονικό n-γωνο να είναι κατασκευάσιμο με κανόνα και διαβήτη. Ισοδυνάμως, στην διατύπωση και απόδειξη της αναγκαίας και ικανής συνθήκης που πρέπει να πληροί ο n ώστε η πρωταρχική n-οστή ρίζα της μονάδας $e^{2\pi i/n}$ να είναι κατασκευάσιμη με κανόνα και διαβήτη.

103. Έστω $n, m \in \mathbb{N} - \{0, 1, 2\}$, ο m διαιρέτης του n. Έστω ότι το κανονικό n-γωνο είναι κ.κ.δ. Θα αποδείξουμε ότι και το κανονικό m-γωνο είναι κ.κ.δ.

Θεωρούμε το κανονικό n-γωνο $A_1A_2\ldots A_n$ εγγεγραμμένο σε κύκλο. Έστω $n = m\,b$. Τότε οι κορυφές του κανονικού n-γώνου μπορούν να γραφούν ως,

$$A_{1+j\,b},\ A_{2+j\,b}\ \ldots,\ A_{(b-1)+j\,b},\ A_{b+j\,b},\quad j = 0, 1, 2, \ldots, m-1,$$

οπότε τα ευθύγραμμα τμήματα, $\overline{A_{1+j\,b}A_{b+1+j\,b}}$ για $j = 0, 1, 2, \ldots, m-1$, $A_{n+1} \equiv A_1$, είναι οι m ίσες χορδές ίσων ανά b τόξων του κύκλου και το συμπέρασμα απεδείχθη.

104. Έστω ότι ένα κανονικό n-γωνο είναι κ.κ.δ., p ένας περιττός πρώτος διαιρέτης του n. Θα αποδείξουμε ότι, ο $p = 2^{2^m} + 1$, με $m \in \mathbb{N}$. Οι πρώτοι της μορφής $2^{2^m} + 1$ λέγονται πρώτοι Fermat.

Από την παράγραφο 103 προκύπτει ότι και το κανονικό p-γωνο είναι κ.κ.δ. Από την παράγραφο 102 προκύπτει ότι η πρωταρχική p-οστή ρίζα της μονάδας, η $e^{2\,\pi\,i/p}$, είναι κ.κ.δ. Από τις παραγράφους 57, 101 προκύπτει ότι ένα ελαχίστου βαθμού πολυώνυμο με ακέραιους συντελεστές που έχει την $e^{2\,\pi\,i/p}$ ως ρίζα είναι το $f(x) = \sum_{k=0}^{p-1} x^k$. Ο βαθμός $p-1$ του $f(x)$ είναι 2^s για κάποιο $s \in \mathbb{N}$ δηλαδή, $p = 2^s + 1$. Αν ο s έχει περιττό διαιρέτη π.χ. τον $2\,r+1$ τότε μπορούμε να γράψουμε $s = (2\,r+1)\,b$ με $b \in \mathbb{N} - \{0\}$. Επίσης,

$$p = 2^{(2\,r+1)\,b} + 1 = \left((2^b)^{2\,r+1} + 1\right) = (2^b + 1)\left(\sum_{j=0}^{2\,r} (-1)^j\,(2^b)^{2\,r-j}\right),$$

αντιβαίνοντας στην υπόθεση ότι ο p είναι περιττός πρώτος. Άρα, ο s μη έχοντας περιττούς διαιρέτες είναι κάποια δύναμη του 2 και το συμπέρασμα απεδείχθη.

105. Έστω ότι ένα κανονικό n-γωνο είναι κ.κ.δ. και p περιττός πρώτος διαιρέτης του n. Θα αποδείξουμε ότι, ο p^2 δεν διαιρεί τον n.

Έστω ότι ο p^2 διαιρεί τον n. Τότε, από την παράγραφο 103 και επειδή $p^2 > 3$ έπεται ότι και το κανονικό p^2-γωνο είναι κ.κ.δ. Από την παράγραφο 102 προκύπτει ότι η πρωταρχική p-οστή ρίζα της μονάδας, η $e^{2\,\pi\,i/p^2}$, είναι κ.κ.δ. Από τις παραγράφους 57, 101 προκύπτει ότι ένα ελαχίστου βαθμού πολυώνυμο με ακέραιους συντελεστές που έχει την $e^{2\,\pi\,i/p^2}$ ως ρίζα είναι το $g(x) = \sum_{\ell=1}^{p} x^{[p\,(p-\ell)]}$. Ο βαθμός $p\,(p-1)$ του $g(x)$ είναι 2^s για κάποιο $s \in \mathbb{N}$ δηλαδή, $p\,(p-1) = 2^s$. Όμως ο p σαν περιττός πρώτος δεν διαιρεί δυνάμεις του 2. Οπότε, η ισότητα $p\,(p-1) = 2^s$ έχει νόημα μόνο αν $p = 1$ και $p - 1 = 2^s$ άτοπο γιατί ο p είναι πρώτος. Το συμπέρασμα απεδείχθη.

106. Έστω ότι ένα κανονικό n-γωνο είναι κ.κ.δ. Θα αποδείξουμε ότι $n = 2^k \prod_{j=1}^{m} p_j$ με $k \in \mathbb{N}$, $m \in \mathbb{N} - \{0\}$, p_j πρώτος Fermat.

Από την παράγραφο 104 προκύπτει ότι, κάθε περιττός διαιρέτης p_j του n είναι πρώτος Fermat. Από την παράγραφο 105 προκύπτει ότι, κάθε περιττός διαιρέτης p_j του n έχει εκθέτη 1 στην ανάλυση του n ως γινόμενο πρώτων παραγόντων. Ο μόνος άρτιος πρώτος που μπορεί να υπάρχει στην ανάλυση του n ως γινόμενο πρώτων παραγόντων είναι ο 2 και γι΄ αυτόν δεν υπάρχει περιορισμός για το πλήθος εμφανίσεων του. Το συμπέρασμα απεδείχθη.

107. Έστω $n \in \mathbb{N} - \{0, 1, 2\}$. Από την παράγραφο 106 προκύπτει ότι,

Αν το κανονικό n-γωνο είναι κ.κ.δ. τότε $\mathbf{n = 2^k \prod_{j=1}^{m} p_j}$, με $\mathbf{k \in \mathbb{N}}$, $\mathbf{m \in \mathbb{N} - \{0\}}$, $\mathbf{p_j}$ διακεκριμένοι πρώτοι Fermat.

Η τελευταία είναι η αναγκαία συνθήκη που πρέπει να ικανοποιεί το πλήθος των πλευρών ενός κανονικού n-γώνου ώστε αυτό να είναι κ.κ.δ. Π.χ. το κανονικό 7-ωνο δεν είναι κ.κ.δ. γιατί ο πρώτος 7 δεν είναι πρώτος Fermat. Επίσης, το κανονικό 9-γωνο δεν είναι κ.κ.δ. γιατί στην ανάλυση του 9 σε γινόμενο πρώτων παραγόντων, ο 3, (που είναι πρώτος Fermat), εμφανίζεται υψωμένος εις την δευτέρα.

Στις επόμενες παραγράφους διαπραγματευόμαστε την διατύπωση και απόδειξη της ικανής συνθήκης που πρέπει να ικανοποιεί το πλήθος των πλευρών ενός

κανονικού n-γώνου ώστε αυτό να είναι κ.κ.δ.

108. Έστω a, b, n τρεις ακέραιοι αριθμοί $n \neq 0$. Θα λέμε ότι οι a, b είναι ισότιμοι $\pmod n$ αν ο n διαιρεί την διαφορά $a-b$. Η ισοτιμία των a, b $\pmod n$ θα συμβολίζεται με $a \equiv b \pmod n$. Ορισμένες χρήσιμες ιδιότητες των ισοτιμιών είναι οι ακόλουθες και προκύπτουν άμεσα από τον ορισμό

- Αν $a \equiv b \pmod n$ τότε και $b \equiv a \pmod n$.
- Αν $a \equiv b \pmod n$ και $b \equiv g \pmod n$ τότε, και $a \equiv g \pmod n$.
- Αν $a \equiv b \pmod n$ και $g \equiv d \pmod n$ τότε, και $a \pm g \equiv b \pm d \pmod n$.
- Αν $a \equiv b \pmod n$ και $g \equiv d \pmod n$ τότε, και $a\,g \equiv b\,d \pmod n$ γιατί $a\,g - b\,d = (a-b)\,g + (g-d)\,b$.
- Αν $a \equiv b \pmod n$ τότε, και $a\,g \equiv b\,g \pmod n$.
- Αν $a\,g \equiv b\,g \pmod n$ και οι g, n είναι πρώτοι μεταξύ τους τότε, και $a \equiv b \pmod n$.
- Αν $a \equiv b \pmod n$ και $k \in \mathbb{N}$ τότε, και $a^k \equiv b^k \pmod n$.

109. Αν οι ακέραιοι αριθμοί a, n είναι πρώτοι μεταξύ τους θα αποδείξουμε ότι $a^{\phi(n)} \equiv 1 \pmod n$. Το συμπέρασμα αυτό είναι γνωστό ως θεώρημα Euler–Fermat.

Από την παράγραφο 98 γνωρίζουμε ότι ο αριθμός $\phi(n)$ εκφράζει το πλήθος των φυσικών αριθμών στο διάστημα $[1,n]$ που είναι σχετικώς πρώτοι με τον n. (Οι εκφράσεις, δύο αριθμοί είναι σχετικώς πρώτοι και δύο αριθμοί είναι πρώτοι μεταξύ τους είναι ταυτόσημες). Έστω ότι με $r_1, r_2, \ldots, r_{\phi(n)}$ συμβολίζουμε τους σχετικώς πρώτους με τον n φυσικούς στο $[1,n]$. Έστω b ένας τυχαίος ακέραιος σχετικώς πρώτος με τον n, (όχι υποχρεωτικώς από το $[1,n]$). Η Ευκλείδεια διαίρεση των b, n δίνει $b = n\,g + \upsilon$ με $g, \upsilon \in \mathbb{Z}$ και $0 \leq \upsilon < n$. Αν $\upsilon = 0$ τότε, $b = n\,g$ αντιβαίνοντας την υπόθεση ότι οι b, n είναι πρώτοι μεταξύ τους.

Άρα, $0 < \upsilon < n$ και $b \equiv \upsilon \pmod n$ με $\upsilon \in [1, n-1]$. Επίσης, οι n, υ δεν έχουν κοινό πρώτο παράγοντα γιατί αν είχαν, έστω τον p, από την ισότητα $b = n\,g + \upsilon$ θα προέκυπτε ότι ο p είναι παράγοντας και του b αντιβαίνοντας στην υπόθεση ότι οι n, b είναι πρώτοι μεταξύ τους. Άρα ο υ είναι κάποιος από τους $r_1, r_2, \ldots, r_{\phi(n)}$. Έστω ότι ο $\upsilon = r_i$ για κάποιο $i \in \{1, 2, \ldots, \phi(n)\}$. Τότε, $b \equiv r_i \pmod n$. Αν επιλέξουμε για b τον αριθμό $a\,r_j$ με $j \in \{1, 2, \ldots, \phi(n)\}$ τότε,

$$a\,r_j \equiv r_i \pmod n. \tag{59}$$

Αν $i \neq j$ τότε, είτε $1 \leq r_i < r_j < n$ είτε $1 \leq r_j < r_i < n$ από όπου προκύπτει ότι, οι $(r_i - r_j)$ και $(r_j - r_i)$ δεν διαιρούνται με το n αφού $|r_i - r_j| < n$. Άρα, $r_j \not\equiv r_i \pmod n$ και επειδή, οι a, n είναι πρώτοι μεταξύ τους,

$$a\,r_j \not\equiv a\,r_i \pmod n. \tag{60}$$

Από την (60) προκύπτει ότι οι $a\,r_j$ είναι διακεκριμένοι $\pmod n$. Είναι προφανές ότι $\prod_{j=1}^{\phi(n)} r_j = \prod_{i=1}^{\phi(n)} r_i$. Από την (59) προκύπτει ότι,

$$\begin{aligned}\prod_{j=1}^{\phi(n)} a\,r_j &\equiv \prod_{i=1}^{\phi(n)} r_i \pmod n = \prod_{j=1}^{\phi(n)} r_j \pmod n,\\ a^{\phi(n)} \prod_{j=1}^{\phi(n)} r_j &\equiv \prod_{j=1}^{\phi(n)} r_j \pmod n \Rightarrow a^{\phi(n)} \equiv 1 \pmod n,\end{aligned}$$

αφού οι n, $\prod_{i=1}^{\phi(n)} r_i$ είναι πρώτοι μεταξύ τους.

110. Έστω p πρώτος αριθμός, a ακέραιος ώστε οι p, a να είναι πρώτοι μεταξύ τους. Θα αποδείξουμε ότι $a^{p-1} \equiv 1 \pmod p$ και $a^p \equiv a \pmod p$. Η τελευταία ισοτιμία είναι γνωστή ως μικρό θεώρημα του Fermat.

Από την παράγραφο 99 γνωρίζουμε ότι $\phi(p) = p-1$. Από την παράγραφο 109 προκύπτει ότι, $a^{\phi(p)} = a^{p-1} \equiv 1 \pmod p$. Η ισοτιμία $a^p \equiv a \pmod p$ προκύπτει από την $a^{p-1} \equiv 1 \pmod p$ δηλαδή, ο p διαιρεί το γινόμενο $a\,(a^{p-1}-1)$.

111. Έστω p πρώτος αριθμός, a ακέραιος, a, p πρώτοι μεταξύ τους. Από την παράγραφο 110 γνωρίζουμε ότι $a^{p-1} \equiv 1 \pmod p$. Αν επιπλέον ισχύει $a^m \not\equiv 1 \pmod p$ για κάθε $1 \le m \le p-2$ ο a λέγεται πρωταρχική ρίζα της μονάδας $\pmod p$.

Επίσης, αν h είναι ο μικρότερος μη μηδενικός φυσικός ώστε $a^h \equiv 1 \pmod p$ λέμε ότι ο a έχει τάξη $h \pmod p$.

112. Έστω $n \in \mathbb{N} - \{0\}$. Θα αποδείξουμε ότι, $\sum_{m|n} \phi(m) = n$ όπου το άθροισμα εκτείνεται σε όλους τους φυσικούς διαιρέτες m του n.

Οι φυσικοί διαιρέτες του n είναι αριθμοί που ανήκουν στο σύνολο $\{1, 2, \ldots, n-1, n\}$. Έστω m ένας φυσικός διαιρέτης του n τότε $n = m\,b$ όπου b επίσης ένας φυσικός διαιρέτης του n. Θεωρούμε τους n το πλήθος ρητούς αριθμούς,

$$\frac{n}{1}, \frac{n}{2}, \frac{n}{3}, \ldots, \frac{n}{n-1}, \frac{n}{n}. \tag{61}$$

Τα κλάσματα της (61) είναι δυνατό να διαχωρισθούν ως εξής,

- Όσα είναι ήδη ανάγωγα. Είναι εκείνα που οι n και $i \in \{1, 2, \ldots, n\}$ είναι πρώτοι μεταξύ τους και το πλήθος τους ισούται με $\phi(n)$.
- Όσα οι n και $i \in \{1, 2, \ldots, n\}$ δεν είναι πρώτοι μεταξύ τους. Τότε, αν d_i είναι ο μέγιστος κοινός διαιρέτης των n και i μπορούμε να τα απλοποιήσουμε διαιρώντας αριθμητή και παρονομαστή με το d_i. Σε αυτή την περίπτωση ο αριθμητής του ισοδύναμου κλάσματος που προκύπτει από την απλοποίηση είναι κάποιος φυσικός διαιρέτης του n. Έστω m ένας τέτοιος αριθμητής. Αυτός εμφανίζεται ως αριθμητής σε εκείνα τα απλοποιημένα κλάσματα ο παρονομαστής των οποίων στην (61) είναι σχετικώς πρώτος με τον m. Άρα, σε $\phi(m)$ το πλήθος κλάσματα.

Όταν απλοποιηθούν τα κλάσματα της (61) οι αριθμητές που θα προκύψουν θα είναι όλοι οι διαιρέτες του n με πιθανή επανάληψη κάποιων από αυτούς. Αυτό γιατί, ανάμεσα στους παρονομαστές των κλασμάτων της (61) υπάρχουν όλοι οι

φυσικοί διαιρέτες του n. Άρα, τα κλάσματα που τους έχουν ως παρονομαστές όταν απλοποιηθούν θα δώσουν ως αποτέλεσμα $m/1$ όπου m ο κάθε φυσικός διαιρέτης του n.

Στα υπόλοιπα κλάσματα n/i που δεν έχουν παρονομαστή φυσικό διαιρέτη του n η διαίρεση των δύο όρων με τον μέγιστο κοινό διαιρέτη τους d_i θα δώσει ως αποτέλεσμα κλάσματα που ο αριθμητής τους θα είναι της μορφής n/d_i δηλαδή κάποιος από τους φυσικούς διαιρέτες του n. Σε αυτά τα κλάσματα είναι που έχουμε επανάληψη εμφάνισης στον απλοποιημένο αριθμητή τους κάποιου από τους φυσικούς διαιρέτες του n. Αν οι διαιρέτες του n είναι ℓ το πλήθος τότε, τα κλάσματα της (61) ομαδοποιούνται σε ℓ το πλήθος ομάδες κάθε μία εκ΄ των οποίων θα περιέχει τα $\phi(m)$ το πλήθος κλάσματα που όταν απλοποιηθούν ο αριθμητής τους θα είναι ο φυσικός διαιρέτης m του n. Άρα, το συνολικό πλήθος n των κλασμάτων της (61) ισούται με $\sum_{m|n}\phi(m)$ και το συμπέρασμα απεδείχθη.

113. Έστω p πρώτος αριθμός, $f(x)=\sum_{i=0}^{n}a_i\,x^i\in\mathbb{Z}[x]$, ο p δεν διαιρεί τον a_n. Θα αποδείξουμε ότι, η $f(x)\equiv 0 \pmod p$ έχει το πολύ n διακεκριμένες $\pmod p$ ακέραιες ρίζες. Σημειώνουμε ότι, με τον όρο b, g διακεκριμένοι ακέραιοι $\pmod p$ εννοούμε $b\not\equiv g \pmod p$.

Εφαρμόζουμε επαγωγή στον n. Αν $n=0$ τότε, από την υπόθεση $a_n=a_0$, ο p δεν διαιρεί τον a_0 και $f(x)=a_0\not\equiv 0 \pmod p$. Έπεται ότι, η $f(x)\equiv 0 \pmod p$ έχει το πολύ $n=0$ ακέραιες ρίζες. Υποθέτουμε ότι το συμπέρασμα ισχύει για όλα τα πολυώνυμα του $\mathbb{Z}[x]$ βαθμού $n-1$ με $n\geq 1$. Έστω $f(x)\in\mathbb{Z}[x]$ πολυώνυμο βαθμού n. Αν η $f(x)\equiv 0 \pmod p$ έχει 0 ρίζες τότε το συμπέρασμα ότι έχει το πολύ n διακεκριμένες $\pmod p$ ακέραιες ρίζες ισχύει αφού $0<n$. Για κάποιο ακέραιο r μπορούμε να γράψουμε,

$$f(x)-f(r)=\sum_{i=0}^{n}a_i\,(x^i-r^i)=(x-r)\sum_{i=1}^{n}a_i\left(\sum_{j=0}^{i-1}x^{i-1-j}\,x^j\right)=(x-r)\,g(x),$$

με $g(x)$ πολυώνυμο βαθμού $n-1$ με ακέραιους συντελεστές και συντελεστή του μεγιστοβάθμιου όρου a_n μη διαιρετό από τον p. Έστω ότι η $f(x)\equiv 0 \pmod p$ έχει κάποιες διακεκριμένες $\pmod p$ ακέραιες ρίζες με r μία από αυτές. Αν r είναι μοναδική τότε, το συμπέρασμα για την εξίσωση $f(x)\equiv 0 \pmod p$ ισχύει αφού $1\leq n$. Έστω ότι υπάρχει και δεύτερη διακεκριμένη $\pmod p$ ως προς την r ακέραια ρίζα της $f(x)\equiv 0 \pmod p$, η ρ.

Επειδή, $f(r)\equiv 0 \pmod p$, προκύπτει ότι η εξίσωση $f(x)\equiv 0 \pmod p$ γράφεται ως $(x-r)\,g(x)\equiv 0 \pmod p$. Επίσης, οι $\rho-r$ και p είναι σχετικώς πρώτοι οπότε,

$$f(\rho)\equiv 0 \pmod p \Rightarrow (\rho-r)\,g(\rho)\equiv 0 \pmod p \Rightarrow g(\rho)\equiv 0 \pmod p.$$

Η εξίσωση $g(x)\equiv 0 \pmod p$ έχει τουλάχιστον μία ακέραια ρίζα άρα από την υπόθεση της επαγωγής έχει το πολύ $n-1$ διακεκριμένες $\pmod p$ ακέραιες ρίζες. Οπότε η εξίσωση,

$$(x-r)\,g(x)\equiv 0 \pmod p,$$

έχει το πολύ n διακεκριμένες $\pmod p$ ακέραιες ρίζες.

114. Έστω p πρώτος αριθμός, $a\in\{1,2,\ldots,p-1\}$. Οι αριθμοί p και a

είναι πρώτοι μεταξύ τους. Από την παράγραφο 110 προκύπτει ότι $a^{p-1} \equiv 1 \pmod{p}$. Αυτό σημαίνει ότι υπάρχει ελάχιστος θετικός ακέραιος h έτσι ώστε $a^h \equiv 1 \pmod{p}$. Θεωρούμε την Ευκλείδεια διαίρεση $p-1 = h\,b + \upsilon$ με $b, \upsilon \in \mathbb{Z}$, $0 \leq \upsilon < h$. Αν $\upsilon \neq 0$ τότε, $a^{p-1} \equiv 1 \pmod{p} \Rightarrow (a^h)^b\, a^\upsilon \equiv 1 \pmod{p} \Rightarrow a^\upsilon \equiv 1 \pmod{p}$ αντιβαίνοντας στην υπόθεση ότι ο h είναι ελάχιστος. Άρα, ο h διαιρεί τον $p-1$.

115. Έστω p πρώτος αριθμός, $a \in \{1, 2, \ldots, p-1\}$. Από την παράγραφο 114 προκύπτει ότι υπάρχει ελάχιστος θετικός ακέραιος h έτσι ώστε $a^h \equiv 1 \pmod{p}$ και ο h διαιρεί τον $p-1$. Σε μία τέτοια περίπτωση θα λέμε ότι ο a έχει τάξη h. Θα αποδείξουμε ότι αν ο $a \in \{1, 2, \ldots, p-1\}$ έχει τάξη h τότε, $\phi(h)$ το πλήθος στοιχεία του $\{1, 2, \ldots, p-1\}$ έχουν τάξη h.

Αφού ο $a \in \{1, 2, \ldots, p-1\}$ έχει τάξη h τότε, η εξίσωση $x^h - 1 \equiv 0 \pmod{p}$ έχει μία ακέραια ρίζα και από την παράγραφο 113 προκύπτει ότι η εξίσωση $x^h - 1 \equiv 0 \pmod{p}$ έχει το πολύ h διακεκριμένες $\pmod{p}$ ακέραιες ρίζες. Επειδή, $a^h \equiv 1 \pmod{p} \Rightarrow a^{k\,h} \equiv 1 \pmod{p}$ για $k = 2, 3, \ldots, h$ δηλαδή, $(a^k)^h - 1 \equiv 0 \pmod{p}$. Οι $a, a^2, a^3, \ldots, a^h$ είναι ακέραιες ρίζες της $x^h - 1 \equiv 0 \pmod{p}$.

Επειδή, οι p, a είναι πρώτοι μεταξύ τους και οι p, a^i και οι p, a^j για $i, j \in \{1, 2, \ldots, h\}$ είναι πρώτοι μεταξύ τους. Αν για κάποια $i, j \in \{1, 2, \ldots, h\}$ με $i \neq j$ συμβαίνει $a^i \equiv a^j \pmod{p}$ τότε, είτε $a^{i-j} \equiv 1 \pmod{p}$, $(i > j)$, είτε $a^{j-i} \equiv 1 \pmod{p}$, $(j > i)$ αντιβαίνοντας σε κάθε περίπτωση στην υπόθεση ότι h ο ελάχιστος θετικός ακέραιος ώστε $a^h \equiv 1 \pmod{p}$. Αποδείξαμε ότι η εξίσωση $x^h - 1 \equiv 0 \pmod{p}$ έχει ακριβώς h διακεκριμένες $\pmod{p}$ ακέραιες ρίζες τις $a, a^2, a^3, \ldots, a^h$. Επειδή, κάθε στοιχείο του $\{1, 2, \ldots, p-1\}$ που έχει τάξη h είναι ρίζα της εξίσωσης $x^h - 1 \equiv 0 \pmod{p}$ και οι διακεκριμένες $\pmod{p}$ ακέραιες ρίζες της είναι οι $a, a^2, a^3, \ldots, a^h$ προκύπτει ότι τα στοιχεία του $\{1, 2, \ldots, p-1\}$ που έχουν τάξη h βρίσκονται μεταξύ των $a, a^2, a^3, \ldots, a^h$.

Έστω ότι για κάποιο $k = 1, 2, \ldots, h$ ο a^k έχει τάξη h. Αν ο k έχει και κοινό πρώτο παράγοντα q με τον h τότε, ο h/q είναι θετικός ακέραιος μικρότερος του h και $(a^k)^{h/q} = (a^h)^{k/q} \equiv 1 \pmod{p}$ αντιβαίνοντας την υπόθεση ότι ο h είναι η τάξη του a^k. Άρα, τα στοιχεία του $\{1, 2, \ldots, p-1\}$ που έχουν τάξη h βρίσκονται μεταξύ εκείνων από τους $a, a^2, a^3, \ldots, a^h$ που ο εκθέτης τους είναι σχετικώς πρώτος με τον h. Επειδή, οι $a, a^2, a^3, \ldots, a^h$ των οποίων ο εκθέτης είναι σχετικώς πρώτος με τον h είναι $\phi(h)$ το πλήθος προκύπτει ότι για το πλήθος $y(h)$ των στοιχείων του $\{1, 2, \ldots, p-1\}$ που έχουν τάξη h ισχύει $y(h) \leq \phi(h)$.

Ορίζουμε την συνάρτηση $\psi : \{\text{Οι θετικοί διαιρέτες του } p-1\} \mapsto \mathbb{N}$ με τύπο,

$$\psi(h) = \begin{cases} y(h) & , \quad h \text{ είναι τάξη κάποιου στοιχείου του } \{1, 2, \ldots, p-1\}, \\ 0 & , \quad h \text{ δεν είναι τάξη κάποιου στοιχείου του } \{1, 2, \ldots, p-1\}. \end{cases}$$

Έχουμε ήδη τονίσει ότι, κάθε στοιχείο του $\{1, 2, \ldots, p-1\}$ έχει τάξη κάποιον θετικό διαιρέτη του $p-1$. Τα στοιχεία του $\{1, 2, \ldots, p-1\}$ κατανέμονται σε ξένα μεταξύ τους υποσύνολα στοιχείων που έχουν την ίδια τάξη. Άρα,

$$p - 1 = \sum_{h|p-1} \psi(h) \leq \sum_{h|p-1} \phi(h) = p - 1,$$

(παράγραφος 112). Συνεπάγεται $\sum_{h|p-1} \psi(h) = \sum_{h|p-1} \phi(h)$ και επειδή $\psi(h) \leq \phi(h)$ έπεται ότι $\psi(h) = \phi(h)$. Η $\psi(h)$ τελικώς δεν λαμβάνει μηδενικές τιμές και σε κάθε διαιρέτη του $p-1$ αντιστοιχούν κάποια στοιχεία του $\{1, 2, \ldots, p-1\}$ με

τάξη τον διαιρέτη αυτόν. Το πλήθος τους είναι $\psi(h) = \phi(h)$. Και στον διαιρέτη $p-1$ του $p-1$ αντιστοιχούν στοιχεία του $\{1, 2, \ldots, p-1\}$ με τάξη $p-1$. Το πλήθος τους είναι $\psi(p-1) = \phi(p-1)$.

116. Έστω p πρώτος αριθμός. Από τις παραγράφους 111, 115 προκύπτει ότι υπάρχουν $\phi(p-1)$ το πλήθος, (διακεκριμένες $\pmod p$), πρωταρχικές ρίζες της μονάδας $\pmod p$.

117. Έστω $p = 2^{2^\nu} + 1$ πρώτος Fermat. Θα αποδείξουμε στις επόμενες παραγράφους ότι μία πρωταρχική p-οστή ρίζα της μονάδας είναι κ.κ.δ.

Από την παράγραφο 98 προκύπτει ότι, οι p-οστές ρίζες της μονάδας είναι οι $1, \zeta_1, \zeta_1^2, \ldots, \zeta_1^{p-1}$. Επειδή οι $1, 2, \ldots, p-1$ είναι σχετικώς πρώτοι με τον p από την ίδια παράγραφο προκύπτει ότι οι $\zeta_1, \zeta_1^2, \ldots, \zeta_1^{p-1}$ είναι όλες οι πρωταρχικές p-οστές ρίζες της μονάδας. Από την παράγραφο 101 προκύπτει ότι οι ζ_1^s, $s = 1, 2, \ldots, p-1$ είναι ρίζες του πολυωνύμου $f(x) = \sum_{k=0}^{p-1} x^k$. Από την παράγραφο 70 και τους τύπους του Viète προκύπτει ότι, $\zeta_1 + \zeta_1^2 + \ldots + \zeta_1^{p-1} = -1$. Αν για κάποια $i, j \in \{1, 2, \ldots, p-1\}$ με $i \neq j$ συμβαίνει $\zeta_1^i = \zeta_1^j$ τότε, είτε $\zeta_1^{i-j} = 1$ με $i > j$ και $0 < i - j < p-1$, είτε $\zeta_1^{j-i} = 1$ με $j > i$ και $0 < j - i < p-1$ αντιβαίνοντας στην υπόθεση ότι η ζ_1 είναι πρωταρχική p-οστή ρίζα της μονάδας. Άρα οι $\zeta_1, \zeta_1^2, \ldots, \zeta_1^{p-1}$ είναι διακεκριμένες μεταξύ τους.

Από την παράγραφο 116 προκύπτει ότι υπάρχουν $\phi(p-1)$ το πλήθος, (διακεκριμένες $\pmod p$), πρωταρχικές ρίζες της μονάδας $\pmod p$. Έστω g μία από αυτές. Αν για κάποια $i, j \in \{1, 2, \ldots, p-1\}$ με $i \neq j$ συμβαίνει $g^i \equiv g^j \pmod p$ τότε, είτε $g^{i-j} \equiv 1 \pmod p$ με $i > j$ και $0 < i - j < p-1$, είτε $g^{j-i} \equiv 1 \pmod p$ με $j > i$ και $0 < j - i < p-1$, αντιβαίνοντας στην υπόθεση ότι η g είναι πρωταρχική ρίζα της μονάδας $\pmod p$. Άρα, οι $g, g^2, \ldots, g^{p-1}$ είναι διακεκριμένες $\pmod p$ και δεν διαιρούνται με τον p αφού η g δεν διαιρείται με τον p.

Θεωρούμε τους $\zeta_1^g, \zeta_1^{g^2}, \ldots, \zeta_1^{g^{p-1}}$. Αυτοί είναι p-οστές ρίζες της μονάδας αφού αν υψωθούν εις την p δίνουν 1. Είναι διακεκριμένες μεταξύ τους γιατί αν δεν ήταν, η ισότητα $\zeta_1^{g^i} = \zeta_1^{g^j}$ για κάποια $i, j \in \{1, 2, \ldots, p-1\}$ με $i \neq j$ θα συνεπάγετω είτε $\zeta_1^{g^i - g^j} = 1$ με $i > j$ και $0 < i - j < p-1$, είτε $\zeta_1^{g^j - g^i} = 1$ με $j > i$ και $0 < j - i < p-1$. Η ζ_1 είναι πρωταρχική p-οστή ρίζα της μονάδας. Αν $\zeta_1^b = 1$, πρέπει $b \geq p$. Από την Ευκλείδεια διαίρεση $b = p\,d + \upsilon$, με $0 \leq \upsilon < p$ προκύπτει ότι, αν $\upsilon \neq 0$, $1 = z_1^b = (z_1^p)^d\, z_1^\upsilon = z_1^\upsilon$ αντιβαίνοντας στην υπόθεση ότι η z_1 είναι πρωταρχική p-οστή ρίζα της μονάδας. Άρα, $\upsilon = 0$ και ο p διαιρεί τον b.

Δηλαδή, αν $\zeta_1^{g^i} = \zeta_1^{g^j}$ όπως αναφέρθηκε πιο πάνω τότε, ο p διαιρεί είτε την $g^i - g^j$ είτε την $g^j - g^i$ αντιβαίνοντας στο γεγονός ότι οι g^i είναι διακεκριμένες $\pmod p$.

Άρα, οι $\zeta_1^g, \zeta_1^{g^2}, \ldots, \zeta_1^{g^{p-1}}$ είναι $p-1$ το πλήθος διακεκριμένες p-οστές ρίζες της μονάδας με εκθέτες $g, g^2, \ldots, g^{p-1}$ σχετικώς πρώτους με τον p. Από την παράγραφο 98 προκύπτει ότι, οι $\zeta_1^g, \zeta_1^{g^2}, \ldots, \zeta_1^{g^{p-1}}$ είναι οι πρωταρχικές p-οστές ρίζες της μονάδας και $\{\zeta_1, \zeta_1^2, \ldots, \zeta_1^{p-1}\} = \{\zeta_1^g, \zeta_1^{g^2}, \ldots, \zeta_1^{g^{p-1}}\}$. Εξ΄ αιτίας αυτού ισχύει,

$$\zeta_1^g + \zeta_1^{g^2} + \ldots + \zeta_1^{g^{p-1}} = -1. \tag{62}$$

Για λόγους απλοποίησης των πολύπλοκων συμβολισμών, στα επόμενα θα γράφουμε $[\mu] = \zeta_1^\mu$. Είναι σαφές από τις ιδιότητες των δυνάμεων ότι $[\mu + \delta] = \zeta_1^\mu\, \zeta_1^\delta$,

$[\mu\,\delta] = (\zeta_1^{\mu})^{\delta} = [\mu]^{\delta}$ και $[\mu^{k+\tau}] = \zeta_1^{\mu^{k+\tau}} = (\zeta_1^{\mu^k})^{\mu^\tau} = [\mu^k]^{\mu^\tau}$. Ορίζουμε,

1. $\Sigma_0 = \{[g], [g^2], \ldots, [g^{p-1}]\}$,

2. $\Sigma_1 = \{[g], [g^3], \ldots, [g^{p-2}]\}$, $\Sigma_2 = \{[g^2], [g^4], \ldots, [g^{p-1}]\}$ δηλαδή,
το Σ_1 περιέχει το πρώτο στοιχείο του Σ_0 και κάθε δεύτερο στοιχείο μετά από αυτό ενώ, το Σ_2 περιέχει το δεύτερο στοιχείο του Σ_0 και κάθε δεύτερο στοιχείο μετά από αυτό,

3. $\Sigma_{1,1} = \{[g], [g^5], \ldots, [g^{p-4}]\}$, $\Sigma_{1,2} = \{[g^3], [g^7], \ldots, [g^{p-2}]\}$ δηλαδή,
το $\Sigma_{1,1}$ περιέχει το πρώτο στοιχείο του Σ_1 και κάθε δεύτερο στοιχείο μετά από αυτό ενώ, το $\Sigma_{1,2}$ περιέχει το δεύτερο στοιχείο του Σ_1 και κάθε δεύτερο στοιχείο μετά από αυτό,
$\Sigma_{2,1} = \{[g^2], [g^6], \ldots, [g^{p-3}]\}$, $\Sigma_{2,2} = \{[g^4], [g^8], \ldots, [g^{p-1}]\}$ δηλαδή,
το $\Sigma_{2,1}$ περιέχει το πρώτο στοιχείο του Σ_2 και κάθε δεύτερο στοιχείο μετά από αυτό ενώ, το $\Sigma_{2,2}$ περιέχει το δεύτερο στοιχείο του Σ_2 και κάθε δεύτερο στοιχείο μετά από αυτό,

4. Επαγωγικώς, $\Sigma_{i_1,i_2,\ldots,i_{m-1},1}$, $\Sigma_{i_1,i_2,\ldots,i_{m-1},2}$, $(m \geq 2,\ i_j \in \{1,2\})$, δηλαδή,
το $\Sigma_{i_1,i_2,\ldots,i_{m-1},1}$ περιέχει το πρώτο στοιχείο του $\Sigma_{i_1,i_2,\ldots,i_{m-1}}$ και κάθε δεύτερο στοιχείο μετά από αυτό ενώ, το $\Sigma_{i_1,i_2,\ldots,i_{m-1},2}$ περιέχει το δεύτερο στοιχείο του $\Sigma_{i_1,i_2,\ldots,i_{m-1}}$ και κάθε δεύτερο στοιχείο μετά από αυτό.

Καλούμε τα σύνολα $\Sigma_{i_1,i_2,\ldots,i_{m-1},1}$, $\Sigma_{i_1,i_2,\ldots,i_{m-1},2}$, που δημιουργούνται κατά την διαδικασία του (4.) m-σύνολα. Κάθε ένα από αυτά τα σύνολα περιέχει $(p-1)/2^m$ στοιχεία. Από το προηγούμενο είναι σαφές ότι τα $m = 2^\nu$-σύνολα θα περιέχουν ένα μόνο στοιχείο έκαστο, που θα είναι μία πρωταρχική p-οστή ρίζα της μονάδας. Δύο m-σύνολα θα λέγονται συμπληρωματικά αν προέρχονται από το ίδιο $m-1$ σύνολο με την διαδικασία του (4.).

Ορίζουμε ως m-περίοδο το άθροισμα των $(p-1)/2^m$ στοιχείων ενός m-συνόλου. Οι περίοδοι δύο m-συμπληρωματικών συνόλων θα λέγονται συμπληρωματικές. Για $m = 2^\nu$ οι m-περίοδοι ισούνται με το μοναδικό στοιχείο που περιέχει κάθε ένα από τα δύο m-σύνολα.

Από την περιγραφείσα διαδικασία στα βήματα 1 έως 4 προκύπτει ότι ένα m-σύνολο δημιουργείται αν επιλέξουμε το πρώτο ή το δεύτερο στοιχείο ενός $m-1$ συνόλου και διαδοχικώς το υψώσουμε εις την g^{2^m}. Μία τέτοια ενέργεια θα παράξει όλα τα στοιχεία του m-συνόλου και από ένα σημείο και μετά τα στοιχεία του m-συνόλου θα επαναλαμβάνονται. Αυτό σημαίνει ότι, για να παράξουμε τα στοιχεία ενός m-συνόλου μπορούμε αντί να επιλέξουμε το πρώτο ή το δεύτερο στοιχείο ενός $(m-1)$-συνόλου, να επιλέξουμε οποιοδήποτε στοιχείο αυτού και να το υψώσουμε διαδοχικώς εις την g^{2^m}.

118. Έστω η_1 μία m-περίοδος και η_2 η συμπληρωματική της. Θα αποδείξουμε ότι για $1 \leq m \leq 2^\nu - 1$ ο $\eta_1\,\eta_2$ εκφράζεται ως γραμμικός συνδυασμός, με μη αρνητικούς ακέραιους συντελεστές, m-περιόδων. Σε αυτόν τον γραμμικό συνδυασμό οι συμπληρωματικές περίοδοι έχουν ίσους συντελεστές. Για $m = 2^\nu$, $\eta_1\,\eta_2 = 1$.

Οι η_1, η_2 ως συμπληρωματικές m-περίοδοι είναι το άθροισμα των στοιχείων δύο συμπληρωματικών m-συνόλων $\Sigma_{i_1,i_2,\ldots,i_{m-1},1}$, $\Sigma_{i_1,i_2,\ldots,i_{m-1},2}$, $i_j \in \{1,2\}$, (για $m = 1$, $\Sigma_{i_0,1} = \Sigma_1$, $\Sigma_{i_0,2} = \Sigma_2$), αντιστοίχως. Αυτά προέρχονται από την εφαρμογή των όσων αναφέραμε στη παράγραφο 117 για κάποιο $(m-1)$-σύνολο.

Αυτό το $(m-1)$-σύνολο δημιουργήθηκε από διαδοχική ύψωση εις την $g^{2^{m-1}}$ κάποιου ζ_1^k δηλαδή, περιέχει τα,

$$[k]\,,\left[k\,g^{2^{m-1}}\right],\left[k\,g^{2^m}\right],\ldots,\left[k\,g^{2^{m-1}\,(f-2)}\right],\;\; f=1+\frac{p-1}{2^{m-1}},$$

όπου,

$$g^{2^{m-1}\,(f-1)}=\left(g^{2^{m-1}}\right)^{(p-1)/2^{m-1}}=g^{(p-1)}\equiv 1 \pmod p,$$

συνεπάγοντας ότι, οι επόμενες δυνάμεις που δημιουργούνται κατ΄ αυτό τον τρόπο επαναλαμβάνουν τα ήδη υπάρχοντα στοιχεία του $m-1$-συνόλου.

Θέτουμε $h=g^{2^{m-1}}$. Τότε, τα στοιχεία του $(m-1)$-συνόλου μπορούν να γραφούν ως,

$$[k],[k\,h],[k\,h^2],\ldots,[k\,h^{f-2}],\;\; f=1+\frac{p-1}{2^{m-1}},$$

οπότε,

$$\begin{aligned}\eta_1 &= [k]+\left[k\,h^2\right]+\cdots+\left[k\,h^{f-3}\right],\\ \eta_2 &= [k\,h]+\left[k\,h^3\right]+\cdots+\left[k\,h^{f-2}\right].\end{aligned}$$

Έστω $1\le m\le 2^\nu-1$. Δεδομένου ότι $[k\,h^\ell]\,[k\,h^j]=[k\,h^\ell+k\,h^j]$ ο πολλαπλασιασμός $\eta_1\,\eta_2$, ομαδοποιώντας καταλλήλως τις προκύπτουσες δυνάμεις, γράφεται,

$$\begin{aligned}\eta_1\,\eta_2 &= [k+k\,h]+\left[k\,h^2+k\,h^3\right]+\cdots+\left[k\,h^{f-3}+k\,h^{f-2}\right]+\\ &+ \left[k+k\,h^3\right]+\left[k\,h^2+k\,h^5\right]+\cdots+\left[k\,h^{f-3}+k\,h\right]+\\ &+ \left[k+k\,h^5\right]+\left[k\,h^2+k\,h^7\right]+\cdots+\left[k\,h^{f-3}+k\,h^3\right]+\\ &\vdots\\ &+ \left[k+k\,h^{f-4}\right]+\left[k\,h^2+k\,h^{f-2}\right]+\cdots+\left[k\,h^{f-3}+k\,h^{f-6}\right]+\\ &+ \left[k+k\,h^{f-2}\right]+\left[k\,h^2+k\,h\right]+\cdots+\left[k\,h^{f-3}+k\,h^{f-4}\right].\end{aligned}$$

Οι προσθεταίοι κάθε γραμμής του αθροίσματος παράγονται από ύψωση ενός τυχαίου προσθεταίου της γραμμής εις την h^2. Θα δείξουμε για τους προσθεταίους του αθροίσματος ότι δεν διαιρούνται με τον p. Αρκεί να το δείξουμε για τους όρους της πρώτης στήλης του αθροίσματος. Οι όροι των υπολοίπων στηλών είναι πολλαπλάσια των όρων της πρώτης στήλης με το h^2. Οι παράγοντες αυτών των γινομένων δηλαδή, οι όροι της πρώτης στήλης και το h^2 δεν διαιρούνται με το p. Άρα, οι όροι των υπολοίπων στηλών δεν διαιρούνται με το p.

Έστω ότι, $k+k\,h^{2\,j+1}\equiv 0 \pmod p$, $j=0,1,\ldots,\frac{p-1}{2^m}-1$. Επειδή, $k=g^\tau$, $\tau=1,2,\ldots,p-1$ με p, k σχετικώς πρώτους, έπεται ότι,

$$\begin{aligned}k+k\,h^{2\,j+1}\equiv 0 \pmod p &\;\Rightarrow\; k\,(1+h^{2\,j+1})\equiv 0 \pmod p \Rightarrow\\ h^{2\,j+1})\equiv -1 \pmod p &\;\Rightarrow\; h^{4\,j+2}\equiv 1 \pmod p\\ g^{2^{m-1}\,(4\,j+2)}\equiv 1 \pmod p &\quad .\end{aligned}$$

Επειδή, η g είναι πρωταρχική ρίζα της μονάδας $\pmod p$ έπεται ότι ο $p-1$ διαιρεί τον $2^{m-1}\,(4\,j+2)$ δηλαδή, τον $2^m\,(2\,j+1)$ δηλαδή, ο 2^{2^ν} διαιρεί τον 2^m αντιβαίνοντας στην υπόθεση $1\le m\le 2^\nu-1$.

Αποδείξαμε ότι η πρώτη γραμμή, (και ομοίως κάθε), γραμμή του αθροίσματος με το οποίο ισούται το $\eta_1\,\eta_2$ αποτελείται από $(p-1)/2^m$ το πλήθος πρωταρχικές p-οστές ρίζες της μονάδας είναι δηλαδή μία m-περίοδος. Λαμβάνοντας υπ΄ όψιν ότι, ύψωση εις την h^2 επαναληπτικώς ενός στοιχείου ενός m-συνόλου δίνει τα υπόλοιπα στοιχεία του m-συνόλου ενώ, ύψωση εις την h ενός στοιχείου ενός m-συνόλου παράγει στοιχείο του συμπληρωματικού του m-συνόλου παρατηρούμε ότι, $[k{+}k\,h]^h = [k\,h{+}k\,h^2] = [k\,h^2{+}k\,h]$. Δηλαδή, η ύψωση εις την h του πρώτου προσθεταίου της πρώτης γραμμής, (ο οποίος είναι στοιχείο ενός m-συνόλου), δίνει τον δεύτερο προσθεταίο της τελευταίας γραμμής, (ο οποίος είναι στοιχείο ενός άλλου m-συνόλου). Η ύψωση εις την h του δεύτερου προσθεταίου της πρώτης γραμμής δίνει τον τρίτο προσθεταίο της τελευταίας γραμμής και ούτω καθ΄ εξής.

Άρα, οι προσθεταίοι της τελευταίας γραμμής είναι στοιχεία του συμπληρωματικού του m-συνόλου που αποτελείται από τους προσθεταίους της πρώτης γραμμής. Ομοίως, οι προσθεταίοι της ℓ από το τέλος γραμμής είναι στοιχεία του συμπληρωματικού του m-συνόλου που αποτελείται από τους προσθεταίους της ℓ από την αρχή γραμμής. Το πλήθος των γραμμών είναι $\frac{f-3}{2}+1=\frac{p-1}{2^m}$ και τα αθροίσματα των ισαπεχόντων γραμμών από την πρώτη και την τελευταία γραμμή είναι συμπληρωματικές m-περίοδοι. Άρα, κάθε m-περίοδος στο συνολικό άθροισμα εμφανίζεται τόσες φορές όσες η συμπληρωματική της. Αν συμβολίσουμε με η_i την m-περίοδο της i γραμμής του αθροίσματος, (με το οποίο ισούται το $\eta_1\,\eta_2$), και με $\tilde{\eta}_i$ την συμπληρωματική της, (δηλαδή, την m-περίοδο της i από το τέλος γραμμής του αθροίσματος), έχουμε αποδείξει ότι,

$$\eta_1\,\eta_2 = \sum_{i=1}^{(p-1)/2^{m+1}} (\eta_i + \tilde{\eta}_i).$$

Στο πιο πάνω άθροισμα όμως, η η_i άρα και η $\tilde{\eta}_i$ μπορεί να εμφανίζονται επαναληπτικώς. Έστω η_{i_j} και $\tilde{\eta}_{i_j}$, $j=1,2,\ldots,t$, $t\le\frac{p-1}{2^{m+1}}$ οι διακεκριμένες m-περίοδοι και οι συμπληρωματικές τους όπως εμφανίζονται στο άθροισμα με το οποίο ισούται το $\eta_1\,\eta_2$. Αν συμβολίσουμε με r_{i_j} το πλήθος των εμφανίσεων των $\eta_{i_j},\tilde{\eta}_{i_j}$ στο άθροισμα με το οποίο ισούται το $\eta_1\,\eta_2$ τελικώς προκύπτει,

$$\eta_1\,\eta_2 = \sum_{j=1}^{t} r_{i_j}\,(\eta_{i_j} + \tilde{\eta}_{i_j}),$$

και το συμπέρασμα απεδείχθη για $1\le m\le 2^\nu-1$.

Για $m=2^\nu$, παρατηρούμε ότι, $h=g^{2^{m-1}}=\left(g^{2^{2^\nu}}\right)^{2^{-1}}=g^{(p-1)/2}$. Επειδή, $g^{p-1}\equiv 1 \pmod p$ έπεται $\left(g^{(p-1)/2}\right)^2\equiv 1 \pmod p$ και ο $g^{(p-1)/2}$ είναι ρίζα της εξίσωσης $x^2\equiv 1 \pmod p$. Ως τέτοια θα πρέπει $g^{(p-1)/2}\equiv\pm 1 \pmod p$ αφού $(\pm 1)^2\equiv 1 \pmod p$ και από την παράγραφο 113 η εξίσωση $x^2-1\equiv 0 \pmod p$ έχει το πολύ 2 διακεκριμένες $\pmod p$ ακέραιες ρίζες. Όμως, δεν μπορεί $g^{(p-1)/2}\equiv 1 \pmod p$ γιατί η g είναι πρωταρχική ρίζα της μονάδας $\pmod p$. Τελικώς, $h=g^{(p-1)/2}\equiv -1 \pmod p$ ή $h+1=p\,a$.

Από την παράγραφο 117 προκύπτει ότι τα 2^ν-σύνολα περιέχουν ένα μόνο στοιχείο οπότε, αν $\eta_1=[k]$, $\eta_2=[k\,h]=[k\,p\,a-k]=[-k]$. Άρα, $\eta_1\,\eta_2=\zeta_1^k\,\zeta_1^{-k}=1$.

119. Θα αποδείξουμε ότι για κάθε m τέτοιο ώστε $0 \leq m \leq 2^\nu$ όλες οι m-περίοδοι είναι κ.κ.δ.

Εφαρμόζουμε επαγωγή στο m. Για $m = 0$ υπάρχει μία 0-περίοδος αυτή του αθροίσματος (62) η οποία ισούται με -1 άρα είναι κ.κ.δ. από την παράγραφο 29. Υποθέτουμε ότι κάθε $(m-1)$-περίοδος είναι κ.κ.δ. Έστω η_1 μία m-περίοδος και η_2 η συμπληρωματική της. Το άθροισμα $\eta_1 + \eta_2$ είναι μία $(m-1)$-περίοδος και από την υπόθεση της επαγωγής είναι κ.κ.δ. Από την παράγραφο 118 προκύπτει ότι το γινόμενο $\eta_1\,\eta_2$ ισούται, είτε με 1 οπότε είναι κ.κ.δ., είτε με,

$$\eta_1\,\eta_2 = \sum_{j=1}^{t} r_{i_j}\,(\eta_{i_j} + \tilde{\eta}_{i_j}),$$

όπου r_{i_j} μη αρνητικοί ακέραιοι, η_{i_j}, $\tilde{\eta}_{i_j}$ συμπληρωματικές m-περίοδοι. Το άθροισμα $\eta_{i_j} + \tilde{\eta}_{i_j}$ είναι μία $(m-1)$-περίοδος και από την υπόθεση της επαγωγής είναι κ.κ.δ. Από την παράγραφο 29 και το γινόμενο $\eta_1\,\eta_2$ είναι κ.κ.δ. Από την παράγραφο 51 προκύπτει ότι οι ρίζες της εξίσωσης $z^2 - (\eta_1 + \eta_2)\,z + (\eta_1\,\eta_2) = 0$ είναι κ.κ.δ. γιατί οι συντελεστές του τριωνύμου $z^2 - (\eta_1 + \eta_2)\,z + (\eta_1\,\eta_2)$ είναι κ.κ.δ. Οι ρίζες τις προαναφερθείσας εξίσωσης είναι η_1 και η_2 άρα το συμπέρασμα απεδείχθη για m.

120. Από τις παραγράφους 117, 118, 119 προκύπτει ότι αν ο $p = 2^{2^\nu} + 1$ είναι πρώτος Fermat μία πρωταρχική p-οστή ρίζα της μονάδας είναι κ.κ.δ. Από την παράγραφο 102 προκύπτει ότι αν ο $p = 2^{2^\nu} + 1$ είναι πρώτος Fermat το κανονικό p-γωνο είναι κ.κ.δ.

121. Έστω m, n σχετικώς πρώτοι φυσικοί αριθμοί. Αν το κανονικό m-γωνο, n-γωνο είναι κ.κ.δ. τότε θα αποδείξουμε ότι και το κανονικό $m\,n$-γωνο είναι κ.κ.δ.

Έστω a, b μία πρωταρχική m-οστή, n-οστή ρίζα της μονάδας αντιστοίχως. Τότε, $(a\,b)^{m\,n} = 1$. Έστω k θετικός φυσικός μικρότερος του $m\,n$ ώστε $(a\,b)^k = 1$. Τότε, $a^k = b^{-k}$ και $1 = a^{k\,m} = b^{-k\,m}$. Όμως, από την Ευκλείδεια διαίρεση των $-k\,m$, n προκύπτει $-k\,m = n\,d + v$ με d ακέραιο, $0 \leq v \leq n-1$ ακέραιο. Αν $v \neq 0$ προκύπτει $1 = b^{-k\,m} = (b^n)^d\,b^v = b^v$ αντιβαίνοντας στην υπόθεση ότι ο b είναι πρωταρχική n-οστή ρίζα της μονάδας. Άρα, $v = 0$ και ο n διαιρεί τον $-k\,m$. Επειδή m, n είναι πρώτοι μεταξύ τους έπεται ότι ο n διαιρεί τον k. Με ακριβώς ανάλογη λογική προκύπτει ότι και ο m διαιρεί τον k. Δηλαδή, $k = n\,r_1 = m\,r_2$. Από την τελευταία ισότητα προκύπτει ότι ο n διαιρεί τον $m\,r_2$. Όμως οι n, m είναι πρώτοι μεταξύ τους. Άρα, ο n διαιρεί τον r_2 και $k = (m\,n)\,r_3$ αντιβαίνοντας στην υπόθεση ότι $k < m\,n$. Άρα, το γινόμενο $a\,b$ είναι μία πρωταρχική $m\,n$-οστή ρίζα της μονάδας.

Αφού το κανονικό m-γωνο, n-γωνο είναι κ.κ.δ. τότε, από την παράγραφο 102 προκύπτει ότι μία πρωταρχική m-οστή, n-οστή ρίζα της μονάδας αντιστοίχως είναι κ.κ.δ. Έστω a, b η πρωταρχική m-οστή, n-οστή ρίζα της μονάδας αντιστοίχως που είναι κ.κ.δ. Από την παράγραφο 30 προκύπτει ότι και το γινόμενο $a\,b$ είναι κ.κ.δ. Από την προηγούμενη ανάλυση όμως το γινόμενο $a\,b$ είναι μία πρωταρχική $m\,n$-οστή ρίζα της μονάδας. Δηλαδή, μία πρωταρχική $m\,n$-οστή ρίζα της μονάδας είναι κ.κ.δ. Από την παράγραφο 102 προκύπτει ότι το κανονικό $m\,n$-γωνο είναι κ.κ.δ.

122. Θα αποδείξουμε ότι για $k \in \mathbb{N} - \{0, 1\}$ το κανονικό 2^k-γωνο είναι κ.κ.δ.

Η κατασκευή μίας πρωταρχικής 2^k-στής ρίζας της μονάδας με κ.κ.δ. είναι δυνατή αν στον μοναδιαίο κύκλο μία επίκεντρη γωνία μέτρου $2\,\pi/2^k$ μπορεί να κ.κ.δ. Αυτό είναι πάντα δυνατό αφού απαιτεί διαδοχικές διχοτομήσεις της γωνίας των $2\,\pi$ ακτινίων. Η κ.κ.δ. της διχοτόμου γωνίας είναι πάντα δυνατή.

123. Θα αποδείξουμε ότι αν το κανονικό n-γωνο είναι κ.κ.δ. τότε, για $k \in \mathbb{N} - \{0\}$ και το κανονικό $2^k\,n$-γωνο είναι κ.κ.δ.

Από την υπόθεση και την παράγραφο 102 προκύπτει ότι μία πρωταρχική n-οστή ρίζα της μονάδας είναι κ.κ.δ. Δηλαδή, μία επίκεντρη γωνία μέτρου $2\,\pi/n$ είναι κ.κ.δ. στον μοναδιαίο κύκλο.Τότε, και διαδοχικές διχοτομήσεις της γωνίας αυτής στον μοναδιαίο κύκλο είναι κ.κ.δ. Άρα, και η επίκεντρη γωνία μέτρου $2\,\pi/(2^k\,n)$ είναι κ.κ.δ. στον μοναδιαίο κύκλο. Οπότε, και μία πρωταρχική $2^k\,n$-οστή ρίζα της μονάδας είναι κ.κ.δ. Από την παράγραφο 102 προκύπτει ότι και το κανονικό $2^k\,n$-γωνο είναι κ.κ.δ.

124. Έστω $n = 2^k \prod_{i=1}^{\ell} \left(2^{2^{m_i}} + 1\right)$ με $k \in \mathbb{N}$, $\ell \in \mathbb{N} - \{0\}$, $m_i \in \mathbb{N}$, $\left(2^{2^{m_i}} + 1\right)$ διακεκριμένους πρώτους Fermat. Θα αποδείξουμε ότι το κανονικό n-γωνο είναι κ.κ.δ.

Από την παράγραφο 120 προκύπτει ότι το κάθε κανονικό $\left(2^{2^{m_i}} + 1\right)$-γωνο είναι κ.κ.δ. Επειδή οι $\left(2^{2^{m_i}} + 1\right)$ είναι διακεκριμένοι πρώτοι αριθμοί είναι και πρώτοι μεταξύ τους. Από την παράγραφο 121 προκύπτει ότι το κανονικό $\prod_{i=1}^{\ell} \left(2^{2^{m_i}} + 1\right)$-γωνο είναι κ.κ.δ. Αν ο k είναι 0 το συμπέρασμα απεδείχθη. Αν $k \in \mathbb{N} - \{0\}$ από την παράγραφο 123 προκύπτει ότι το κανονικό n-γωνο είναι κ.κ.δ.

125. Από τις παραγράφους 107, 124 προκύπτει η ικανή και αναγκαία συνθήκη που πρέπει να ικανοποιεί το πλήθος n των πλευρών ενός κανονικού n-γώνου ώστε αυτό να είναι κ.κ.δ. δηλαδή,

Ένα κανονικό n-γωνο είναι κατασκευάσιμο με κανόνα και διαβήτη αν και μόνο αν ο n αναλύεται ως $\mathbf{2^k \prod_{i=1}^{\ell} \left(2^{2^{m_i}} + 1\right)}$, με $\mathbf{k \in \mathbb{N}}$, $\mathbf{\ell \in \mathbb{N} - \{0\}}$, $\mathbf{m_i \in \mathbb{N}}$, $\mathbf{\left(2^{2^{m_i}} + 1\right)}$ διακεκριμένους πρώτους Fermat.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Ανδρεαδάκη Σ., *"Μαθήματα επί της Θεωρίας του Galois"*, Αθήνα, 1975.

[2] Μπρίκα Μ., *"Τα Περίφημα Άλυτα Γεωμετρικά Προβλήματα της Αρχαιότητος"*, Αθήνα, 1970.

[3] Dörrie H., *"100 Great Problems of Elementary Mathematics"*, Dover, 1965.

[4] Gall L., *"Classical Galois Theory"*, AMS Chelsea, 1998.

[5] Hadlock C.R., *"Field Theory and its Classical Problems"*, The Mathematical Association of America, 2000.

[6] Jacobson N., *"Basic Algebra I"*, Freeman, Sec. Edition, 1985.

[7] Milne J.S., *"Fields and Galois Theory (v4.51)"*, `www.milne.org/math/`, 2015.

[8] Stewart I., *"Galois Theory"*, Chapman and Hall/CRC, 2004.

[9] Tignol J.P., *"Galois' Theory of Algebraic Equations"*, World Scientific, 2001, Rep. 2004.

[10] Rotman J., *"Galois Theory"*, Springer Verlag, 1990.