ΠΟΛΥΩΝΥΜΙΚΕΣ ΕΞΙΣΩΣΕΙΣ ΕΠΙΛΥΣΙΜΕΣ ΔΙΑ ΡΙΖΙΚΩΝ ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΘΕΩΡΙΑ GALOIS

ΗΛΙΑΣ ΛΑΜΠΑΚΗΣ

$$a_n\,x^n + a_{n-1}\,x^{n-1} + \cdots + a_1\,x + a_0 = 0$$

4ο ΓΥΜΝΑΣΙΟ ΠΥΡΓΟΥ–ΗΛΕΙΑΣ, 2017

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Κάθε εξίσωση της μορφής,

$$a_n\, x^n + a_{n-1}\, x^{n-1} + \cdots + a_1\, x + a_0 = 0,$$

με $a_n, a_{n-1}, \ldots, a_0$ γνωστές ποσότητες και n μη μηδενικό φυσικό αριθμό, λέγεται πολυωνυμική. Έως τα μέσα του 16ου αιώνα οι μαθηματικοί είχαν διαπιστώσει ότι οι λύσεις των πολυωνυμικών εξισώσεων πρώτου, δευτέρου, τρίτου και τετάρτου βαθμού n μπορούν να εκφρασθούν ως αλγεβρικές παραστάσεις γνωστών ποσοτήτων μεταξύ των οποίων σημειώνονται οι τέσσερις πράξεις της αριθμητικής και σύμβολα εξαγωγής ριζών κάποιας τάξης.

Οι γνωστές ποσότητες που εμφανίζονται στις προαναφερθείσες εκφράσεις των λύσεων πολυωνυμικών εξισώσεων έως και τετάρτου βαθμού είναι είτε οι συντελεστές της εξίσωσης είτε προκύπτουν ως αποτελέσματα των τεσσάρων πράξεων της αριθμητικής μεταξύ των συντελεστών της εξίσωσης.

Τέθηκε λοιπόν το ερώτημα κατά πόσον ανάλογης μορφής αλγεβρικές παραστάσεις μπορούν να εκφράσουν τις λύσεις πολυωνυμικών εξισώσεων οιουδήποτε βαθμού και αν αυτό δεν είναι δυνατό, ποιες είναι οι ικανές και αναγκαίες συνθήκες που πρέπει να ισχύουν ώστε αυτό να είναι δυνατό.

Μακροχρόνια και επίπονη έρευνα από τα μέσα του 16ου αιώνα έως και το 1831 σε σχέση με το προαναφερθέν ερώτημα οδήγησε στην διατύπωση των απαρχών της θεωρίας Galois η οποία αποτελεί την βάση εξέλιξης της σύγχρονης άλγεβρας.

Σκοπός της παρούσης μονογραφίας είναι να, παρουσιάσει με τρόπο όσο το δυνατόν πιο προσιτό την θεωρία επιλυσιμότητας πολυωνυμικών εξισώσεων δια ριζικών και μέσω αυτής να εισαγάγει τον αναγνώστη στις βασικές έννοιες της θεωρίας Galois.

Δίνεται έμφαση στα κίνητρα που οδήγησαν στην υιοθέτηση των Μαθηματικών εργαλείων που χρησιμοποιήθηκαν στις αρχές του 20ου αιώνα ώστε η θεωρία Galois να πάρει την τελική της μορφή σε σχέση με αυτήν που είχε κατά τον 19ο αιώνα οπότε και διαμορφωνόταν.

Οι αποδείξεις είναι πλήρεις και αναλυτικές, αποφεύγοντας, (εκτός πολύ τετριμμένων περιπτώσεων), το συχνό φαινόμενο της παράληψης ενδιαμέσων βημάτων που αφήνονται προς σκέψη για τον αναγνώστη. Το φαινόμενο αυτό συναντάται σχεδόν σε όλα τα Μαθηματικά κείμενα που επεξεργάζονται θέματα ανάλογου περιεχομένου.

ΠΟΛΥΩΝΥΜΙΚΕΣ ΕΞΙΣΩΣΕΙΣ ΕΠΙΛΥΣΙΜΕΣ ΔΙΑ ΡΙΖΙΚΩΝ ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΘΕΩΡΙΑ GALOIS

Ορισμένα Στοιχεία από την Θεωρία Σωμάτων

§1. Η διαδικασία επίλυσης της πιο απλής πολυωνυμικής εξίσωσης, που είναι η $a\,x + b = 0$, με a μη μηδενική γνωστή ποσότητα, b γνωστή ποσότητα και x άγνωστη ποσότητα, μας οδηγεί στην ανάγκη να εκφράσουμε την ποσότητα x ως παράσταση των γνωστών ποσοτήτων a και b μεταξύ των οποίων σημειώνεται η πράξη της διαίρεσης αφού $x = -b/a$.

Σε περιπτώσεις επίλυσης πολυωνυμικών εξισώσεων μεγαλύτερου βαθμού, όπως οι δευτεροβάθμιες ή οι τριτοβάθμιες, απαιτείται η χρήση και των τεσσάρων πράξεων, πρόσθεσης, αφαίρεσης, πολλαπλασιασμού και διαίρεσης μεταξύ των συντελεστών της εξίσωσης.

Καταλαβαίνουμε λοιπόν ότι, για να προχωρήσουμε στην διαδικασία επίλυσης μίας πολυωνυμικής εξίσωσης πρέπει το σύνολο των αριθμών με το οποίο αρχικά δουλεύουμε και από το οποίο προέρχονται οι συντελεστές της εξίσωσης να έχει ορισμένες αλγεβρικές ιδιότητες. Να έχει συγκεκριμένη αλγεβρική δομή δηλαδή, να ορίζονται σε αυτό οι τέσσερις πράξεις της αριθμητικής και να έχουν συγκεκριμένες αλγεβρικές ιδιότητες. Έτσι, η πρώτη απαραίτητη αλγεβρική έννοια που χρειάζεται να εισάγουμε είναι αυτή του **σώματος**.

§2. Τα γνωστά μας σύνολα των ρητών $\mathbb{Q}$, πραγματικών $\mathbb{R}$, μιγαδικών $\mathbb{C}$ αριθμών χαρακτηρίζονται από ένα πλήθος κοινών ιδιοτήτων που μας δίνουν τη δυνατότητα να οικοδομήσουμε σε αυτά κανόνες αριθμητικής. Αν συμβολίσουμε με S οποιοδήποτε από τα $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ το S εφοδιασμένο με τις πράξεις της γνωστής μας πρόσθεσης και του γνωστού μας πολλαπλασιασμού ικανοποιεί τις ιδιότητες,

I1. $a + b = b + a \in S$, για κάθε $a, b \in S$.

I2. Υπάρχει μοναδικό στοιχείο του S το 0 ώστε $a + 0 = 0 + a = a$ για κάθε $a \in S$.

I3. Για κάθε $a \in S - \{0\}$ υπάρχει μοναδικό στοιχείο το $-a \in S - \{0\}$ ώστε $a + (-a) = (-a) + a = 0$. Για το 0 ισχύει $0 + 0 = 0 + 0 = 0$. Η ύπαρξη του αντιθέτου στοιχείου $-a$ επάγει στο S την πράξη της αφαίρεσης.

I4. $a + (b + g) = (a + b) + g$, για κάθε $a, b, g \in S$.

I5. $a\,b = b\,a \in S$, για κάθε $a, b \in S$.

I6. Για κάθε $a \in S - \{0\}$ υπάρχει μοναδικό στοιχείο του S το 1 ώστε $a\,1 = 1\,a = a$. $0\,1 = 1\,0 = 0$ αλλά σε αυτή την περίπτωση το 1 δεν είναι το μοναδικό στοιχείο του S με αυτή την ιδιότητα αφού και $a\,0 = 0\,a = 0$ για κάθε $a \in S$.

I7. Για κάθε $a \in S - \{0\}$ υπάρχει μοναδικό στοιχείο το $a^{-1} \in S - \{0\}$ ώστε $a\,a^{-1} = a^{-1}\,a = 1$. Η ύπαρξη του αντιστρόφου στοιχείου a^{-1} επάγει στο S την πράξη της διαίρεσης.

I8. $a\,(b\,g) = (a\,b)\,g$, για κάθε $a, b, g \in S$.

I9. Για κάθε $a, b, g \in S$ ισχύει $a\,(b+g) = a\,b + a\,g$.

Γενικότερα, όταν τα στοιχεία οιουδήποτε συνόλου S, (πέραν των γνωστών μας $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$), εφοδιασμένου με μία πράξη «πρόσθεσης» και μία πράξη «πολλαπλασιασμού» ικανοποιούν τις ιδιότητες (I1–I9), το S λέγεται σώμα.

Όταν γράφουμε «πρόσθεσης», «πολλαπλασιασμού» εννοούμε πράξεις που μπορεί να μην είναι η γνωστή μας από τα $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ πρόσθεση ή πολλαπλασιασμός, αλλά πράξεις που ικανοποιούν ακριβώς τις ιδιότητες (I1–I9) οπότε αλγεβρικά συμπεριφέρονται όπως η γνωστή μας πρόσθεση και ο γνωστός μας πολλαπλασιασμός.

Σε μια τέτοια περίπτωση και όταν δεν υπάρχει κίνδυνος σύγχυσης συμβολίζουμε την «πρόσθεση» και τον «πολλαπλασιασμό» με τα συνήθη $(+)$, $(\cdot)$ ή κενό. Εάν υπάρχει κίνδυνος σύγχυσης χρησιμοποιούμε τα σύμβολα $(\oplus)$, $(\odot)$ ή $(\oplus_S)$, $(\odot_S)$ όπου S είναι το σύνολο επί του οποίου ορίζονται οι πράξεις.

§3. Έστω F, K σώματα. Κάθε συνάρτηση $\mathbf{f : F \mapsto K}$ με τις ιδιότητες,

- **H f είναι ένα προς ένα.**
- **H f είναι επί.**
- $\mathbf{f(a \oplus_F b) = f(a) \oplus_K f(b)}$ **και** $\mathbf{f(a \odot_F b) = f(a) \odot_K f(b)}$ **για κάθε** $\mathbf{a, b \in F}$.

λέγεται ισομορφισμός των F, K.

Οι ισομορφισμοί σωμάτων είναι σημαντικοί γιατί μεταφέρουν τις αλγεβρικές πληροφορίες από το ένα σώμα στο άλλο. Και αυτό γιατί, οι αλγεβρικές πληροφορίες ενός σώματος προέρχονται από τις πράξεις με τις οποίες αυτό είναι εφοδιασμένο και τις ιδιότητες των πράξεων αυτών. Οι ισομορφισμοί σωμάτων διατηρούν τις πράξεις των σωμάτων και τις ιδιότητές τους.

§4. Έστω F ένα σώμα. Για συντομία θα συμβολίζουμε την πρόσθεσή του με το σύνηθες $+$ και τον πολλαπλασιασμό του με κενό. $a \in F$, $n \in \mathbb{N}$. Ορίζουμε,

$$-n\,a = \underbrace{(-a) + (-a) + \cdots + (-a)}_{n-\text{προσθεταίοι}}, \quad \text{όταν} \quad n > 0,$$

$$n\,a = 0 \in F, \quad \text{όταν} \quad n = 0,$$

$$n\,a = \underbrace{a + a + \cdots + a}_{n-\text{προσθεταίοι}}, \quad \text{όταν} \quad n > 0.$$

Επίσης, με $n \pm m$, $n\,m$, $\frac{n}{m} = n/m$ συμβολίζουμε τις συνήθεις πράξεις μεταξύ των στοιχείων των $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Από τον πιο πάνω ορισμό και με $1 \in F$ είναι φανερά τα,

$$(n \pm m)\,1 = (n\,1) \pm (m\,1)\ ,\ \forall\, n, m \in \mathbb{Z}, \tag{1}$$

$$(n\,m)\,1 = n\,(m\,1) = m\,(n\,1)\ ,\ \forall\, n, m \in \mathbb{Z}, \tag{2}$$

$$(n\,1)\,(m\,1) = (n\,1)\,(\underbrace{1 + 1 + \cdots + 1}_{m-\text{προσθεταίοι}}) =$$

$$
\begin{aligned}
&= \underbrace{(n\,1)\,1 + (n\,1)\,1 + \cdots + (n\,1)\,1}_{m-\text{προσθεταίοι}} = \\
&= \underbrace{(n\,1) + (n\,1) + \cdots + (n\,1)}_{m-\text{προσθεταίοι}} = \\
&= m\,(n\,1) \overset{(2)}{=} (n\,m)\,1\ ,\ \forall\, n, m \in \mathbb{Z}. \qquad (3)
\end{aligned}
$$

Ο μικρότερος θετικός φυσικός n για τον οποίο ισχύει $\mathbf{n\,1 = 0}$, (αν υπάρχει τέτοιος n), λέγεται χαρακτηριστική του σώματος F. Αν τέτοιος n δεν υπάρχει λέμε ότι το σώμα F έχει χαρακτηριστική 0.

Στην συνέχεια, θεωρούμε ότι **όλα τα σώματα με τα οποία εργαζόμαστε έχουν χαρακτηριστική 0.** Π.χ. τα $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ έχουν χαρακτηριστική 0. Για κάθε $n, k \in \mathbb{Z}$ και κάθε $m, t \in \mathbb{Z} - \{0\}$ και υιοθετώντας τον συμβολισμό $(n\,1)\,(m\,1)^{-1} = \frac{n\,1}{m\,1} \in F$ ισχύει,

$$
\begin{aligned}
\frac{n\,1}{m\,1} = \frac{k\,1}{t\,1} \quad &\Leftrightarrow \quad (n\,1)\,(m\,1)^{-1} = (k\,1)\,(t\,1)^{-1} \Leftrightarrow \\
&\quad (n\,1)\,(t\,1) = (k\,1)\,(m\,1) \overset{(3)}{\Leftrightarrow} (n\,t)\,1 = (k\,m)\,1 \Leftrightarrow \\
&\quad (n\,t)\,1 - (k\,m)\,1 = 0 \in F \Leftrightarrow (n\,t - k\,m)\,1 = 0 \in F \Leftrightarrow \\
&\quad (\text{το } F \text{ έχει χαρατηριστική } 0) \\
&\quad n\,t - k\,m = 0 \in \mathbb{N} \Leftrightarrow \frac{n}{m} = \frac{k}{t}\,, \qquad (4)
\end{aligned}
$$

$$
\begin{aligned}
(t\,n\,m)\,1 = (t\,m\,n)\,1 \quad &\Leftrightarrow \quad [(t\,n)\,1]\,(m\,1) = [(t\,m)\,1]\,(n\,1) \Leftrightarrow \\
&\quad [(t\,n)\,1]\,[(t\,m)\,1]^{-1} = (n\,1)\,(m\,1)^{-1} \Leftrightarrow \\
&\quad \frac{(t\,n)\,1}{(t\,m)\,1} = \frac{n\,1}{m\,1} \overset{(3)}{\wedge} \frac{(t\,1)\,(n\,1)}{(t\,1)\,(m\,1)} = \frac{n\,1}{m\,1}\,. \qquad (5)
\end{aligned}
$$

§5. Έστω F ένα σώμα. Από την §4 προκύπτει ότι, για κάθε $n \in \mathbb{Z}$ το $n\,1$ είναι στοιχείο του F. Έστω $m \in \mathbb{Z} - \{0\}$. Επειδή το $(n\,1)\,(m\,1)^{-1} = \frac{n\,1}{m\,1}$ είναι στοιχείο του F, το σύνολο,

$$
F_{\mathbb{Q}} = \left\{ \frac{n\,1}{m\,1} \ :\ n \in \mathbb{Z},\, m \in \mathbb{Z} - \{0\} \right\}.
$$

είναι υποσύνολο του F. Η πρόσθεση του F περιορισμένη στο $F_{\mathbb{Q}}$ λαμβάνει την μορφή,

$$
\begin{aligned}
\frac{n\,1}{m\,1} + \frac{k\,1}{t\,1} \quad &\overset{(5)}{=} \quad \frac{(t\,1)\,(n\,1)}{(t\,1)\,(m\,1)} + \frac{(m\,1)\,(k\,1)}{(m\,1)\,(t\,1)} = \\
&= \quad [(t\,1)\,(n\,1)]\,[(t\,1)\,(m\,1)]^{-1} + [(m\,1)\,(k\,1)]\,[(t\,1)\,(m\,1)]^{-1} = \\
&= \quad [(t\,1)\,(n\,1) + (m\,1)\,(k\,1)]\,[(t\,1)\,(m\,1)]^{-1} = \\
&= \quad \frac{(t\,1)\,(n\,1) + (m\,1)\,(k\,1)}{(t\,1)\,(m\,1)} \overset{(1,3)}{=} \frac{(t\,n + m\,k)\,1}{(t\,m)\,1}\,. \qquad (6)
\end{aligned}
$$

Ο πολλαπλασιασμός του F περιορισμένος στο $F_{\mathbb{Q}}$ λαμβάνει την μορφή,

$$\frac{n\,1}{m\,1}\,\frac{k\,1}{t\,1} = (n\,1)\,(m\,1)^{-1}\,(k\,1)\,(t\,1)^{-1} = (n\,1)\,(k\,1)\,(m\,1)^{-1}\,(t\,1)^{-1} =$$

$$= (n\,1)\,(k\,1)\,[(m\,1)\,(t\,1)]^{-1} \overset{(3)}{=} [(n\,k)\,1]\,[(m\,t)\,1]^{-1} = \frac{(n\,k)\,1}{(m\,t)\,1}\,. \qquad (7)$$

Είναι άμεση εφαρμογή των (6), (7) και του γεγονότος ότι το $F_{\mathbb{Q}}$ είναι υποσύνολο του F, να αποδειχθεί ότι για το $F_{\mathbb{Q}}$ ισχύουν οι ιδιότητες (I1–I9) και αυτό είναι σώμα, (υποσώμα του F).

Θεωρούμε την συνάρτηση $f : \mathbb{Q} \mapsto F_{\mathbb{Q}}$ με $f\left(\frac{n}{m}\right) = \frac{n\,1}{m\,1}$. Είναι προφανές ότι η f είναι ένα προς ένα, (από την (4)), και επί, (από τον ορισμό της). Επιπλέον,

$$f\left(\frac{n}{m}+\frac{k}{t}\right) = f\left(\frac{n\,t+k\,m}{m\,t}\right) = \frac{(n\,t+k\,m)\,1}{(m\,t)\,1} \overset{(6)}{=} \frac{n\,1}{m\,1}+\frac{k\,1}{t\,1} =$$

$$= f\left(\frac{n}{m}\right)+f\left(\frac{k}{t}\right), \qquad (8)$$

$$f\left(\frac{n}{m}\,\frac{k}{t}\right) = f\left(\frac{n\,k}{m\,t}\right) = \frac{(n\,k)\,1}{(m\,t)\,1} \overset{(7)}{=} \frac{n\,1}{m\,1}\,\frac{k\,1}{t\,1} = f\left(\frac{n}{m}\right) f\left(\frac{k}{t}\right). \qquad (9)$$

Από την §3 προκύπτει ότι η f είναι ισομορφισμός σωμάτων. Στην περίπτωση αυτή τα στοιχεία του $F_{\mathbb{Q}}$ έχουν την ίδια αλγεβρική συμπεριφορά εντός του F με αυτή των στοιχείων του $\mathbb{Q}$ εντός του $\mathbb{R}$ ή του $\mathbb{C}$. Γι΄ αυτό λέμε ότι **το $\mathbf{F}_{\mathbb{Q}}$ είναι ισομορφική εμφύτευση του $\mathbb{Q}$ στο $\mathbf{F}$.** Στα προηγούμενα, το σώμα F επελέγη τυχαίως ανάμεσα στα σώματα με χαρακτηριστική 0. Άρα,

Κάθε σώμα $\mathbf{F}$ χαρακτηριστικής 0 περιέχει ως υποσώμα του το σώμα $\mathbf{F}_{\mathbb{Q}}$ που είναι ισομορφικό με το $\mathbb{Q}$. Δηλαδή, το $\mathbf{F}_{\mathbb{Q}}$ περιέχει τους «ρητούς» του $\mathbf{F}$. Φυσικά, αν $\mathbf{F} = \mathbb{Q}$ ή $\mathbb{R}$ ή $\mathbb{C}$, τότε $\mathbf{F}_{\mathbb{Q}} = \mathbb{Q}$.

Από τα προηγούμενα συνάγεται ότι το μικρότερο σώμα χαρακτηριστικής 0 είναι το $\mathbb{Q}$ μιας και το να δουλεύει κάποιος αλγεβρικά με το $\mathbf{F}_{\mathbb{Q}}$ είναι ισοδύναμο με το να δουλεύει με το $\mathbb{Q}$ αφού ότι αλγεβρικό γίνεται στο $\mathbb{Q}$ μεταφέρεται μέσω του ισομορφισμού $\mathbf{f}$ στο $\mathbf{F}_{\mathbb{Q}}$ και αντιστρόφως.

§6. Στα επόμενα, όταν δεν αναφέρεται ρητώς το σώμα από το οποίο προέρχονται οι συντελεστές ενός πολυωνύμου θα θεωρούμε ότι αυτό είναι το μικρότερο δυνατό σώμα δηλαδή, το $\mathbb{Q}$.

Ορισμένα Στοιχεία από την Θεωρία Διαιρετότητας Πολυωνύμων

§7. Από την εμπειρία μας κατά την διαδικασία επίλυσης πολυωνυμικών εξισώσεων, είναι πολύ χρήσιμο να μπορούμε να γράψουμε το πολυώνυμο της εξίσωσης ως γινόμενο άλλων πολυωνύμων βαθμού μικρότερου του βαθμού του αρχικού πολυωνύμου που μας δόθηκε. Αυτό γίνεται παραγοντοποιώντας το αρχικό πολυώνυμο σε γινόμενο πολυωνύμων με συντελεστές από το σώμα προέλευσης των συντελεστών του αρχικού πολυωνύμου. Κάποιες φορές όμως αυτό δεν γίνεται.

Όλα αυτά οδηγούν σε μία δεύτερη δέσμη απαραίτητων αλγεβρικών εννοιών που πρέπει να εισαχθούν, σε σχέση με το προς διερεύνηση αντικείμενο.

Αυτές οι έννοιες αφορούν μέρος της θεωρίας διαιρετότητας πολυωνύμων και παρουσιάζονται στις επόμενες ενότητες.

§8. Κάθε σύνολο R τα στοιχεία του οποίου ικανοποιούν τις ιδιότητες (I1–I6) καθώς και τις ιδιότητες (I8–I9) της §2, λέγεται μεταθετικός δακτύλιος με μονάδα.

Δηλαδή, ένας μεταθετικός δακτύλιος με μονάδα έχει τις ιδιότητες ενός σώματος εκτός από αυτήν της ύπαρξης αντιστρόφου για κάθε μη μηδενικό στοιχείο του. Μπορεί κάποια μη μηδενικά στοιχεία ενός μεταθετικού δακτυλίου με μονάδα να έχουν αντίστροφο. Δεν μπορεί όμως όλα τα μη μηδενικά στοιχεία ενός μεταθετικού δακτυλίου με μονάδα να έχουν αντίστροφο. Π.χ., τα στοιχεία 1, -1 ενός μεταθετικού δακτυλίου με μονάδα έχουν αντίστροφο τα 1, -1 αντιστοίχως. Κλασικό παράδειγμα μεταθετικού δακτυλίου με μονάδα είναι το σύνολο των ακεραίων $\mathbb{Z}$.

§9. Έστω σώμα F. Θεωρούμε το σύνολο $F[x]$ των πολυωνύμων με συντελεστές από το F δηλαδή, $F[x] = \left\{\sum_{k=0}^{n} a_k\, x^k \,:\, a_k \in F,\ n \in \mathbb{N}\right\}$, όπου το κενό στο $a_k\, x^k$ σημαίνει τον πολλαπλασιασμό του σώματος F ή του σώματος $K \supseteq F$ όταν το x λάβει τιμή από το F ή το K αντιστοίχως. Ομοίως και για την πρόσθεση των μονωνύμων του πολυωνύμου δηλαδή, είναι η πρόσθεση του σώματος F ή του σώματος $K \supseteq F$ όταν το x λάβει τιμή από το F ή το K αντιστοίχως.

Το $F[x]$ εφοδιασμένο με τις γνωστές μας πράξεις της πρόσθεσης και του πολλαπλασιασμού πολυωνύμων είναι μεταθετικός δακτύλιος με μονάδα. Η επαλήθευση ότι τα στοιχεία του $F[x]$ ικανοποιούν τις ιδιότητες (I1–I6) καθώς και τις ιδιότητες (I8–I9) της §2, προκύπτει άμεσα από το γεγονός ότι οι συντελεστές των πολυωνύμων ανήκουν σε σώμα και από τον τρόπο ορισμού της γνωστή μας πρόσθεσης και του γνωστού μας πολλαπλασιασμού πολυωνύμων.

§10. Όπως στο $\mathbb{Z}$ έτσι και στον δακτύλιο $F[x]$ μπορεί να αναπτυχθεί μία θεωρία διαιρετότητας μεταξύ των στοιχείων του.

- **Έστω $\mathbf{a(x) \in F[x]}$, $\mathbf{b(x) \in F[x] - \{0\}}$. Λέμε ότι το $\mathbf{b(x)}$ διαιρεί το $\mathbf{a(x)}$, (στο $\mathbf{F[x]}$), αν υπάρχει $\mathbf{q(x) \in F[x]}$ ώστε $\mathbf{a(x) = b(x)\, q(x)}$.**

  Όταν $K \supseteq F$ σώμα, και το $b(x)$ διαιρεί το $a(x)$ στο $F[x]$ είναι προφανές ότι το διαιρεί και στο $K[x]$ γιατί $a(x), b(x), q(x) \in F[x] \subseteq K[x]$.

- **Έστω $\mathbf{a_1(x), \ldots, a_n(x) \in F[x]}$. Το $\mathbf{q(x) \in F[x]}$ λέγεται κοινός διαιρέτης των $\mathbf{a_1(x), \ldots, a_n(x)}$ αν διαιρεί κάθε ένα από αυτά.**

- **Έστω $\mathbf{a_1(x), \ldots, a_n(x) \in F[x]}$. Ο κοινός τους διαιρέτης $\mathbf{q(x) \in F[x]}$ λέγεται μέγιστος κοινός διαιρέτης αν διαιρείται από κάθε κοινό διαιρέτη των $\mathbf{a_1(x), \ldots, a_n(x) \in F[x]}$.**

§11. Έστω $\mathbf{p_1(x)}$, $\mathbf{p_2(x) \in F[x]}$. $\mathbf{d(x) \in F[x]}$ μέγιστος κοινός διαιρέτης των $\mathbf{p_1(x)}$, $\mathbf{p_2(x)}$. Κάθε άλλος μέγιστος κοινός διαιρέτης $\mathbf{u(x) \in F[x]}$ των $\mathbf{p_1(x)}$, $\mathbf{p_2(x)}$ γράφεται ως $\mathbf{u(x) = a\, d(x)}$, $\mathbf{a \in F - \{0\}}$. Αντιστρόφως, για κάθε $\mathbf{a \in F - \{0\}}$ το $\mathbf{u(x) = a\, d(x)}$ είναι μέγιστος κοινός διαιρέτης των $\mathbf{p_1(x)}$, $\mathbf{p_2(x)}$.

Έστω $u(x)$ ένας μέγιστος κοινός διαιρέτης των $p_1(x)$, $p_2(x)$ διαφορετικός του $d(x)$. Τότε, ο $d(x)$ σαν μέγιστος κοινός διαιρέτης των $p_1(x)$, $p_2(x)$ είναι και κοινός διαιρέτης τους και άρα διαιρεί τον μέγιστο κοινό τους διαιρέτη $u(x)$. Δηλαδή, υπάρχει $b(x) \in F[x]$ ώστε $u(x) = d(x)\, b(x)$. Ομοίως, ο $u(x)$ είναι και κοινός διαιρέτης των $p_1(x)$, $p_2(x)$ άρα διαιρεί τον μέγιστο κοινό τους διαιρέτη $d(x)$. Δηλαδή, υπάρχει $k(x) \in F[x]$ ώστε $d(x) = u(x)\, k(x)$. Άρα, $u(x) = d(x)\, b(x) = u(x)\, (k(x)\, b(x))$ ή $u(x)\, (1 - k(x)\, b(x)) = 0$.

Όμως, $u(x) \neq 0$ ως διαιρέτης των $p_1(x)$, $p_2(x)$. Άρα, $k(x)\, b(x) = 1$. Τα μόνα αντιστρέψιμα στοιχεία του δακτυλίου πολυωνύμων $F[x]$ είναι τα μη μηδενικά σταθερά πολυώνυμα. Οπότε, τα $k(x)$, $b(x)$ είναι μη μηδενικά σταθερά πολυώνυμα του $F[x]$. Θέτοντας $b(x) = a \in F - \{0\}$ το συμπέρασμα προκύπτει.

Έστω $u(x) = a\, d(x)$ για $a \in F - \{0\}$. Το $a\, d(x)$ διαιρεί τα $p_1(x)$, $p_2(x)$ αφού μπορούμε να γράψουμε, $p_1(x) = (a\, d(x))\, (a^{-1}\, q_1(x))$ και $p_2(x) = (a\, d(x))$ $(a^{-1}\, q_2(x))$ όπου $q_1(x)$, $q_2(x)$ τα πηλίκα της διαίρεσης των $p_1(x)$, $p_2(x)$ με το $d(x)$ αντιστοίχως. Άρα το $a\, d(x)$ είναι κοινός διαιρέτης των $p_1(x)$, $p_2(x)$. Κάθε κοινός διαιρέτης των $p_1(x)$, $p_2(x)$ διαιρεί τον μέγιστο κοινό διαιρέτη τους $d(x)$ άρα, και το $a\, d(x)$. Το συμπέρασμα προκύπτει.

Το ίδιο συμπέρασμα ισχύει και για τους μέγιστους κοινούς διαιρέτες οιουδήποτε πεπερασμένου πλήθους πολυωνύμων.

§12. Όπως στο $\mathbb{Z}$ έτσι και στον δακτύλιο $F[x]$ μπορεί να αποδειχθεί ότι υπάρχει Ευκλείδεια διαίρεση μεταξύ των στοιχείων του.

Έστω $\mathbf{a(x) \in F[x],\ \ b(x) \in F[x] - \{0\}}$. Υπάρχουν μοναδικά $\mathbf{q(x)}$, (πηλίκο), $\mathbf{r(x)}$, (υπόλοιπο), $\in \mathbf{F[x]}$ τέτοια ώστε, $\mathbf{a(x) = b(x)\, q(x) + r(x)}$ και είτε $\mathbf{r(x) = 0}$, είτε $\mathbf{deg[r(x)] < deg[b(x)]}$, όπου deg συμβολίζει τον βαθμό ενός πολυωνύμου.

Πρώτα αποδεικνύουμε την ύπαρξη των $q(x)$ και $r(x)$. Έστω $a(x) = 0$. Τότε $a(x) = b(x)\, 0 + 0$ με $q(x) = 0$, $r(x) = 0$.

Έστω $a(x) \neq 0$. Αν $deg[a(x)] < deg[b(x)]$ τότε μπορούμε να γράψουμε, $a(x) = b(x)\, 0 + a(x)$ με $q(x) = 0$, $r(x) = a(x)$ και $deg[r(x)] = deg[a(x)] < deg[b(x)]$.

Αν $deg[a(x)] \geq deg[b(x)]$ θα προχωρήσουμε εφαρμόζοντας επαγωγή στον βαθμό του $a(x)$. Αν $deg[a(x)] = 0$ τότε και $deg[b(x)] = 0$ και τα $a(x)$, $b(x)$ είναι μη μηδενικά σταθερά πολυώνυμα έστω $a(x) = a \in F - \{0\}$, $b(x) = b \in F - \{0\}$. Μπορούμε να γράψουμε, $a = b\, (b^{-1}\, a) + 0$ με $q(x) = b^{-1}\, a$ και $r(x) = 0$. Έστω $n \in \mathbb{N} - \{0\}$. Υποθέτουμε ότι το προς απόδειξη συμπέρασμα ισχύει για κάθε πολυώνυμο $a(x)$ με $deg[a(x)] < n$. Θα δείξουμε ότι αυτό ισχύει και για τα πολυώνυμα $a(x)$ με $deg[a(x)] = n$.

Έστω $a(x) = \sum_{k=0}^{n} a_k\, x^k$, $b(x) = \sum_{k=0}^{m} b_k\, x^k$, $n \geq m$. Οι συντελεστές a_n, b_m των μεγιστοβάθμιων όρων των $a(x)$, $b(x)$ είναι μη μηδενικά στοιχεία του σώματος F αλλιώς τα $a(x)$, $b(x)$ δεν θα ήταν βαθμού n, m αντιστοίχως. Θεωρούμε το πολυώνυμο $g(x) = a(x) - (a_n/b_m)\, x^{n-m}\, b(x)$. Από την κατασκευή του $g(x)$ προκύπτει ότι $deg[g(x)] < deg[a(x)] = n$. Άρα, από την υπόθεση της επαγωγής υπάρχουν $Q(x)$, $R(x)$ τέτοια άστε $g(x) = b(x)\, Q(x) + R(x)$ και είτε $R(x) = 0$, είτε $deg[R(x)] < deg[b(x)]$. Δηλαδή,

$$a(x) - \frac{a_n}{b_m}\, x^{n-m}\, b(x) = b(x)\, Q(x) + R(x) \Leftrightarrow$$

$$a(x) = b(x)\left(\frac{a_n}{b_m}\,x^{n-m} + Q(x)\right) + R(x),$$

και το συμπέρασμα ισχύει για $q(x) = \left(\frac{a_n}{b_m}\,x^{n-m} + Q(x)\right)$, $r(x) = R(x)$ και είτε $r(x) = R(x) = 0$, είτε $deg[r(x)] = deg[R(x)] < deg[b(x)]$.

Τώρα θα δείξουμε την μοναδικότητα των $q(x)$, $r(x)$. Έστω ότι υπάρχουν $q_1(x)$, $q_2(x)$, $r_1(x)$, $r_2(x)$ τέτοια ώστε,

$$\begin{aligned} a(x) &= b(x)\,q_1(x) + r_1(x) \quad , \quad \text{και είτε } r_1(x) = 0, \text{ είτε } deg[r_1(x)] < deg[b(x)], \\ a(x) &= b(x)\,q_2(x) + r_2(x) \quad , \quad \text{και είτε } r_2(x) = 0, \text{ είτε } deg[r_2(x)] < deg[b(x)]. \end{aligned}$$

Τότε, αφαιρώντας τις πιο πάνω ισότητες κατά μέλη λαμβάνουμε, $r_2(x) - r_1(x) = b(x)\,[q_1(x) - q_2(x)]$. Η τελευταία ισότητα συνεπάγεται ότι το $b(x)$ διαιρεί το $r_2(x) - r_1(x)$ του οποίου ο βαθμός είναι μικρότερος από τον βαθμό του $b(x)$. Για να συμβεί αυτό πρέπει $r_2(x) - r_1(x) = 0$. Άρα, $r_2(x) = r_1(x)$. Το τελευταίο συμπέρασμα και οι πιο πάνω ισότητες συνεπάγονται ότι $b(x)\,q_1(x) = b(x)\,q_2(x)$ δηλαδή, $q_1(x) = q_2(x)$.

Ένας ακόμη σημαντικός λόγος, (πέραν αυτού που αναφέραμε στην §1), επιλογής των συντελεστών των πολυωνύμων να προέρχονται από σώμα προκύπτει από την πιο πάνω απόδειξη ύπαρξης Ευκλείδειας διαίρεσης στο $\mathbf{F[x]}$. Αν οι συντελεστές $\mathbf{a_n}$, $\mathbf{b_m}$ δεν προέρχονταν από σώμα, δεν θα μπορούσαμε να γράψουμε $\mathbf{a_n/b_m}$ στην απόδειξη που προηγήθηκε και έτσι δεν θα μπορούσαμε να θεμελιώσουμε Ευκλείδεια διαίρεση μεταξύ πολυωνύμων.

§13. Έστω $\mathbf{p_1(x),\ p_2(x) \in F[x]}$. Υπάρχουν $\mathbf{u(x), a_1(x), a_2(x) \in F[x]}$ τέτοια ώστε $\mathbf{a_1(x)\,p_1(x) + a_2(x)\,p_2(x) = u(x)}$ και το $\mathbf{u(x)}$ είναι μέγιστος κοινός διαιρέτης των $\mathbf{p_1(x), p_2(x)}$.

Αν $p_2(x) = 0$ τότε ο μέγιστος κοινός διαιρέτης των $p_1(x)$, $p_2(x)$ είναι το $p_1(x)$ και το συμπέρασμα ισχύει για $u(x) = p_1(x)$, $a_1(x) = 1$, $a_2(x) = 0$.

Αν $p_2(x) \neq 0$ τότε εφαρμόζοντας επαναληπτικώς την ταυτότητα της Ευκλείδειας διαίρεσης πολυωνύμων της §12 λαμβάνουμε,

$$\begin{aligned} p_1(x) &= p_2(x)\,q_1(x) + r_1(x),\ r_1(x) = 0 \text{ ή } deg[r_1(x)] < deg[p_2(x)], && (E1) \\ p_2(x) &= r_1(x)\,q_2(x) + r_2(x),\ r_2(x) = 0 \text{ ή } deg[r_2(x)] < deg[r_1(x)], && (E2) \\ r_1(x) &= r_2(x)\,q_3(x) + r_3(x),\ r_3(x) = 0 \text{ ή } deg[r_3(x)] < deg[r_2(x)], && (E3) \\ &\vdots \\ r_{n-2}(x) &= r_{n-1}(x)\,q_n(x) + r_n(x),\ r_n(x) = 0 \text{ ή } deg[r_n(x)] < deg[r_{n-1}(x)], && (En) \\ r_{n-1}(x) &= r_n(x)\,q_{n+1}(x) + r_{n+1}(x),\ r_{n+1}(x) = 0 \text{ ή} \\ &\qquad deg[r_{n+1}(x)] < deg[r_n(x)]. && (En+1) \end{aligned}$$

Επειδή όμως ο $deg[p_2(x)]$ είναι πεπερασμένος φυσικός αριθμός, η γνησίως φθίνουσα ακολουθία φυσικών αριθμών,

$$deg[p_2(x)] > deg[r_1(x)] > deg[r_2(x)] > \cdots > deg[r_n(x)] > deg[r_{n+1}(x)], \quad (10)$$

δεν έχει άπειρο πλήθος όρων αλλά πεπερασμένο. Υπάρχει $n \in \mathbb{N} - \{0\}$ ώστε το $r_{n+1}(x) = 0$ αλλιώς, αν $r_{n+1}(x) \neq 0$ θα ορίζετε βαθμός για το $r_{n+1}(x)$ και

η διαδικασία που περιγράφεται στις (E1)–(E$n+1$) θα παράξει ένα $r_{n+2}(x)$ με $deg[r_{n+2}(x)] < deg[r_{n+1}(x)]$ και με αυτόν τον τρόπο η ακολουθία (10) θα συνεχίζεται επ΄ άπειρον. Άρα, για κάποιο $n \in \mathbb{N} - \{0\}$ η διαδικασία που περιγράφεται στις (E1)–(E$n+1$) παράγει $r_{n+1}(x) = 0$.

Θα δείξουμε ότι το $r_n(x)$, (το τελευταίο μη μηδενικό υπόλοιπο της διαδικασίας (E1)–(E$n+1$)), είναι μέγιστος κοινός διαιρέτης των $p_1(x)$, $p_2(x)$. Αφού $r_{n+1}(x) = 0$, η (E$n+1$) επάγει $r_{n-1}(x) = r_n(x)\, q_{n+1}(x)$ και το $r_n(x)$ διαιρεί το $r_{n-1}(x)$ και άρα διαιρεί το άθροισμα $r_{n-1}(x)\, q_n(x) + r_n(x)$. Η (E$n$) επάγει ότι το $r_n(x)$ διαιρεί το $r_{n-2}(x)$. Συνεχίζοντας την διαδικασία αυτή αντιστρόφως από την (E$n+1$) έως την (E1) προκύπτει ότι το $r_n(x)$ διαιρεί τα $p_1(x)$ και $p_2(x)$ είναι δηλαδή κοινός διαιρέτης τους.

Έστω τώρα $d(x) \in F[x]$ ένας κοινός διαιρέτης των $p_1(x)$, $p_2(x)$ διαφορετικός του $r_n(x)$. Το $d(x)$ διαιρεί την διαφορά $p_1(x) - p_2(x)\, q_1(x)$. Η (E1) επάγει ότι το $d(x)$ διαιρεί και το $r_1(x)$. Το $d(x)$ διαιρεί την διαφορά $p_2(x) - r_1(x)\, q_2(x)$. Η (E2) επάγει ότι το $d(x)$ διαιρεί και το $r_2(x)$. Συνεχίζοντας την διαδικασία αυτή από την (E1)–(En) προκύπτει ότι το $d(x)$ διαιρεί και το $r_n(x)$. Άρα, κάθε κοινός διαιρέτης των $p_1(x)$, $p_2(x)$ διαιρεί το $r_n(x)$ και αυτό είναι μέγιστος κοινός διαιρέτης των $p_1(x)$, $p_2(x)$. Γράφοντας εκ΄ νέου της εξισώσεις (E1)–(E$n+1$) με την βοήθεια τετραγωνικών πινάκων διάστασης 2 λαμβάνουμε,

$$\begin{aligned}
\begin{pmatrix} p_1(x) \\ p_2(x) \end{pmatrix} &= \begin{pmatrix} q_1(x) & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p_2(x) \\ r_1(x) \end{pmatrix}, \text{ από την εξίσωση } (E1) \\
\begin{pmatrix} p_2(x) \\ r_1(x) \end{pmatrix} &= \begin{pmatrix} q_2(x) & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_1(x) \\ r_2(x) \end{pmatrix}, \text{ από την εξίσωση } (E2) \\
\begin{pmatrix} r_1(x) \\ r_2(x) \end{pmatrix} &= \begin{pmatrix} q_3(x) & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_2(x) \\ r_3(x) \end{pmatrix}, \text{ από την εξίσωση } (E3) \\
&\vdots \\
\begin{pmatrix} r_{n-2}(x) \\ r_{n-1}(x) \end{pmatrix} &= \begin{pmatrix} q_n(x) & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{n-1}(x) \\ r_n(x) \end{pmatrix}, \text{ από την εξίσωση } (En) \\
\begin{pmatrix} r_{n-1}(x) \\ r_n(x) \end{pmatrix} &= \begin{pmatrix} q_{n+1}(x) & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_n(x) \\ r_{n+1}(x) \end{pmatrix} = \\
&= \begin{pmatrix} q_{n+1}(x) & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_n(x) \\ 0 \end{pmatrix}, \text{ από την εξίσωση } (En+1)
\end{aligned}$$

Αντικαθιστώντας το πρώτο μέλος της εξίσωσης (Ei) στο δεύτερο μέλος της εξίσωσης (E$i-1$), $i = n+1, n, \ldots, 2$ λαμβάνουμε,

$$\begin{pmatrix} p_1(x) \\ p_2(x) \end{pmatrix} = \begin{pmatrix} q_1(x) & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2(x) & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_{n+1}(x) & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_n(x) \\ 0 \end{pmatrix} \tag{11}$$

Όμως, κάθε πίνακας,

$$\begin{pmatrix} q_i(x) & 1 \\ 1 & 0 \end{pmatrix}, \; i = 1, 2, \ldots, n+1,$$

έχει αντίστροφο τον,

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_i(x) \end{pmatrix},\ i = 1, 2, \ldots, n+1. \tag{12}$$

οπότε, πολλαπλασιάζοντας την (11) από αριστερά διαδοχικά με τους πίνακες (12) προκύπτει,

$$\begin{aligned} \begin{pmatrix} r_n(x) \\ 0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & -q_{n+1}(x) \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_2(x) \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_1(x) \end{pmatrix} \begin{pmatrix} p_1(x) \\ p_2(x) \end{pmatrix} \\ &= \begin{pmatrix} u_1(x) & u_2(x) \\ u_3(x) & u_4(x) \end{pmatrix} \begin{pmatrix} p_1(x) \\ p_2(x) \end{pmatrix},\ u_i(x) \in F[x], i = 1, 2, 3, 4. \end{aligned} \tag{13}$$

Η (13) συνεπάγεται ότι $u_1(x)\, p_1(x) + u_2(x)\, p_2(x) = r_n(x)$ και το προς απόδειξη συμπέρασμα ισχύει για $a_1(x) = u_1(x)$, $a_2(x) = u_2(x)$, $u(x) = r_n(x)$.

§14. Από την §13 προκύπτει ότι η εύρεση του μέγιστου κοινού διαιρέτη δύο και κατ΄ αναλογία ενός πλήθους πολυωνύμων γίνεται με εφαρμογή του αλγόριθμου της Ευκλείδειας διαίρεσης. Η συγκεκριμένη ταυτότητα, παράγει αποτελέσματα μέσω προσθέσεων, αφαιρέσεων, πολλαπλασιασμών και διαιρέσεων μεταξύ των συντελεστών των εμπλεκομένων πολυωνύμων. Αν οι συντελεστές αυτοί ανήκουν στο ίδιο σώμα F, τότε και τα πολυώνυμα που προκύπτουν ως αποτελέσματα, έχουν συντελεστές στο F.

Αν οι συντελεστές των εμπλεκομένων πολυωνύμων ανήκουν σε διαφορετικά σώματα, αυτοί υποχρεωτικά πρέπει να ανήκουν στην μη κενή τομή αυτών των σωμάτων, (που και αυτή είναι σώμα), αλλιώς προσθέσεις, αφαιρέσεις, πολλαπλασιασμοί και διαιρέσεις μεταξύ τους δεν μπορούν να συμβούν και η ταυτότητα της Ευκλείδειας διαίρεσης δεν εφαρμόζεται.

Ένα πολυώνυμο $f(x)$ του $F[x]$ είναι και πολυώνυμο του $K[x]$ όταν $K \supseteq F$. Αυτό γιατί, οι συντελεστές του $f(x)$ ως στοιχεία του F είναι και στοιχεία του K. Αν τώρα $f(x)$ και $g(x)$ είναι πολυώνυμα του $F[x]$ από όσα προαναφέραμε, και ο μέγιστος κοινός τους διαιρέτης $d(x)$ θα είναι πολυώνυμο του $F[x]$ δηλαδή, οι συντελεστές του θα περιέχονται στο ελάχιστο σώμα που περιέχει τους συντελεστές των $f(x)$ και $g(x)$.

Για κάθε σώμα $K \supseteq F$ ο μέγιστος κοινός διαιρέτης των $f(x)$, $g(x)$ αν τα δούμε ως πολυώνυμα του $K[x] \supseteq F[x]$ είναι εκ΄ νέου ο $d(x)$. Δεν έχει σημασία αν βλέπουμε τα $f(x)$, $g(x)$ ως πολυώνυμα πολύ ευρύτερων $K[x]$ σε σχέση με τον $F[x]$. Εφ΄ όσον οι συντελεστές των $f(x)$, $g(x)$ προέρχονται από το μικρότερο F σε σχέση με το μεγαλύτερο K, οι προσθέσεις, αφαιρέσεις, πολλαπλασιασμοί και διαιρέσεις μεταξύ των συντελεστών αυτών είναι πράξεις μεταξύ στοιχείων του F και τα αποτελέσματα ανήκουν στο F. Συμπερασματικά,

Αν $\mathbf{f(x), g(x) \in F[x]}$ έχουν μέγιστο κοινό διαιρέτη $\mathbf{d(x)}$, τότε $\mathbf{d(x) \in F[x]}$ και το $\mathbf{d(x)}$ είναι ο μέγιστος κοινός διαιρέτης των $\mathbf{f(x), g(x)}$ αν τα δούμε και ως πολυώνυμα οιουδήποτε $\mathbf{K[x]}$ με $\mathbf{K \supseteq F}$.

§15. Έστω $\mathbf{p_1(x), p_2(x) \in F[x]}$. Λέμε ότι αυτά είναι πρώτα μεταξύ τους όταν ένας μέγιστος κοινός διαιρέτης τους είναι στοιχείο του $\mathbf{F - \{0\}}$.

Έστω ότι τα $p_1(x)$, $p_2(x)$ είναι πρώτα μεταξύ τους. Έστω $b \in F - \{0\}$ ένας μέγιστος κοινός διαιρέτης τους. Από την §13 μπορούμε να γράψουμε,

$$a_1(x)\,p_1(x) + a_2(x)\,p_2(x) = b,$$

με $a_1(x)$, $a_2(x) \in F[x]$. Τότε και

$$(b^{-1}\,a_1(x))\,p_1(x) + (b^{-1}\,a_2(x))\,p_2(x) = 1.$$

Άρα, όταν τα $p_1(x)$, $p_2(x)$ είναι πρώτα μεταξύ τους υπάρχουν $b_1(x)$, $b_2(x) \in F[x]$ ώστε $b_1(x)\,p_1(x) + b_2(x)\,p_2(x) = 1$. Αντιστρόφως, έστω ότι υπάρχουν $b_1(x)$, $b_2(x) \in F[x]$ ώστε,

$$b_1(x)\,p_1(x) + b_2(x)\,p_2(x) = 1.$$

Τότε κάθε μέγιστος κοινός διαιρέτης των $p_1(x)$, $p_2(x)$ π.χ. το $d(x)$ διαιρεί το άθροισμα $b_1(x)\,p_1(x) + b_2(x)\,p_2(x)$ άρα διαιρεί και το 1. Αυτό σημαίνει ότι $1 = d(x)\,k(x)$ με $k(x) \in F[x]$. Τα μόνα αντιστρέψιμα στοιχεία του δακτυλίου πολυωνύμων $F[x]$ είναι τα μη μηδενικά σταθερά πολυώνυμα. Άρα, το $d(x)$ είναι στοιχείο του $F - \{0\}$ και τα $p_1(x)$, $p_2(x)$ είναι πρώτα μεταξύ τους. Συμπέρασμα,

Έστω $\mathbf{p_1(x)}$, $\mathbf{p_2(x)} \in \mathbf{F[x]}$. Αυτά είναι πρώτα μεταξύ τους αν και μόνο αν υπάρχουν $\mathbf{b_1(x)}$, $\mathbf{b_2(x)} \in \mathbf{F[x]}$ ώστε,

$$\mathbf{b_1(x)\,p_1(x) + b_2(x)\,p_2(x) = 1}. \tag{14}$$

§16. Έστω $\mathbf{p(x)} \in \mathbf{F[x]}$, $\mathbf{K \supseteq F}$ σώμα, $\mathbf{s \in K}$. Το s λέγεται ρίζα του πολυωνύμου $\mathbf{p(x)}$ αν $\mathbf{p(s) = 0}$.

§17. Έστω $\mathbf{p(x)} \in \mathbf{F[x]}$, $\mathbf{K \supseteq F}$ σώμα. Το $\mathbf{s \in K}$ είναι ρίζα του $\mathbf{p(x)}$ αν και μόνο αν το $\mathbf{x - s}$ διαιρεί το $\mathbf{p(x)}$ στο $\mathbf{K[x]}$.

Έστω ότι το $s \in K$ είναι ρίζα του $p(x)$. Από την ταυτότητα της Ευκλείδειας διαίρεσης πολυωνύμων, (στο $K[x]$, §12), λαμβάνουμε ότι,

$$p(x) = (x - s)\,q(x) + r(x),$$

με $r(x) = 0$ είτε $deg[r(x)] < deg[x - s] = 1$. Αν $r(x) \neq 0$ τότε $deg[r(x)] < deg[x - s] = 1$ που συνεπάγεται ότι $deg[r(x)] = 0$ και το $r(x)$ είναι μη μηδενικό σταθερό πολυώνυμο δηλαδή, $r(x) = k \in K - \{0\}$. Όμως τότε παίρνουμε $p(s) = (s - s)\,q(s) + r(s)$ ή $0 = 0\,q(s) + k$ ή $0 = k$ άτοπο. Άρα, $r(x) = 0$ και $p(x) = (x - s)\,q(x)$.

Αντιστρόφως, αν το $x - s$ διαιρεί το $p(x)$ στο $K[x]$ παίρνουμε ότι $p(x) = (x - s)\,q(x)$ με $q(x) \in K[x]$ και $p(s) = (s - s)\,q(s) = 0$. Το s είναι ρίζα του $p(x)$.

§18. Έστω $\mathbf{p(x) = \sum_{k=0}^{n} a_k\,x^k} \in \mathbf{F[x]}$. Ορίζουμε ως πρώτη παράγωγο του $\mathbf{p(x)}$ το πολυώνυμο $\mathbf{p'(x) = 0}$ αν $\mathbf{n = 0}$ ή $\mathbf{p(x) = 0}$, ενώ το πολυώνυμο $\mathbf{p'(x) = \sum_{k=1}^{n} k\,a_k\,x^{k-1}} \in \mathbf{F[x]}$ αν $\mathbf{n \in \mathbb{N} - \{0\}}$.

§19. Έστω $\mathbf{a(x) = \sum_{k=0}^{n} a_k\,x^k} \in \mathbf{F[x]}$, $\mathbf{b(x) = \sum_{k=0}^{m} b_k\,x^k} \in \mathbf{F[x]}$, $\mathbf{n \geq m}$. Η πρώτη παράγωγος πολυωνύμων ικανοποιεί τις ιδιότητες,

- $\mathbf{(a(x) + b(x))' = a'(x) + b'(x)}$,
- $\mathbf{(a(x)\,b(x))' = a'(x)\,b(x) + a(x)\,b'(x)}$.

$$(a(x)+b(x))' = \left(\sum_{k=m+1}^{n} a_k\,x^k + \sum_{k=0}^{m}(a_k+b_k)\,x^k\right)' = \left(\sum_{k=0}^{n} c_k\,x^k\right)' =$$

$$= \sum_{k=1}^{n} k\,c_k\,x^{k-1} = \sum_{k=m+1}^{n} k\,a_k\,x^{k-1} + \sum_{k=1}^{m} k\,(a_k+b_k)\,x^{k-1}, \quad (15)$$

$$a'(x) = \sum_{k=1}^{n} k\,a_k\,x^{k-1},$$

$$b'(x) = \sum_{k=1}^{m} k\,b_k\,x^{k-1},$$

$$a'(x)+b'(x) = \sum_{k=1}^{n} k\,a_k\,x^{k-1} + \sum_{k=1}^{m} k\,b_k\,x^{k-1} =$$

$$= \sum_{k=m+1}^{n} k\,a_k\,x^{k-1} + \sum_{k=1}^{m} k\,(a_k+b_k)\,x^{k-1}. \quad (16)$$

Από τις (15), (16) προκύπτει η ζητούμενη ιδιότητα.

Αν $n=0$ τότε $a(x)=a_0\in F-\{0\}$ σταθερό πολυώνυμο και επειδή $n\geq m$ και $m=0$, $b(x)=b_0\in F-\{0\}$ σταθερό πολυώνυμο. Τότε,

$$(a(x)\,b(x))' = (a_0\,b_0)' = 0 = 0\,b(x) + a(x)\,0 = a'(x)\,b(x) + a(x)\,b'(x).$$

Έστω $n\geq 1$. Θα προχωρήσουμε με επαγωγή στο πλήθος των όρων του $a(x)$. Αν το $a(x)$ αποτελείται από έναν όρο τότε $a(x)=a_h\,x^h$ για κάποιο $h\in\mathbb{N}-\{0\}$, (αν $h=0$ τότε $a(x)=a_0$ και αναγόμεθα στην προηγούμενη περίπτωση). Επίσης, $a_h\neq 0$ αλλιώς $a(x)=0$ που είναι τετριμμένη περίπτωση.

$$(a(x)\,b(x))' = \left(\sum_{k=0}^{m} a_h\,b_k\,x^{h+k}\right)' = \sum_{k=0}^{m}(h+k)\,a_h\,b_k\,x^{h+k-1}, \quad (17)$$

$$a'(x)\,b(x) = h\,a_h\,x^{h-1}\sum_{k=0}^{m} b_k\,x^k = \sum_{k=0}^{m} h\,a_h\,b_k\,x^{h+k-1}, \quad (18)$$

$$a(x)\,b'(x) = a_h\,x^h\sum_{k=1}^{m} k\,b_k\,x^{k-1} = \sum_{k=1}^{m} k\,a_h\,b_k\,x^{h+k-1} =$$

$$= \sum_{k=0}^{m} k\,a_h\,b_k\,x^{h+k-1}, \quad (19)$$

$$a'(x)\,b(x)+a(x)\,b'(x) \overset{(18,19)}{=} \sum_{k=0}^{m} h\,a_h\,b_k\,x^{h+k-1} + \sum_{k=0}^{m} k\,a_h\,b_k\,x^{h+k-1} =$$

$$= \sum_{k=0}^{m}(h+k)\,a_h\,b_k\,x^{h+k-1}. \quad (20)$$

Από τις (17), (20) προκύπτει ότι $(a(x)\,b(x))' = a'(x)\,b(x)+a(x)\,b'(x)$. Δείξαμε ότι η ζητούμενη ιδιότητα ισχύει για κάθε πολυώνυμο $a(x)$ που έχει έναν όρο. Υποθέτουμε ότι η ζητούμενη ιδιότητα ισχύει για κάθε πολυώνυμο $a(x)$ που έχει $n\geq 1$ όρους. Θα δείξουμε ότι αυτή ισχύει και για κάθε πολυώνυμο $a(x)$ που έχει $n+1$ όρους.

Έστω $a(x)=\sum_{k=0}^{n} a_k\,x^k = a_n\,x^n+g(x)$ όπου $g(x)$ ένα πολυώνυμο του $F[x]$ που έχει n όρους. Τότε,

$$\begin{aligned}(a(x)\,b(x))' &= ((a_n\,x^n+g(x))\,b(x))' = (a_n\,x^n\,b(x)+g(x)\,b(x))' = \\ &= (a_n\,x^n\,b(x))'+(g(x)\,b(x))'. \end{aligned} \tag{21}$$

Όμως το $a_n\,x^n$ έχει έναν όρο. Από τα προηγούμενα,

$$(a_n\,x^n\,b(x))' = (a_n\,x^n)'\;b(x)+a_n\,x^n\,b'(x). \tag{22}$$

Το $g(x)$ έχει n όρους. Από την υπόθεση της επαγωγής,

$$(g(x)\,b(x))' = g'(x)\,b(x)+g(x)\,b'(x). \tag{23}$$

Η (21) λόγω των (22), (23) δίνει,

$$\begin{aligned}(a(x)\,b(x))' &= (a_n\,x^n)'\;b(x)+a_n\,x^n\,b'(x)+g'(x)\,b(x)+g(x)\,b'(x) = \\ &= (a_n\,x^n+g(x))'\;b(x)+(a_n\,x^n+g(x))\;b'(x) = \\ &= a'(x)\,b(x)+a(x)\,b'(x),\end{aligned}$$

και η ζητούμενη ιδιότητα απεδείχθη.

§20. Έστω $\mathbf{p_1(x), p_2(x), q(x)\in F[x]}$, τέτοια ώστε το $\mathbf{q(x)}$ να διαιρεί το γινόμενο $\mathbf{p_1(x)\,p_2(x)}$ και τα $\mathbf{p_1(x)}$, $\mathbf{q(x)}$ να είναι πρώτα μεταξύ τους. Τότε το $\mathbf{q(x)}$ διαιρεί το $\mathbf{p_2(x)}$.

Αφού τα $p_1(x)$, $q(x)$ είναι πρώτα μεταξύ τους τότε από την §15 σχέση (14) λαμβάνουμε,

$$\begin{aligned} b_1(x)\,p_1(x)+b_2(x)\,q(x) &= 1 \Rightarrow \\ b_1(x)\,p_1(x)\,p_2(x)+b_2(x)\,p_2(x)\,q(x) &= p_2(x).\end{aligned}$$

Το $q(x)$ διαιρεί τα $p_1(x)\,p_2(x)$ και $p_2(x)\,q(x)$ άρα και το άθροισμα

$$b_1(x)\,p_1(x)\,p_2(x)+b_2(x)\,p_2(x)\,q(x),$$

οπότε και το $p_2(x)$.

§21. Έστω $\mathbf{p(x)\in F[x]}$, $\mathbf{m\in\mathbb{N}-\{0\}}$, $\mathbf{K\supseteq F}$ σώμα. Λέμε ότι το $\mathbf{s\in K}$ είναι ρίζα του $\mathbf{p(x)}$ πολλαπλότητας $\mathbf{m}$ αν το $\mathbf{(x-s)^m}$ διαιρεί το $\mathbf{p(x)}$ στο $\mathbf{K[x]}$.

§22. Έστω $\mathbf{p(x)\in F[x]}$, $\mathbf{K\supseteq F}$ σώμα, $\mathbf{s\in K}$ ρίζα του $\mathbf{p(x)}$ πολλαπλότητας $\mathbf{m\in\mathbb{N}-\{0\}}$. Τότε, αν $\mathbf{m=1}$ το $\mathbf{s}$ δεν είναι ρίζα του $\mathbf{p'(x)}$ ενώ αν $\mathbf{m>1}$ το $\mathbf{s}$ είναι ρίζα του $\mathbf{p'(x)}$ πολλαπλότητας $\mathbf{m-1}$.

Έστω ότι το s είναι ρίζα του $p(x)$ πολλαπλότητας $m=1$. Τότε, $p(x)=(x-s)\,q(x)$ με $q(x)\in K[x]$. $q(s)\neq 0$ αλλιώς, $q(x)=(x-s)\,a(x)$ με $a(x)\in K[x]$ και $p(x)=(x-s)\,q(x)=(x-s)^2\,a(x)$ επάγει ότι το s είναι ρίζα του $p(x)$ πολλαπλότητας 2, άτοπο. Τώρα, $p'(x)=((x-s)\,q(x))'=q(x)+(x-s)\,q'(x)$. Αν $p'(s)=0$ τότε, η προηγούμενη σχέση επάγει $q(s)=0$, άτοπο. Άρα το s δεν είναι ρίζα του $p'(x)$.

Έστω ότι το s είναι ρίζα του $p(x)$ πολλαπλότητας $m > 1$. Τότε, $p(x) = (x - s)^m\, q(x)$ με $q(x) \in K[x]$. $q(s) \neq 0$ αλλιώς, $q(x) = (x - s)\, a(x)$ με $a(x) \in K[x]$ και $p(x) = (x - s)^m\, q(x) = (x - s)^{m+1}\, a(x)$ επάγει ότι το s είναι ρίζα του $p(x)$ πολλαπλότητας $m + 1$, άτοπο. Τώρα,

$$\begin{aligned} p'(x) &= ((x - s)^m\, q(x))' = m\,(x - s)^{m-1}\, q(x) + (x - s)^m\, q'(x) = \\ &= (x - s)^{m-1}\,(m\, q(x) + (x - s)\, q'(x)) = \\ &= (x - s)^{m-1}\, b(x) \text{ με } b(x) \in K[x]. \end{aligned}$$

Το $b(s) \neq 0$ αλλιώς, $0 = b(s) = m\, q(s) + (s - s)\, q'(s) = m\, q(s)$ επάγοντας ότι $q(s) = 0$ άτοπο. Άρα το s είναι ρίζα του $p'(x)$ πολλαπλότητας $m - 1$.

§23. Έστω $\mathbf{p(x) \in F[x]}$, $\mathbf{K \supseteq F}$ σώμα, $\mathbf{s \in K}$ ρίζα του $\mathbf{p(x)}$ πολλαπλότητας $\mathbf{m \in \mathbb{N} - \{0, 1\}}$, $\mathbf{d(x) \in F[x]}$ ένας μέγιστος κοινός διαιρέτης των $\mathbf{p(x)}$, $\mathbf{p'(x)}$. Τότε το $\mathbf{s}$ είναι ρίζα του πολυωνύμου $\mathbf{p(x)/d(x)}$ πολλαπλότητας 1.

$$\begin{aligned} p(x) &= (x - s)^m\, q(x) \text{ με } q(x) \in K[x]. && (24) \\ p'(x) &= ((x - s)^m\, q(x))' = m\,(x - s)^{m-1}\, q(x) + (x - s)^m\, q'(x) = \\ &= (x - s)^{m-1}\,(m\, q(x) + (x - s)\, q'(x)) = \\ &= (x - s)^{m-1}\, b(x) \text{ με } b(x) \in K[x]. && (25) \end{aligned}$$

Το $q(s) \neq 0$ αλλιώς $q(x) = (x - s)\, g(x)$ με $g(x) \in K[x]$ και $p(x) = (x - s)^m\, q(x) = (x-s)^{m+1}\, g(x)$ επάγοντας ότι το s είναι ρίζα του $p(x)$ πολλαπλότητας $m + 1$, άτοπο. Από την §13 προκύπτει ότι ο μέγιστος κοινός διαιρέτης $d(x)$ των $p(x)$, $p'(x)$ μπορεί να γραφεί ως,

$$\begin{aligned} d(x) &= a_1(x)\, p(x) + a_2(x)\, p'(x) \overset{(24,25)}{=} \\ &= a_1(x)\,(x - s)^m\, q(x) + a_2(x)\,(x - s)^{m-1}\, b(x) = \\ &= (x - s)^{m-1}\,((x - s)\, a_1(x)\, q(x) + a_2(x)\, b(x)) = \\ &= (x - s)^{m-1}\, f(x), \end{aligned}$$

με $a_1(x), a_2(x) \in F[x] \subseteq K[x]$, $f(x) \in K[x]$. Αν το $f(s) = 0$ τότε $f(s) = (x-s)\, k(x)$ με $k(x) \in K[x]$ και $d(x) = (x-s)^{m-1}\, f(x) = (x-s)^m\, k(x)$. Επειδή, $p'(x) = d(x)\, h(x)$ με $h(x) \in F[x]$ παίρνουμε $p'(x) = (x - s)^m\, k(x)\, h(x)$ που επάγει ότι το s είναι ρίζα του $p'(x)$ πολλαπλότητας m, άτοπο από το συμπέρασμα της §22. Άρα $f(s) \neq 0$.

Το $p(x) = d(x)\, t(x)$ με $t(x) \in F[x]$. Οπότε, $(x-s)^m\, q(x) = (x-s)^{m-1}\, f(x)\, t(x)$ ή $(x - s)\, q(x) = f(x)\, t(x)$. Έστω $D(x) \in K[x]$ ένας μέγιστος κοινός διαιρέτης των $f(x)$, $x - s$. Τότε, $x - s = D(x)\, u(x)$ με $u(x) \in K[x]$. Η τελευταία σχέση επάγει ότι είτε $deg[D(x)] = 1$ είτε $deg[D(x)] = 0$. Στην πρώτη περίπτωση, $deg[u(x)] = 0$ και το $u(x)$ είναι ένα μη μηδενικό σταθερό πολυώνυμο του $K[x]$ δηλαδή, $u(x) = u \in K - \{0\}$. Οπότε, $D(x) = u^{-1}\,(x - s)$. Όμως, και $f(x) = D(x)\, w(x)$ με $w(x) \in K[x]$. Άρα, $f(x) = u^{-1}\,(x - s)\, w(x)$ που επάγει ότι το s είναι ρίζα του $f(x)$, άτοπο. Ισχύει ότι $deg[D(x)] = 0$ και το $D(x)$ είναι ένα μη μηδενικό πολυώνυμο του $K[x]$ δηλαδή, $D(x) = D \in K - \{0\}$. Ένας μέγιστος κοινός διαιρέτης των $f(x)$, $x - s$ είναι στοιχείο του $K - \{0\}$. Από την §15 προκύπτει ότι τα $f(x)$, $x - s$ είναι πρώτα μεταξύ τους.

Έχουμε ήδη δείξει ότι, $(x-s)\,q(x) = f(x)\,t(x)$. Άρα, το $f(x)$ διαιρεί το γινόμενο $(x-s)\,q(x)$ και είναι πρώτο με το $x-s$. Από την §20 το $f(x)$ διαιρεί το $q(x)$ δηλαδή, $q(x) = f(x)\,y(x)$ με $y(x) \in K[x]$. Αν $y(s) = 0$, τότε και $q(s) = f(s)\,y(s) = 0$, άτοπο. Οπότε, $y(s) \neq 0$. Το πολυώνυμο,

$$\frac{p(x)}{d(x)} = \frac{(x-s)^m\,q(x)}{(x-s)^{m-1}\,f(x)} = (x-s)\,\frac{f(x)\,y(x)}{f(x)} = (x-s)\,y(x),$$

επάγει ότι το s είναι ρίζα του $p(x)/d(x)$ πολλαπλότητας 1.

§24. Έστω $\mathbf{p(x) \in F[x]}$, $\mathbf{\deg[p(x)] \geq 1}$. Λέμε ότι το $\mathbf{p(x)}$ είναι ανάγωγο στο $\mathbf{F[x]}$ αν δεν υπάρχουν $\mathbf{a(x), b(x) \in F[x]}$ ώστε $\mathbf{\deg[a(x)] \geq 1}$, $\mathbf{\deg[b(x)] \geq 1}$ και $\mathbf{p(x) = a(x)\,b(x)}$. Στα επόμενα δεν θα τονίζουμε ιδιαίτερα ότι τα ανάγωγα πολυώνυμα έχουν υποχρεωτικώς βαθμό μεγαλύτερο ή ίσο του 1. Αυτό θα εννοείται.

§25. Υπάρχουν ορισμένα κριτήρια αναγωγιμότητας πολυωνύμων,

- **Αν $\mathbf{f(x) \in \mathbb{Z}[x]}$ είναι ανάγωγο στο $\mathbb{Z}[x]$, τότε είναι ανάγωγο στο $\mathbb{Q}[x]$.**

  Ανάγωγο στο $\mathbb{Z}[x]$ σημαίνει ότι αναφέρθηκε στην §24 με τον δακτύλιο $\mathbb{Z}$ στην θέση του σώματος F. Το κριτήριο αυτό υπάρχει στο [**9**] της βιβλιογραφίας, Θεώρημα 23.

- **Έστω $\mathbf{f(x) = \sum_{i=0}^{n} a_i\,x^i \in \mathbb{Z}[x]}$. Αν υπάρχει πρώτος αριθμός $\mathbf{p}$ ώστε ο $\mathbf{p}$ διαιρεί τα $\mathbf{a_0, a_1, \ldots, a_{n-1}}$, δεν διαιρεί τον $\mathbf{a_n}$, ενώ ο $\mathbf{p^2}$ δεν διαιρεί τον $\mathbf{a_0}$, τότε το $\mathbf{f(x)}$ είναι ανάγωγο στο $\mathbb{Q}[x]$.**

  Το προαναφερθέν κριτήριο του Eisenstein υπάρχει στο [**9**] της βιβλιογραφίας, Θεώρημα 24.

- **Έστω $\mathbf{p}$ πρώτος, $\mathbb{Z}_p$ το σώμα των ακεραίων $\bmod p$, $\mathbf{f(x) = \sum_{i=0}^{n} a_i\,x^i \in \mathbb{Z}[x]}$. Αν ο $\mathbf{p}$ έχει επιλεγεί έτσι ώστε το πολυώνυμο,**

  $$\mathbf{f(x) \bmod p = \sum_{i=0}^{n} (a_i \bmod p)\,(x^i \bmod p)},$$

  να έχει βαθμό $\mathbf{n}$ και να είναι ανάγωγο στο $\mathbb{Z}_p[x]$, τότε το $\mathbf{f(x)}$ είναι ανάγωγο στο $\mathbb{Z}[x]$.

  Το κριτήριο αυτό υπάρχει στο [**9**] της βιβλιογραφίας, ασκήσεις 66, 67.

- **Το $\mathbf{f(x) \in F[x]}$ είναι ανάγωγο στο $\mathbf{F[x]}$ αν και μόνο αν το $\mathbf{f(x+k)}$ είναι ανάγωγο στο $\mathbf{F[x]}$ με $\mathbf{k}$ οιοδήποτε στοιχείο του $\mathbf{F}$.**

  Το κριτήριο αυτό υπάρχει στο [**9**] της βιβλιογραφίας, άσκηση 69.

Το Θεώρημα GIRARD–KRONECKER

§26. Όπως έχουμε προαναφέρει σκοπός μας είναι να μελετήσουμε την επιλυσιμότητα δια ριζικών πολυωνυμικών εξισώσεων. Όμως για να μιλήσουμε για

λύσεις πολυωνυμικών εξισώσεων πρέπει πρώτα να έχουμε εξασφαλίσει ότι αυτές υπάρχουν και κατόπιν να διερευνήσουμε αν εκφράζονται δια μέσου ριζικών.

Οι επόμενες ενότητες αναφέρονται στην απόδειξη του Θεωρήματος Girard–Kronecker που είναι γενίκευση του γνωστού Θεμελιώδους Θεωρήματος της Άλγεβρας. Πιο συγκεκριμένα το Θεώρημα Girard–Kronecker λέει ότι,

Για κάθε πολυώνυμο βαθμού $\mathbf{n}$ με συντελεστές σε κάποιο σώμα $\mathbf{F}$ υπάρχει σώμα $\mathbf{L}$ ώστε $\mathbf{F \subseteq L}$ και το $\mathbf{L}$ περιέχει ακριβώς $\mathbf{n}$ το πλήθος ρίζες του πολυωνύμου, (λαμβάνοντας υπ' όψιν την πολλαπλότητα της κάθε ρίζας).

Το Θεμελιώδες θεώρημα της Άλγεβρας είναι εφαρμογή του προαναφερθέντος Θεωρήματος για $F = L = \mathbb{C}$.

§27. Έστω $\mathbf{A}$ ένα σύνολο. Κάθε συνάρτηση από το καρτεσιανό γινόμενο $\mathbf{A \times A}$ στο $\mathbf{A}$ λέγεται διμελής πράξη.

Οι συνήθεις πράξεις της πρόσθεσης, αφαίρεσης, πολλαπλασιασμού και διαίρεσης είναι διμελής πράξεις. Στα επόμενα θα αναφερόμαστε σε μία διμελή πράξη με τον όρο πράξη.

§28. Έστω $\mathbf{A \neq \emptyset}$ ένα σύνολο εφοδιασμένο με μία πράξη $\mathbf{*}$ δηλαδή, $\mathbf{a * b \in A}$ για κάθε $\mathbf{a, b \in A}$. Αν τα στοιχεία του $\mathbf{A}$ ικανοποιούν και τις ιδιότητες,

- **υπάρχει στοιχείο $\mathbf{e \in A}$ ώστε $\mathbf{e * a = a * e = a}$ για κάθε $\mathbf{a \in A}$.**
- **για κάθε $\mathbf{a \in A}$, υπάρχει στοιχείο $\mathbf{a' \in A}$ με $\mathbf{a * a' = a' * a = e}$.**
- **για κάθε $\mathbf{a, b, g \in A}$ ισχύει, $\mathbf{(a * b) * g = a * (b * g)}$.**

το $\mathbf{A}$ λέγεται ομάδα.

Το στοιχείο e λέγεται ουδέτερο στοιχείο της ομάδας και είναι μοναδικό. Πράγματι αν υπάρχει και δεύτερο π.χ. το E θα έχουμε $e = e * E$. Επίσης $E = e * E$ γιατί και το e είναι ουδέτερο στοιχείο. Άρα, $e = E$.

Για κάθε $a \in A$ το a' είναι μοναδικό. Πράγματι αν υπάρχει και δεύτερο π.χ. το a'' τότε, $a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$.

Έστω $\mathbf{A, B}$ δύο ομάδες εφοδιασμένες με την ίδια πράξη και $\mathbf{B \subseteq A}$. Η $\mathbf{B}$ λέγεται υποομάδα της $\mathbf{A}$.

§29. Έστω $\mathbf{p(x) \in F[x]}$. Θέτουμε $\mathbf{\langle p(x) \rangle = \{a(x)\, p(x) : a(x) \in F[x]\}}$. Το σύνολο αυτό, εφοδιασμένο με την πράξη της πρόσθεσης πολυωνύμων είναι μία ομάδα.

- Για κάθε $a_1(x)\, p(x)$, $a_2(x)\, p(x) \in \langle p(x) \rangle$, το άθροισμα

$$a_1(x)\, p(x) + a_2(x)\, p(x) = (a_1(x) + a_2(x))\, p(x) \in \langle p(x) \rangle.$$

- Για κάθε $a(x)\, p(x) \in \langle p(x) \rangle$ το $0 = 0\, p(x) \in \langle p(x) \rangle$ και

$$a(x)\, p(x) + 0 = 0 + a(x)\, p(x) = a(x)\, p(x).$$

- Για κάθε $a(x)\,p(x) \in \langle p(x)\rangle$ το $-a(x)\,p(x) \in \langle p(x)\rangle$ και

$$a(x)\,p(x) + (-a(x)\,p(x)) = (-a(x)\,p(x)) + a(x)\,p(x) = 0.$$

- Για κάθε $a_1(x)\,p(x)$, $a_2(x)\,p(x)$, $a_3(x)\,p(x) \in \langle p(x)\rangle$ ισχύει,

$$\begin{aligned} a_1(x)\,p(x) + (a_2(x)\,p(x) + a_3(x)\,p(x)) &= \\ a_1(x)\,p(x) + (a_2(x) + a_3(x))\,p(x) &= \\ (a_1(x) + (a_2(x) + a_3(x)))\,p(x) &= \\ ((a_1(x) + a_2(x)) + a_3(x))\,p(x) &= \\ ((a_1(x) + a_2(x))\,p(x) + a_3(x)\,p(x) &= \\ (a_1(x)\,p(x) + a_2(x)\,p(x)) + a_3(x)\,p(x). & \end{aligned}$$

§30. Για το σύνολο $\langle \mathbf{p(x)}\rangle$ ισχύει ότι, $\mathbf{b(x)\,(a(x)\,p(x))} \in \langle \mathbf{p(x)}\rangle$ για κάθε $\mathbf{b(x)} \in \mathbf{F[x]}$ δηλαδή, το $\langle \mathbf{p(x)}\rangle$ απορροφά κάθε στοιχείο του $\mathbf{F[x]}$ που πολλαπλασιάζεται με στοιχείο του $\langle \mathbf{p(x)}\rangle$. Αυτό μπορεί να συμβολισθεί και ως $\mathbf{b(x)}\,\langle \mathbf{p(x)}\rangle = \langle \mathbf{p(x)}\rangle$ για κάθε $\mathbf{b(x)} \in \mathbf{F[x]}$.

Πράγματι για κάθε $b(x) \in F[x]$, $a(x)\,p(x) \in \langle p(x)\rangle$ το $b(x)\,(a(x)\,p(x)) = (b(x)\,a(x))\,p(x) \in \langle p(x)\rangle$ γιατί $b(x)\,a(x) \in F[x]$.

§31. Κάθε μη κενό υποσύνολο ενός μεταθετικού δακτυλίου με μονάδα που εφοδιασμένο με την πράξη της πρόσθεσης του δακτυλίου είναι ομάδα και απορροφά πολλαπλασιαστικώς τα στοιχεία του δακτυλίου λέγεται ιδεώδες. Από τις §29, §30 προκύπτει ότι το σύνολο $\langle \mathbf{p(x)}\rangle$ είναι ιδεώδες του $\mathbf{F[x]}$.

§32. Έστω $\mathbf{b(x), p(x)} \in \mathbf{F[x]}$. Ορίζουμε το σύνολο $\mathbf{b(x)} + \langle \mathbf{p(x)}\rangle$ ως εξής,

$$\mathbf{b(x)} + \langle \mathbf{p(x)}\rangle = \{\mathbf{b(x)} + \mathbf{a(x)\,p(x)} : \mathbf{a(x)} \in \mathbf{F[x]}\}.$$

Ορίζουμε το σύνολο $\mathbf{F[x]}/\langle \mathbf{p(x)}\rangle$ ως εξής,

$$\mathbf{F[x]}/\langle \mathbf{p(x)}\rangle = \{\mathbf{b(x)} + \langle \mathbf{p(x)}\rangle : \mathbf{b(x)} \in \mathbf{F[x]}\}.$$

Εφοδιάζουμε το $F[x]/\langle p(x)\rangle$ με μία πράξη πρόσθεσης $\oplus$ και μία πράξη πολλαπλασιασμού $\odot$ ως εξής,

$$\begin{aligned} (b_1(x) + \langle p(x)\rangle) \oplus (b_2(x) + \langle p(x)\rangle) &= (b_1(x) + b_2(x)) + \langle p(x)\rangle, \\ (b_1(x) + \langle p(x)\rangle) \odot (b_2(x) + \langle p(x)\rangle) &= (b_1(x)\,b_2(x)) + \langle p(x)\rangle. \end{aligned}$$

- Το $F[x]/\langle p(x)\rangle$ είναι κλειστό ως προς τις πράξεις $\oplus, \odot$.

- Επειδή, $(b_1(x) + \langle p(x)\rangle) \oplus (b_2(x) + \langle p(x)\rangle) =$

$$\begin{aligned} &= (b_1(x) + b_2(x)) + \langle p(x)\rangle = \\ &= (b_2(x) + b_1(x)) + \langle p(x)\rangle = \\ &= (b_2(x) + \langle p(x)\rangle) \oplus (b_1(x) + \langle p(x)\rangle), \end{aligned}$$

και $(b_1(x) + \langle p(x)\rangle) \odot (b_2(x) + \langle p(x)\rangle) =$

$$= (b_1(x)\,b_2(x)) + \langle p(x)\rangle =$$

$$\begin{aligned} &= (b_2(x)\, b_1(x)) + \langle p(x)\rangle = \\ &= (b_2(x) + \langle p(x)\rangle) \odot (b_1(x) + \langle p(x)\rangle), \end{aligned}$$

οι πράξεις $\oplus, \odot$ είναι μεταθετικές.

- Τα $0 + \langle p(x)\rangle = \langle p(x)\rangle$, $1 + \langle p(x)\rangle$ είναι τα ουδέτερα στοιχεία των πράξεων $\oplus, \odot$ αντιστοίχως.
- Το $-b(x) + \langle p(x)\rangle$ είναι το αντίθετο του $b(x) + \langle p(x)\rangle$ όταν $b(x) \neq 0$.
- Επειδή, $((b_1(x) + \langle p(x)\rangle) \oplus (b_2(x) + \langle p(x)\rangle)) \oplus (b_3(x) + \langle p(x)\rangle) =$

$$\begin{aligned} &= ((b_1(x) + b_2(x)) + \langle p(x)\rangle) \oplus (b_3(x) + \langle p(x)\rangle) = \\ &= ((b_1(x) + b_2(x)) + b_3(x)) + \langle p(x)\rangle = \\ &= (b_1(x) + (b_2(x) + b_3(x))) + \langle p(x)\rangle = \\ &= (b_1(x) + \langle p(x)\rangle) \oplus ((b_2(x) + b_3(x)) + \langle p(x)\rangle) = \\ &= (b_1(x) + \langle p(x)\rangle) \oplus ((b_2(x) + \langle p(x)\rangle) \oplus (b_3(x) + \langle p(x)\rangle)), \end{aligned}$$

και $((b_1(x) + \langle p(x)\rangle) \odot (b_2(x) + \langle p(x)\rangle)) \odot (b_3(x) + \langle p(x)\rangle) =$

$$\begin{aligned} &= ((b_1(x)\, b_2(x)) + \langle p(x)\rangle) \odot (b_3(x) + \langle p(x)\rangle) = \\ &= ((b_1(x)\, b_2(x))\, b_3(x)) + \langle p(x)\rangle = \\ &= (b_1(x)\, (b_2(x)\, b_3(x))) + \langle p(x)\rangle = \\ &= (b_1(x) + \langle p(x)\rangle) \odot ((b_2(x)\, b_3(x)) + \langle p(x)\rangle) = \\ &= (b_1(x) + \langle p(x)\rangle) \odot ((b_2(x) + \langle p(x)\rangle) \odot (b_3(x) + \langle p(x)\rangle)), \end{aligned}$$

οι πράξεις $\oplus, \odot$ είναι προσετεριστικές.

- Επειδή, $((b_1(x) + \langle p(x)\rangle) \odot ((b_2(x) + \langle p(x)\rangle) \oplus (b_3(x) + \langle p(x)\rangle)) =$

$$\begin{aligned} &= (b_1(x) + \langle p(x)\rangle) \odot ((b_2(x) + b_3(x)) + \langle p(x)\rangle) = \\ &= (b_1(x)\, (b_2(x) + b_3(x)) + \langle p(x)\rangle = \\ &= (b_1(x)\, b_2(x) + b_1(x)\, b_3(x)) + \langle p(x)\rangle = \\ &= (b_1(x)\, b_2(x) + \langle p(x)\rangle) \oplus (b_1(x)\, b_3(x) + \langle p(x)\rangle) = \\ &= (b_1(x) + \langle p(x)\rangle) \odot (b_2(x) + \langle p(x)\rangle) \oplus \\ &\quad \oplus (b_1(x) + \langle p(x)\rangle) \odot (b_3(x) + \langle p(x)\rangle), \end{aligned}$$

ισχύει η επιμεριστική ιδιότητα του «πολλαπλασιασμού» $\odot$ επί της «πρόσθεσης» $\oplus$.

Αποδείξαμε ότι το σύνολο $F[x]/\langle p(x)\rangle$ εφοδιασμένο με την «πρόσθεσης» $\oplus$ και τον «πολλαπλασιασμό» $\odot$ είναι μεταθετικός δακτύλιος με μονάδα.

§33. Έστω $\mathbf{p(x)}$ ένα ανάγωγο πολυώνυμο στο $\mathbf{F[x]}$. Το σύνολο $\mathbf{F[x]/\langle p(x)\rangle}$ εφοδιασμένο με τις πράξεις $\oplus, \odot$ όπως ορίσθηκαν στην §32 είναι σώμα.

Στην §32 αποδείξαμε ότι η δομή $(F[x]/\langle p(x)\rangle, \oplus, \odot)$ είναι μεταθετικός δακτύλιος με μονάδα. Αρκεί να δείξουμε ότι για κάθε μη μηδενικό στοιχείο του

$F[x]/\langle p(x)\rangle$ υπάρχει «πολλαπλασιαστικό» αντίστροφο ως προς τον «πολλαπλασιασμό» $\odot$. Έστω $b(x)+\langle p(x)\rangle$ μη μηδενικό στοιχείο του $F[x]/\langle p(x)\rangle$ δηλαδή, $b(x)+\langle p(x)\rangle \neq 0+\langle p(x)\rangle = \langle p(x)\rangle$. Άρα, $b(x)+\langle p(x)\rangle \neq \langle p(x)\rangle$. Αν το $p(x)$ διαιρεί το $b(x)$ τότε, $b(x)=p(x)\,q(x)$, με $q(x)\in F[x]$ δηλαδή, $b(x)\in\langle p(x)\rangle$ και

$$\begin{aligned} b(x)+\langle p(x)\rangle &= \{b(x)+a(x)\,p(x) : a(x)\in F[x]\} = \\ &= \{p(x)\,q(x)+a(x)\,p(x) : q(x),a(x)\in F[x]\} = \\ &= \{(q(x)+a(x))\,p(x) : q(x),a(x)\in F[x]\} = \\ &= \{g(x)\,p(x) : g(x)\in F[x]\} = \langle p(x)\rangle, \end{aligned}$$

άτοπο. Άρα το $p(x)$ δεν διαιρεί το $b(x)$. Έστω $d(x)\in F[x]$ είναι ένας μέγιστος κοινός διαιρέτης των $p(x)$, $b(x)$. Αν $deg[d(x)]\geq 1$ τότε η σχέση $p(x)=d(x)\,k(x)$, με $k(x)\in F[x]$ επάγει ότι $deg[k(x)]=0$, (γιατί το $p(x)$ είναι ανάγωγο). Οπότε, $k(x)=k\in F-\{0\}$ και $p(x)=k\,d(x)$ ή $d(x)=k^{-1}\,p(x)$. Από την $b(x)=d(x)\,t(x)$ με $t(x)\in F[x]$ έπεται $b(x)=k^{-1}\,t(x)\,p(x)$ και το $p(x)$ διαιρεί το $b(x)$, άτοπο. Άρα, τα $p(x)$, $b(x)$ είναι πρώτα μεταξύ τους και από την §15 σχέση (14) μπορούμε να γράψουμε,

$$\begin{aligned} b_1(x)\,b(x)+b_2(x)\,p(x)=1 &\Rightarrow \\ (\text{ με } b_1(x),\, b_2(x)\in F[x]) & \\ b_1(x)\,b(x)=1+(-b_2(x))\,p(x) &\Rightarrow \\ (b_1(x)+\langle p(x)\rangle)\odot(b(x)+\langle p(x)\rangle)=(b_1(x)\,b(x))+\langle p(x)\rangle &= \\ \{b_1(x)\,b(x)+a(x)\,p(x) : a(x)\in F[x]\} &= \\ \{1+(-b_2(x))\,p(x)+a(x)\,p(x) : -b_2(x),a(x)\in F[x]\} &= \\ \{1+(-b_2(x)+a(x))\,p(x) : -b_2(x),a(x)\in F[x]\} &= \\ \{1+u(x)\,p(x) : u(x)\in F[x]\} &= \\ 1+\langle p(x)\rangle. & \end{aligned}$$

Δείξαμε ότι το μη μηδενικό στοιχείο $b(x)+\langle p(x)\rangle$ του $F[x]/\langle p(x)\rangle$ έχει αντίστροφο ως προς την πράξη $\odot$ και το $F[x]/\langle p(x)\rangle$ είναι σώμα.

§34. Θεωρούμε το σύνολο $\mathbf{FI}=\{\mathbf{b}+\langle\mathbf{p(x)}\rangle : \mathbf{b}\in\mathbf{F}\}$, $\mathbf{p(x)}$ ανάγωγο πολυώνυμο στο $\mathbf{F[x]}$. Το $\mathbf{FI}$ είναι υποσύνολο του $\mathbf{F[x]/\langle p(x)\rangle}$. Ορίζουμε την συνάρτηση $\mathbf{f : F\mapsto FI}$ με κανόνα $\mathbf{f(b)=b+\langle p(x)\rangle}$. Η συνάρτηση αυτή είναι ισομορφική εμφύτευση του σώματος $\mathbf{F}$ στο σώμα $\mathbf{F[x]/\langle p(x)\rangle}$.

Έστω $b_1=b_2$ στοιχεία του F. Τότε και $b_1-b_2=0$ και,

$$\begin{aligned} (b_1-b_2)+\langle p(x)\rangle &= \{(b_1-b_2)+a(x)\,p(x) : a(x)\in F[x]\} = \\ &= \{0+a(x)\,p(x) : a(x)\in F[x]\} = \\ &= \{a(x)\,p(x) : a(x)\in F[x]\} = \\ &= \langle p(x)\rangle = 0+\langle p(x)\rangle \Rightarrow \\ (b_1+\langle p(x)\rangle)-(b_2+\langle p(x)\rangle) &= 0+\langle p(x)\rangle \Rightarrow \\ b_1+\langle p(x)\rangle &= b_2+\langle p(x)\rangle, \end{aligned}$$

και η f είναι καλώς ορισμένη. Επίσης,

$$b_1+\langle p(x)\rangle = b_2+\langle p(x)\rangle \Rightarrow$$

$$\begin{aligned}
(b_1 - b_2) + \langle p(x)\rangle &= 0 + \langle p(x)\rangle = \langle p(x)\rangle \Rightarrow \\
\{(b_1 - b_2) + a(x)\,p(x) : a(x) \in F[x]\} &= \{a(x)\,p(x) : a(x) \in F[x]\} \Rightarrow \\
(b_1 - b_2) + a_1(x)\,p(x) &= a_2(x)\,p(x) \Rightarrow \\
&\quad \text{για κάποια } a_1(x),\, a_2(x) \in F[x] \\
b_1 - b_2 &= (a_1(x) - a_2(x))\,p(x).
\end{aligned}$$

Αν $a_1(x) \neq a_2(x)$ τότε το $p(x)$ βαθμού μεγαλύτερου ή ίσου του 1, (ως ανάγωγο), διαιρεί το σταθερό πολυώνυμο $b_1 - b_2$. Αυτό μπορεί να συμβαίνει μόνο αν το $b_1 - b_2$ είναι το μηδενικό πολυώνυμο δηλαδή, $b_1 = b_2$. Αν $a_1(x) = a_2(x)$ τότε $b_1 - b_2 = 0\,p(x) = 0$ και $b_1 = b_2$. Αποδείξαμε ότι η f είναι ένα προς ένα.

$$\begin{aligned}
f(b_1 + b_2) &= (b_1 + b_2) + \langle p(x)\rangle = (b_1 + \langle p(x)\rangle) \oplus (b_2 + \langle p(x)) = \\
&= f(b_1) \oplus f(b_2), \\
f(b_1\,b_2) &= (b_1\,b_2) + \langle p(x)\rangle = (b_1 + \langle p(x)\rangle) \odot (b_2 + \langle p(x)) = \\
&= f(b_1) \odot f(b_2).
\end{aligned}$$

Η f απεικονίζει τις πράξεις του σώματος F στις πράξεις του σώματος $F[x]/\langle p(x)\rangle$ όταν αυτές σημειώνονται ανάμεσα στα σταθερά στοιχεία του $F[x]/\langle p(x)\rangle$. Τα σταθερά στοιχεία του $F[x]/\langle p(x)\rangle$ συγκροτούν το σύνολο FI. Για κάθε $b + \langle p(x)\rangle \in FI$ υπάρχει στοιχείο του F το b ώστε $f(b) = b + \langle p(x)\rangle$ επάγοντας ότι η f είναι επί του FI.

Τελικώς έχουμε δείξει ότι η συνάρτηση f είναι ένας ένα προς ένα και επί ομομορφισμός από το σώμα F στο σύνολο FI. Δηλαδή η f είναι ένα ισομορφισμός από το σώμα F στο σύνολο FI και άρα επάγει στο FI δομή σώματος με τις πράξεις $\oplus, \odot$.

§35. Το σύνολο $\mathbf{FI[x]} = \{\sum_{\mathbf{k=0}}^{\mathbf{n}}(\mathbf{b_k} + \langle \mathbf{p(x)}\rangle)\,\mathbf{x^k} : \mathbf{n} \in \mathbb{N},\, \mathbf{b_k} \in \mathbf{F}\}$ εφοδιασμένο με τις πράξεις «πρόσθεσης» $\oplus_{\mathbf{FI}}$ και «πολλαπλασιασμού» $\odot_{\mathbf{FI}}$ ώστε,

$$\begin{aligned}
&\sum_{\mathbf{k=0}}^{\mathbf{n}}(\mathbf{b_k} + \langle \mathbf{p(x)}\rangle)\,\mathbf{x^k} \oplus_{\mathbf{FI[x]}} \sum_{\mathbf{k=0}}^{\mathbf{m}}(\mathbf{g_k} + \langle \mathbf{p(x)}\rangle)\,\mathbf{x^k} \quad = \\
&\qquad \sum_{\mathbf{k=0}}^{\mathbf{max\{n,m\}}} ((\mathbf{b_k} + \langle \mathbf{p(x)}\rangle) \oplus (\mathbf{g_k} + \langle \mathbf{p(x)}\rangle))\,\mathbf{x^k}, \\
&\sum_{\mathbf{k=0}}^{\mathbf{n}}(\mathbf{b_k} + \langle \mathbf{p(x)}\rangle)\,\mathbf{x^k} \odot_{\mathbf{FI[x]}} \sum_{\mathbf{k=0}}^{\mathbf{m}}(\mathbf{g_k} + \langle \mathbf{p(x)}\rangle)\,\mathbf{x^k} \quad = \\
&\sum_{\mathbf{k=0}}^{\mathbf{n+m}} \left(\sum_{\mathbf{i=0}}^{\mathbf{k}} (\mathbf{b_{k-i}} + \langle \mathbf{p(x)}\rangle) \odot (\mathbf{g_i} + \langle \mathbf{p(x)}\rangle) \right) \mathbf{x^k},
\end{aligned}$$

είναι δακτύλιος πολυωνύμων.

Είναι άμεση εφαρμογή των ιδιοτήτων των πράξεων του F και του FI να δείξουμε ότι το $FI[x]$ είναι δακτύλιος.

Να τονίσουμε ότι ο πολλαπλασιασμός $(\mathbf{b_k} + \langle \mathbf{p(x)}\rangle)\,\mathbf{x^k}$ είναι εκείνος που επάγεται από τον πολλαπλασιασμό του σώματος από το οποίο λαμβάνει τιμές η μεταβλητή $\mathbf{x}$. Εννοείται ότι ο πολλαπλασιασμός αυτός με στοιχεία του $\mathbf{F[x]}/\langle \mathbf{p(x)}\rangle$ πρέπει να έχει νόημα.

§36. Έστω οι δακτύλιοι πολυωνύμων F[x], FI[x]. Μέσω της συνάρτησης f της παραγράφου §34 ορίζουμε την συνάρτηση,

$$\mathcal{F} : \mathbf{F[x]} \mapsto \mathbf{FI[x]}$$

με κανόνα,

$$\mathcal{F}(\mathbf{b(x)}) = \mathcal{F}\left(\sum_{\mathbf{k=0}}^{\mathbf{n}} \mathbf{b_k}\,\mathbf{x^k}\right) = \sum_{\mathbf{k=0}}^{\mathbf{n}} \mathbf{f(b_k)}\,\mathbf{x^k}.$$

Η $\mathcal{F}$ είναι ισομορφισμός δακτυλίων πολυωνύμων.

Αν $b(x) = \sum_{k=0}^{n} b_k\,x^k = \sum_{k=0}^{m} g_k\,x^k = g(x)$ τότε $n = m$, $b_k = g_k$ και $f(b_k) = f(g_k)$ γιατί η f είναι καλώς ορισμένη. Οπότε,

$$\mathcal{F}(b(x)) = \sum_{k=0}^{n} f(b_k)\,x^k = \sum_{k=0}^{m} f(g_k)\,x^k = \mathcal{F}(g(x)),$$

και η $\mathcal{F}$ είναι καλώς ορισμένη. Ενώ,

$$\begin{aligned} \mathcal{F}(b(x)) = \mathcal{F}\left(\sum_{k=0}^{n} b_k\,x^k\right) &= \mathcal{F}\left(\sum_{k=0}^{m} g_k\,x^k\right) = \mathcal{F}(g(x)) \Rightarrow \\ \sum_{k=0}^{n} f(b_k)\,x^k &= \sum_{k=0}^{m} f(g_k)\,x^k, \end{aligned}$$

και $n = m$, $f(b_k) = f(g_k)$ που επάγει $b_k = g_k$ επειδή η f είναι ένα προς ένα. Άρα,

$$b(x) = \sum_{k=0}^{n} b_k\,x^k = \sum_{k=0}^{m} g_k\,x^k = g(x),$$

και η $\mathcal{F}$ είναι ένα προς ένα. Για κάθε πολυώνυμο,

$$B(x) = \sum_{k=0}^{n} (b_k + \langle p(x)\rangle)\,x^k = \sum_{k=0}^{n} f(b_k)\,x^k,$$

του $FI[x]$, υπάρχει το πολυώνυμο $b(x) = \sum_{k=0}^{n} b_k\,x^k$ του $F[x]$ ώστε $\mathcal{F}(b(x)) = B(x)$ και η $\mathcal{F}$ είναι επί του $FI[x]$.

$$\begin{aligned} \mathcal{F}(b(x) + g(x)) &= \mathcal{F}\left(\sum_{k=0}^{\max\{n,m\}} (b_k + g_k)\,x^k\right) = \sum_{k=0}^{\max\{n,m\}} f(b_k + g_k)\,x^k = \\ &= \sum_{k=0}^{\max\{n,m\}} ((b_k + g_k) + \langle p(x)\rangle)\,x^k = \\ &= \sum_{k=0}^{\max\{n,m\}} ((b_k + \langle p(x)\rangle) \oplus (g_k + \langle p(x)\rangle))\,x^k = \\ &= \sum_{k=0}^{n} (b_k + \langle p(x)\rangle)\,x^k \oplus_{FI[x]} \sum_{k=0}^{m} (g_k + \langle p(x)\rangle)\,x^k = \end{aligned}$$

$$
\begin{aligned}
&= \sum_{k=0}^{n} f(b_k)\, x^k \oplus_{FI[x]} \sum_{k=0}^{m} f(g_k)\, x^k = \\
&= \mathcal{F}(b(x)) \oplus_{FI[x]} \mathcal{F}(g(x)), \\
\mathcal{F}(b(x)\, g(x)) &= \mathcal{F}\left(\sum_{k=0}^{n} b_k\, x^k \sum_{k=0}^{m} g_k\, x^k\right) = \mathcal{F}\left(\sum_{k=0}^{n+m}\left(\sum_{i=0}^{k} b_{k-i}\, g_i\right) x^k\right) = \\
&= \sum_{k=0}^{n+m}\left(\sum_{i=0}^{k} f(b_{k-i}\, g_i)\right) x^k = \\
&= \sum_{k=0}^{n+m}\left(\sum_{i=0}^{k} (b_{k-i} + \langle p(x)\rangle) \odot (g_i + \langle p(x)\rangle)\right) x^k = \\
&= \sum_{k=0}^{n} (b_k + \langle p(x)\rangle)\, x^k \odot_{FI[x]} \sum_{k=0}^{m} (g_k + \langle p(x)\rangle)\, x^k = \\
&= \sum_{k=0}^{n} f(b_k)\, x^k \odot_{FI[x]} \sum_{k=0}^{m} f(g_k)\, x^k = \\
&= \mathcal{F}(b(x)) \odot_{FI[x]} \mathcal{F}(g(x)),
\end{aligned}
$$

και η $\mathcal{F}$ είναι ομομορφισμός δακτυλίων πολυωνύμων. Άρα η $\mathcal{F}$ είναι ένα προς ένα, επί και ομομορφισμός δηλαδή ισομορφισμός δακτυλίων πολυωνύμων.

§37. Έστω $\mathbf{p(x)} \in \mathbf{F[x]}$ ανάγωγο πολυώνυμο στο $\mathbf{F[x]}$. Το σώμα $\mathbf{F[x]/\langle p(x)\rangle}$ περιέχει μία ρίζα του πολυωνύμου $\mathcal{F}(\mathbf{p(x)})$.

$$
\begin{aligned}
p(x) &= \sum_{k=0}^{n} p_k\, x^k, \\
\mathcal{F}(p(x)) = P(x) &= \sum_{k=0}^{n} f(p_k)\, x^k = \sum_{k=0}^{n} (p_k + \langle p(x)\rangle)\, x^k \Rightarrow \\
P(x + \langle p(x)\rangle) &= \sum_{k=0}^{n} (p_k + \langle p(x)\rangle) \odot (x + \langle p(x)\rangle)^k = \\
&= \sum_{k=0}^{n} (p_k + \langle p(x)\rangle) \odot (x^k + \langle p(x)\rangle) = \\
&= \sum_{k=0}^{n} ((p_k\, x^k) + \langle p(x)\rangle) = \\
&= \left(\sum_{k=0}^{n} p_k\, x^k\right) + \langle p(x)\rangle = \\
&= p(x) + \langle p(x)\rangle = \\
&= \{p(x) + a(x)\, p(x) : a(x) \in F[x]\} =
\end{aligned}
$$

$$\begin{aligned} &= \{(1+a(x))\,p(x) : a(x) \in F[x]\} = \\ &= \{u(x)\,p(x) : u(x) \in F[x]\} = \langle p(x)\rangle = \\ &= 0 + \langle p(x)\rangle. \end{aligned}$$

Άρα το στοιχείο $x + \langle p(x)\rangle$ του $F[x]/\langle p(x)\rangle$ είναι ρίζα του πολυωνύμου $P(x)$ δηλαδή του $\mathcal{F}(p(x))$.

§38. Για κάθε μη κενό σύνολο A υπάρχει ένα μη κενό σύνολο B ώστε τα στοιχεία του A να βρίσκονται σε ένα προς ένα και επί αντιστοιχία με τα στοιχεία του B.

Θεωρούμε ένα στοιχείο b που δεν ανήκει στο σύνολο A. Το σύνολο,

$$B = \{b_a : \text{ για κάθε } a \in A\},$$

πληρεί την ζητούμενη προϋπόθεση.

§39. Έστω $\mathbf{p(x) \in F[x]}$ ανάγωγο πολυώνυμο στο $\mathbf{F[x]}$. Θεωρούμε το σύνολο $\mathbf{(F[x]/\langle p(x)\rangle) - FI}$. Θέτουμε EF ένα σύνολο του οποίου τα στοιχεία βρίσκονται σε ένα προς ένα και επί αντιστοιχία με αυτά του συνόλου $\mathbf{(F[x]/\langle p(x)\rangle) - FI}$. Από την §38 ξέρουμε ότι το EF υπάρχει. Συμβολίζουμε με Φ την ένα προς ένα και επί συνάρτηση από το EF στο $\mathbf{(F[x]/\langle p(x)\rangle) - FI}$ που εξασφαλίζει ότι τα στοιχεία των δύο συνόλων βρίσκονται σε ένα προς ένα και επί αντιστοιχία. Ορίζουμε την συνάρτηση $\mathbf{\mathfrak{F} : (EF \cup F) \mapsto F[x]/\langle p(x)\rangle}$ έτσι ώστε,

$$\mathfrak{F}(\mathbf{a}) = \begin{cases} \mathbf{f(a)} & , \text{ όταν } \mathbf{a \in F}, \\ \mathbf{\Phi(a)} & , \text{ όταν } \mathbf{a \in EF}. \end{cases}$$

όπου f είναι η συνάρτηση που ορίσαμε στην §34. Είναι προφανές από τον ορισμό της ότι η $\mathfrak{F}$ είναι μία καλώς ορισμένη ένα προς ένα και επί συνάρτηση. Ορίζουμε πράξεις «πρόσθεσης» $\oplus_{\mathfrak{F}}$ και «πολλαπλασιασμού» $\odot_{\mathfrak{F}}$ στο $\mathbf{EF \cup F}$ ως εξής,

$$\mathbf{a} \oplus_{\mathfrak{F}} \mathbf{b} = \mathfrak{F}^{-1}(\mathfrak{F}(\mathbf{a}) \oplus \mathfrak{F}(\mathbf{b})), \tag{26}$$

$$\mathbf{a} \odot_{\mathfrak{F}} \mathbf{b} = \mathfrak{F}^{-1}(\mathfrak{F}(\mathbf{a}) \odot \mathfrak{F}(\mathbf{b})). \tag{27}$$

Όταν $\mathbf{a, b \in F}$ οι πιο πάνω ορισθείσες πράξεις είναι η πρόσθεση και ο πολλαπλασιασμός του σώματος F όπως φαίνεται από τις,

$$\begin{aligned} \mathbf{a} \oplus_{\mathfrak{F}} \mathbf{b} &= \mathfrak{F}^{-1}(\mathfrak{F}(\mathbf{a}) \oplus \mathfrak{F}(\mathbf{b})) = \mathfrak{F}^{-1}(\mathbf{f(a)} \oplus \mathbf{f(b)}) = \\ &= \mathfrak{F}^{-1}(\mathbf{f(a+b)}) = \mathbf{f^{-1}(f(a+b))} = \mathbf{a+b}, \\ \mathbf{a} \odot_{\mathfrak{F}} \mathbf{b} &= \mathfrak{F}^{-1}(\mathfrak{F}(\mathbf{a}) \odot \mathfrak{F}(\mathbf{b})) = \mathfrak{F}^{-1}(\mathbf{f(a)} \odot \mathbf{f(b)}) = \\ &= \mathfrak{F}^{-1}(\mathbf{f(a\,b)}) = \mathbf{f^{-1}(f(a\,b))} = \mathbf{a\,b}. \end{aligned}$$

Είναι άμεσο να επαληθευθεί ότι το $\mathbf{EF \cup F}$ εφοδιασμένο με τις πιο πάνω ορισθείσες πράξεις είναι σώμα και η $\mathfrak{F}$ ένας ένα προς ένα και επί ομομορφισμός δηλαδή, ισομορφισμός μεταξύ των σωμάτων $\mathbf{EF \cup F}$ και $\mathbf{F[x]/\langle p(x)\rangle}$.

Από την παράγραφο §37 γνωρίζουμε ότι το σώμα $F[x]/\langle p(x)\rangle$ περιέχει το

στοιχείο $x+\langle p(x)\rangle$ που είναι μία ρίζα του $P(x)=\mathcal{F}(p(x))$. Επειδή το x δεν είναι σταθερό στοιχείο έπεται ότι το $x+\langle p(x)\rangle$ ανήκει στο $F[x]/\langle p(x)\rangle - FI$. Από τα πιο πάνω, υπάρχει στοιχείο $\rho=\Phi^{-1}(x+\langle p(x)\rangle)=\mathfrak{F}^{-1}(x+\langle p(x)\rangle)$ του $EF\subset(EF\cup F)$ ώστε αν $p(x)=\sum_{k=0}^{n}p_k\,x^k$ να λαμβάνουμε,

$$\begin{aligned}
\mathfrak{F}(p(\rho)) &= \mathfrak{F}\left(p_n\odot_{\mathfrak{F}}\rho^n\oplus_{\mathfrak{F}}p_{n-1}\odot_{\mathfrak{F}}\rho^{n-1}\oplus_{\mathfrak{F}}\cdots\oplus_{\mathfrak{F}}p_1\odot_{\mathfrak{F}}\rho\oplus_{\mathfrak{F}}p_0\right)\overset{(26,27)}{=}\\
&= \sum_{k=0}^{n}\mathfrak{F}(p_k)\odot\mathfrak{F}(\rho^k)=\\
&= \sum_{k=0}^{n}\mathfrak{F}(p_k)\odot\mathfrak{F}(\rho)^k=\sum_{k=0}^{n}f(p_k)\odot(x+\langle p(x)\rangle)^k=\\
&= \sum_{k=0}^{n}(p_k+\langle p(x)\rangle)\odot(x^k+\langle p(x)\rangle)=\\
&= \sum_{k=0}^{n}(p_k\,x^k+\langle p(x)\rangle)=\\
&= \left(\sum_{k=0}^{n}p_k\,x^k\right)+\langle p(x)\rangle=\\
&= p(x)+\langle p(x)\rangle=\\
&= \{p(x)+a(x)\,p(x):a(x)\in F[x]\}=\\
&= \{(1+a(x))\,p(x):a(x)\in F[x]\}=\\
&= \{u(x)\,p(x):u(x)\in F[x]\}=\langle p(x)\rangle=\\
&= 0+\langle p(x)\rangle.
\end{aligned}$$

Όμως για το ουδέτερο στοιχείο της πρόσθεσης του σώματος $EF\cup F$ ισχύει, $\mathfrak{F}(0\oplus_{\mathfrak{F}}0)=\mathfrak{F}(0)\oplus\mathfrak{F}(0)=f(0)\oplus f(0)=(0+\langle p(x)\rangle)\oplus(0+\langle p(x)\rangle)=0+\langle p(x)\rangle$ δηλαδή, $\mathfrak{F}(0)=\mathfrak{F}(0\oplus_{\mathfrak{F}}0)=0+\langle p(x)\rangle$. Τελικώς, $\mathfrak{F}(p(\rho))=0+\langle p(x)\rangle=\mathfrak{F}(0)$ και επειδή η $\mathfrak{F}$ είναι ένα προς ένα λαμβάνουμε $p(\rho)=0$ επάγοντας ότι,

Για κάθε ανάγωγο στο $\mathbf{F[x]}$ πολυώνυμο $\mathbf{p(x)\in F[x]}$ υπάρχει ένα σώμα $\mathbf{K=EF\cup F\supseteq F}$ που περιέχει μία ρίζα του $\mathbf{p(x)}$.

Το τελευταίο συμπέρασμα επάγει ότι κάθε ανάγωγο στο $F[x]$ πολυώνυμο έχει ρίζα όχι στο σώμα F στο οποίο ανήκουν οι συντελεστές του αλλά σε ένα ευρύτερο σώμα K του σώματος των συντελεστών και αυτή η ρίζα ανήκει στο $K-F$.

§40. Έστω $\mathbf{f(x)\in F[x]}$. Υπάρχει σώμα $\mathbf{M\supseteq F}$ τέτοιο ώστε να περιέχει μία ρίζα του $\mathbf{f(x)}$.

Αν το $f(x)$ είναι ανάγωγο στο $F[x]$ τότε, από την §39 υπάρχει σώμα $K\supseteq F$ που περιέχει μία ρίζα ρ του $f(x)$ και το συμπέρασμα ισχύει για $M=K$. Αν το $f[x]$ δεν είναι ανάγωγο στο $F[x]$ τότε αυτό παραγοντοποιείται σε γινόμενο αναγώγων πολυωνύμων του $F[x]$. Έστω $p(x)$ ένα από αυτά. Από την §39 υπάρχει σώμα $K\supseteq F$ που περιέχει μία ρίζα ρ του $p(x)$. Η ρ όμως είναι και ρίζα του $f(x)$ αφού το $p(x)$ είναι διαιρέτης του $f(x)$. Εκ' νέου το συμπέρασμα ισχύει για

$M = K$.

§41. Έστω $\mathbf{a(x) \in F[x] - \{0\}}$. Υπάρχει σώμα $\mathbf{L \supseteq F}$ τέτοιο ώστε το $\mathbf{a(x)}$ να παραγοντοποιείται σε γινόμενο πρωτοβάθμιων πολυωνύμων του $\mathbf{L[x]}$.

Προχωρούμε εφαρμόζοντας επαγωγή στον βαθμό του $a(x)$. Για κάθε σώμα F και για κάθε πρωτοβάθμιο πολυώνυμο του $F[x]$ το συμπέρασμα ισχύει τετριμμένα με $L = F$.

Υποθέτουμε ότι το συμπέρασμα ισχύει για κάθε σώμα F και κάθε πολυώνυμο $b(x) \in F[x]$ με $deg[b(x)] \leq n$. Για κάθε σώμα F και κάθε πολυώνυμο $a(x) \in F[x]$ με $deg[a(x)] = n+1$ από την §40 υπάρχει σώμα $M \supseteq F$ που να περιέχει μία ρίζα ρ του $a(x)$. Από την §17 μπορούμε να γράψουμε,

$$a(x) = (x - \rho)\, p(x), \tag{28}$$

με $p(x) \in M[x]$ και $deg[p(x)] = n$. Από την υπόθεση της επαγωγής, υπάρχει σώμα $L \supseteq M$ ώστε το $p(x)$ να παραγοντοποιείται σε γινόμενο πρωτοβαθμίων πολυωνύμων του $L[x]$. Όμως $x - \rho \in M[x] \subseteq L[x]$ και από την (28) προκύπτει ότι το $a(x)$ παραγοντοποιείται σε γινόμενο πρωτοβαθμίων πολυωνύμων του $L[x]$ με $L \supseteq M \supseteq F$.

§42. Έστω $\mathbf{F}$ σώμα, $\mathbf{a(x) \in F[x] - \{0\}}$. Υπάρχει σώμα $\mathbf{K \supseteq F}$ ώστε να μπορούμε να γράψουμε,

$$\mathbf{a(x) = a_n\,(x - b_1) \cdots (x - b_n)},$$

με $\mathbf{a_n \in F - \{0\}}$, $\mathbf{b_1, \ldots, b_n \in K}$.

Έστω $a(x) = \sum_{k=0}^{n} a_k\, x^k$. Επειδή το $a(x)$ έχει βαθμό n έπεται $a_n \neq 0$. Οπότε, $a(x) = a_n \sum_{k=0}^{n} (a_n^{-1}\, a_k)\, x^k = a_n \sum_{k=0}^{n} g_k\, x^k = a_n\, g(x)$ με $g_n = 1$, $g_k \in F$. Από την §41 υπάρχει σώμα $K \supseteq F$ ώστε το $g(x)$ να παραγοντοποιείται σε γινόμενο πρωτοβάθμιων πολυωνύμων του $K[x]$ έστω,

$$g(x) = (t_1\, x + h_1)\,(t_2\, x + h_2) \cdots (t_m\, x + h_m),$$

με $t_1, t_2, \ldots, t_m \in K - \{0\}$, $h_1, h_2, \ldots, h_m \in K$. Μπορούμε να γράψουμε,

$$\begin{aligned} g(x) &= (t_1\, t_2 \cdots t_m)\,(x - (-t_1^{-1}\, h_1))\,(x - (-t_2^{-1}\, h_2)) \cdots (x - (-t_m^{-1}\, h_m)) = \\ &= t\,(x - b_1)\,(x - b_2) \cdots (x - b_m). \end{aligned}$$

Όμως ο συντελεστής του μεγιστοβάθμιου όρου του $g(x)$ ο $g_n = 1$ επάγει ότι $t = 1$ και τελικώς το $a(x)$ γράφεται,

$$a(x) = a_n\, g(x) = a_n\,(x - b_1) \cdots (x - b_n),$$

με $a_n \in F - \{0\}$, $b_1, \ldots, b_n \in K$. Το συμπέρασμα που μόλις αποδείξαμε είναι γνωστό ως θεώρημα Girard–Kronecker. Το γνωστό μας Θεμελιώδες Θεώρημα της Άλγεβρας είναι εφαρμογή του θεωρήματοςGirard–Kronecker στην περίπτωση $F = \mathbb{C}$. Στην περίπτωση αυτή ο Gauss απέδειξε ότι και $K = \mathbb{C}$.

Το θεώρημα Girard–Kronecker εξασφαλίζει ότι το πλήθος των λύσεων, (όχι απαραιτήτως διακεκριμένων μεταξύ τους), της πολυωνυμικής εξίσωσης $a(x) = 0$

ισούται με τον βαθμό του πολυωνύμου $a(x)$. Αυτό που δεν εξασφαλίζει είναι ότι οι λύσεις αυτές είναι στοιχεία του σώματος F από το οποίο προέρχονται οι συντελεστές του πολυωνύμου $a(x)$. Μπορεί κάποιες ή όλες εξ΄ αυτών να ανήκουν στο F, μπορεί και όλες να είναι στοιχεία κάποιου σώματος K ευρύτερου του F.

Επίσης, το θεώρημα Girard–Kronecker εξασφαλίζει την εξαγωγή ριζών n τάξης για τα στοιχεία ενός σώματος F δηλαδή, για κάθε $a \in F$, $n \in \mathbb{N} - \{0\}$, υπάρχει σώμα K ώστε $F \subseteq K$ και $k^n = a$ για κάποιο $k \in K$. Πράγματι, από το θεώρημα Girard–Kronecker η εξίσωση $x^n - a = 0$ έχει n το πλήθος λύσεις σε κάποιο σώμα K με $F \subseteq K$. Άρα, υπάρχει $k \in K$ ώστε $k^n - a = 0 \Rightarrow k^n = a$.

Έτσι, το σύμβολο $\sqrt[n]{a}$ με $a \in F$, σημαίνει κάποια από τις n το πλήθος λύσεις $k \in K$, με $F \subseteq K$, της εξίσωσης $x^n - a = 0$. Αυτό που δεν εξασφαλίζουμε είναι ότι όταν $a \in F$ τότε και $\sqrt[n]{a} \in F$. Παράδειγμα, $2 \in \mathbb{Q}$ αλλά $\sqrt[n]{2} \in \mathbb{C}$.
Φυσικά ο Kronecker απέδειξε το προαναφερθέν θεώρημα αρκετά μετά το θάνατο του Galois. Όμως το θεώρημα ήταν γνωστό στους μαθηματικούς από τα μέσα του 17ου αιώνα, (Girard). Το χρησιμοποιούσαν όμως χωρίς να έχει δοθεί μία αυστηρή απόδειξη και αναφέρονταν σε σύνολα τα στοιχεία των οποίων ικανοποιούν τις ιδιότητες (I1–I9) χωρίς να έχει ακόμη αναπτυχθεί ρητά η έννοια του σώματος.

Στοιχεία από την Θεωρία Επεκτάσεων Σωμάτων

§43. Τώρα γνωρίζουμε ότι, κάθε πολυώνυμο με συντελεστές από ένα σώμα έχει οπωσδήποτε ρίζες. Όμως οι ρίζες αυτές δεν είναι υποχρεωτικώς στοιχεία του σώματος προέλευσης των συντελεστών του πολυωνύμου. Μπορεί κάποιες ή και όλες να ανήκουν σε σώμα ευρύτερο του σώματος προέλευσης των συντελεστών του πολυωνύμου.

Για να μπορούμε να διαπιστώσουμε την αλγεβρική μορφή που έχουν οι ρίζες του πολυωνύμου πρέπει να γνωρίζουμε την αλγεβρική μορφή που έχει το σώμα που περιέχει τις ρίζες αυτές και ακόμη περισσότερο, την σχέση αυτής της αλγεβρικής μορφής με την αντίστοιχη του σώματος προέλευσης των συντελεστών του πολυωνύμου αφού αυτό είναι το αρχικό σώμα ή σώμα βάσης εντός του οποίου ξεκινάμε την διαδικασία εύρεσης των ριζών. Η διαδικασία αυτή όμως μπορεί να μας οδηγήσει σε σώματα ευρύτερα του αρχικού σώματος.

Χρειάζεται λοιπόν να εισάγουμε έννοιες από την θεωρεία επεκτάσεως σωμάτων δηλαδή, την μελέτη των αλγεβρικών ιδιοτήτων σωμάτων που είναι ευρύτερα κάποιου αρχικώς δοθέντος σώματος αλλά, με κάποιο τρόπο η αλγεβρική τους δομή συνδέεται με αυτήν του αρχικώς δοθέντος σώματος.

§44. Έστω $\mathbf{F}, \mathbf{K}$ σώματα. Το $\mathbf{K}$ λέγεται επέκταση του $\mathbf{F}$ αν $\mathbf{K} \supseteq \mathbf{F}$ και θα συμβολίζεται ως $\mathbf{K/F}$.

§45. Έστω $\mathbf{W}$ σύνολο εφοδιασμένο με μία πράξη «πρόσθεσης» μεταξύ των στοιχείων του την $(+)$. Έστω $\mathbf{F}$ σώμα ώστε να ορίζεται μία πράξη «εξωτερικού πολλαπλασιασμού» μεταξύ των στοιχείων του $\mathbf{W}$ και του $\mathbf{F}$ την οποία συμβολίζουμε με κενό.

(Με $+$ και κενό συμβολίζουμε και την πρόσθεση και πολλαπλασιασμό του σώματος $\mathbf{F}$. Στα επόμενα θα είναι σαφές ότι $\mathbf{a} + \mathbf{b}$ θα σημαίνει την πρόσθεση του $\mathbf{W}$ όταν $\mathbf{a}, \mathbf{b} \in \mathbf{W}$, $\mathbf{ab}$ θα σημαίνει τον εξωτερικό πολλαπλασιασμό μεταξύ των στοιχείων των $\mathbf{F}, \mathbf{W}$ όταν $\mathbf{a} \in \mathbf{F}$, $\mathbf{b} \in \mathbf{W}$, ενώ θα σημαίνουν την πρόσθεση, πολλαπλασιασμό του $\mathbf{F}$ όταν $\mathbf{a}, \mathbf{b} \in \mathbf{F}$ αντιστοίχως.)

Θα λέμε ότι το $\mathbf{W}$ είναι διανυσματικός χώρος επί του $\mathbf{F}$, (και τα στοιχεία του θα καλούνται διανύσματα), αν συμβαίνουν τα κάτωθι,

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

Έστω $\mathbf{w_1, w_2, \ldots, w_n}$ διανύσματα του διανυσματικού χώρου $\mathbf{W}$ επί του σώματος $\mathbf{F}$. Θα λέμε ότι τα $\mathbf{w_i}$, $\mathbf{i = 1, 2, \ldots, n}$ είναι γραμμικώς ανεξάρτητα επί του $\mathbf{F}$ αν κάθε γραμμικός συνδυασμός $\mathbf{f_1\, w_1 + f_2\, w_2 + \cdots + f_n\, w_n = 0}$, με $\mathbf{f_i \in F}$, $\mathbf{i = 1, 2, \ldots, n}$ συνεπάγεται $\mathbf{f_1 = f_2 = \cdots = f_n = 0}$.

Θα λέμε ότι τα $\mathbf{w_i}$, $\mathbf{i = 1, 2, \ldots, n}$ είναι μία βάση του $\mathbf{W}$ επί του $\mathbf{F}$ αν τα $\mathbf{w_i}$ είναι γραμμικώς ανεξάρτητα επί του $\mathbf{F}$ και επιπλέον, για κάθε $\mathbf{w \in W}$ υπάρχουν $\mathbf{f_i \in F}$, $\mathbf{i = 1, 2, \ldots, n}$ ώστε,

$$\mathbf{w = f_1\, w_1 + f_2\, w_2 + \cdots + f_n\, w_n}.$$

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 $\mathbf{F}$ διανυσμάτων δηλαδή, το πλήθος των στοιχείων της κάθε βάσης καλείται διάσταση του $\mathbf{W}$ επί του $\mathbf{F}$.

§46. Έστω $\mathbf{F, K}$ σώματα, $\mathbf{K/F}$ επέκταση του $\mathbf{F}$. Το $\mathbf{K}$ είναι διανυσματικός χώρος επί του $\mathbf{F}$ με πρόσθεση την πρόσθεση του $\mathbf{K}$ και εξωτερικό πολλαπλασιασμό τον πολλαπλασιασμό του $\mathbf{K}$.

Επειδή το σύνολο K είναι σώμα, για την πρόσθεσή του ισχύουν,

- $k_1 + k_2 = k_2 + k_1 \in K$, $\forall\, k_1, k_2 \in K$.
- Υπάρχει στοιχείο $0 \in K$ ώστε $0 + k = k + 0 = k$, $\forall\, k \in K$.

- $\forall\, k \in K - \{0\}$ υπάρχει στοιχείο $-k \in K - \{0\}$, ώστε $k + (-k) = (-k) + k = 0 \in K$.
- $k_1 + (k_2 + k_3) = (k_1 + k_2) + k_3$, $\forall\, k_1, k_2, k_3 \in K$.

Επειδή το σύνολο K είναι σώμα και $F \subseteq K$ για τον πολλαπλασιασμό του K ισχύουν,

- $f\, k \in K$, $\forall\, f \in F$, $\forall\, k \in K$.
- $1\, k = k$, $1 \in F \subseteq K$, $\forall\, k \in K$.
- $(f_1\, f_2)\, k = f_1\, (f_2\, k) = f_2\, (f_1\, k)$, $\forall\, f_1, f_2 \in F$, $\forall\, k \in K$.
- $(f_1 + f_2)\, k = f_1\, k + f_2\, k$, $\forall\, f_1, f_2 \in F$, $\forall\, k \in K$.
- $f\, (k_1 + k_2) = f\, k_1 + f\, k_2$, $\forall\, f \in F$, $\forall\, k_1, k_2 \in K$.

Θα συμβολίζουμε την διάσταση του $\mathbf{K}$ ως διανυσματικού χώρου επί του $\mathbf{F}$ με $(\mathbf{K} : \mathbf{F})$.

§47. Έστω $\mathbf{F}, \mathbf{K}$ σώματα, $\mathbf{K/F}$ επέκταση του $\mathbf{F}$. Η επέκταση $\mathbf{K/F}$ λέγεται πεπερασμένη αν η διάσταση, $(\mathbf{K} : \mathbf{F})$, του $\mathbf{K}$ ως διανυσματικού χώρου επί του $\mathbf{F}$ είναι πεπερασμένη.

§48. Έστω $\mathcal{E} = \{\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_n}\}$, $\mathcal{K} = \{\mathbf{k_1}, \mathbf{k_2}, \ldots, \mathbf{k_m}\}$ υποσύνολα του ιδίου σώματος. Συμβολίζουμε με $\mathcal{E}\,\mathcal{K} = \{\mathbf{e_1\, k_1}, \ldots, \mathbf{e_i\, k_j}, \ldots, \mathbf{e_n\, k_m}\}$ το σύνολο που έχει ως στοιχεία του τα γινόμενα $\mathbf{e_i\, k_j}$ για κάθε $\mathbf{i = 1, 2, \ldots, n}$ και $\mathbf{j = 1, 2, \ldots, m}$.

§49. Έστω $\mathbf{E, K, F}$ σώματα, με $\mathbf{E \supseteq K \supseteq F}$ και $\mathbf{E/K}$, $\mathbf{K/F}$ επεκτάσεις των $\mathbf{K, F}$ αντιστοίχως. Για την διάσταση της επέκτασης $\mathbf{E/F}$ του $\mathbf{F}$ ισχύει $(\mathbf{E} : \mathbf{F}) = (\mathbf{E} : \mathbf{K})\, (\mathbf{K} : \mathbf{F})$.

Έστω $\mathcal{E} = \{e_1, e_2, \ldots, e_n\}$ μία βάση του E επί του K και $\mathcal{K} = \{k_1, k_2, \ldots, k_m\}$ μία βάση του K επί του F. Από την §46 γνωρίζουμε ότι κάθε υπερσώμα E του F είναι διανυσματικός χώρος επί του F. Θα δείξουμε ότι το σύνολο $\mathcal{E}\,\mathcal{K}$ όπως ορίσθηκε στην §48 είναι μία βάση του E επί του F.

Έστω $f_{ij} \in F$, $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, m$ τέτοια ώστε ο γραμμικός συνδυασμός,

$$\sum_{i=1}^{n} \sum_{j=1}^{m} f_{ij}\, e_i\, k_j = 0.$$

Τότε,

$$\sum_{i=1}^{n} \left(\sum_{j=1}^{m} f_{ij}\, k_j \right) e_i = 0,$$

με $\sum_{j=1}^{m} f_{ij}\, k_j \in K$, $i = 1, 2, \ldots, n$ αφού $f_{ij} \in F \subseteq K$. Επειδή τα e_i είναι στοιχεία μίας βάσης του E επί του K, κάθε γραμμικός συνδυασμός τους επί του K, ίσος με μηδέν, επάγει ότι οι συντελεστές των e_i είναι μηδέν. Άρα,

$$\sum_{j=1}^{m} f_{ij}\, k_j = 0, \;\; i = 1, 2, \ldots, n.$$

Επειδή τα k_j είναι στοιχεία μίας βάσης του K επί του F, κάθε γραμμικός συνδυασμός τους επί του F, ίσος με μηδέν, επάγει ότι οι συντελεστές των k_j είναι μηδέν. Άρα, $f_{ij} = 0$, $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, m$. Δείξαμε ότι τα στοιχεία του $\mathcal{E}\,\mathcal{K}$ είναι γραμμικώς ανεξάρτητα επί του F.

Έστω e ένα τυχαίο στοιχείο του E. Αφού το $\mathcal{E}$ είναι βάση του E επί του K, υπάρχουν $a_i \in K$, $i = 1, 2, \ldots, n$ ώστε $e = \sum_{i=1}^{n} a_i\, e_i$. Επειδή το $\mathcal{K}$ είναι μία βάση του K επί του F υπάρχουν f_{ij}, $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, m$ ώστε το κάθε $a_i = \sum_{j=1}^{m} f_{ij}\, k_j$. Άρα,

$$e = \sum_{i=1}^{n} \sum_{j=1}^{m} f_{ij}\, e_i\, k_j,$$

και κάθε στοιχείο του E γράφεται ως γραμμικός συνδυασμός επί του F των στοιχείων του $\mathcal{E}\,\mathcal{K}$. Το $\mathcal{E}\,\mathcal{K}$ είναι μία βάση του E επί του F και $(E : F) = n\,m = (E : K)\,(K : F)$.

§50. Ήδη από την διαδικασία επίλυσης πολυωνυμικών εξισώσεων δευτέρου βαθμού με σώμα προέλευσης των συντελεστών της εξίσωσης το $\mathbb{Q}$, προέκυψαν λύσεις που αρκετές φορές δεν ανήκουν στο $\mathbb{Q}$. Αυτό γιατί ο αριθμός $\sqrt{\Delta}$ που εμφανίζεται στην έκφραση των λύσεων δεν είναι πάντοτε ρητός. Σε μία τέτοια περίπτωση οι λύσεις της εξίσωσης δεν είναι στοιχεία του $\mathbb{Q}$ αλλά ενός σώματος ευρύτερου του $\mathbb{Q}$ που περιέχει τον $\sqrt{\Delta}$. Η εύλογη ερώτηση είναι, πόσο ευρύτερου; Τόσο όσο να περιέχει το $\mathbb{Q}$ και τον $\sqrt{\Delta}$ που μας ενδιαφέρει. Τότε το σώμα αυτό περιέχει όλες τις λύσεις μιας πολυωνυμικής εξίσωσης δευτέρου βαθμού.

Κατ΄ επέκταση, αν F είναι σώμα, $f(x) \in F[x]$ μας ενδιαφέρουν εκείνες οι επεκτάσεις του F που περιέχουν όλες τις ρίζες του $f(x)$. Για την ακρίβεια οι μικρότερες δυνατές επεκτάσεις του F που περιέχουν το F και όλες τις ρίζες του $f(x)$. Καθώς επίσης και το πόσες είναι. Μία ή περισσότερες; Η γνώση της αλγεβρικής συμπεριφοράς τέτοιας μορφής επεκτάσεων του μικρότερου σώματος των συντελεστών ενός πολυωνύμου, μπορεί να μας δώσει πληροφορίες για την μορφή των ριζών του πολυωνύμου μιας και αυτές περιέχονται σε αυτές τις επεκτάσεις.

Έστω $\mathbf{F}, \mathbf{K}$ σώματα με $\mathbf{K} \supseteq \mathbf{F}$, $\mathbf{k} \in \mathbf{K}$. Ορίζουμε ως $\mathbf{F(k)}$ την τομή όλων των υποσωμάτων του σώματος $\mathbf{K}$ που περιέχουν τα $\mathbf{k}$ και $\mathbf{F}$.

Από τον ορισμό είναι σαφές ότι το $F(k)$ είναι σώμα ως τομή υποσωμάτων του σώματος K, ότι αν $k \in F$, τότε $F(k) = F$ και ότι το $F(k)$ είναι το μικρότερο υποσώμα του K που περιέχει τα k και F. Φυσικά το $F(k)$ είναι επέκταση του F. Ο πιο πάνω ορισμός μπορεί να γενικευθεί κατ΄ αναλογία,

Έστω $\mathbf{F}, \mathbf{K}$ σώματα με $\mathbf{K} \supseteq \mathbf{F}$, $\mathbf{k_1}, \mathbf{k_2}, \ldots, \mathbf{k_n} \in \mathbf{K}$. Ορίζουμε ως $\mathbf{F(k_1, k_2, \ldots, k_n)}$ την τομή όλων των υποσωμάτων του σώματος $\mathbf{K}$ που περιέχουν τα $\mathbf{k_1}, \mathbf{k_2}, \ldots, \mathbf{k_n}$ και $\mathbf{F}$.

Οι παρατηρήσεις που παραθέσαμε μετά τον ορισμό του $F(k)$ ισχύουν και για το $F(k_1, k_2, \ldots, k_n)$ αναλόγως προσαρμοσμένες. Για το $F(k_1, k_2, \ldots, k_n)$ λέμε ότι προέκυψε από το σώμα F με προσάρτηση των $k_1, k_2, \ldots, k_n$ και είναι επέκταση του F.

§51. Έστω $\mathbf{F}, \mathbf{K}$ σώματα με $\mathbf{K} \supseteq \mathbf{F}$, $\mathbf{k_1}, \mathbf{k_2}, \ldots, \mathbf{k_n} \in \mathbf{K}$. Τότε,

$$(((\mathbf{F}(\mathbf{k_1}))(\mathbf{k_2}))\cdots)(\mathbf{k_n}) = \mathbf{F}(\mathbf{k_1}, \mathbf{k_2}, \ldots, \mathbf{k_n}).$$

Αρκεί να δείξουμε ότι $(F(k_1))(k_2) = F(k_1, k_2)$. Το αποτέλεσμα για την γενικότερη περίπτωση προκύπτει επαγωγικά. Από τον ορισμό του, το $F(k_1, k_2)$ περιέχει το k_1 και το F. Το $F(k_1, k_2)$ είναι υποσώμα του K που συμμετέχει στην τομή όλων των υποσωμάτων που περιέχουν τα k_1 και F. Το $F(k_1, k_2)$ περιέχει την τομή όλων των υποσωμάτων που περιέχουν τα k_1 και F. Άρα, $F(k_1) \subseteq F(k_1, k_2)$.

Επίσης, το $k_2 \in F(k_1, k_2)$. Το $F(k_1, k_2)$ είναι υποσώμα του K που συμμετέχει στην τομή όλων των υποσωμάτων που περιέχουν τα k_2 και $F(k_1)$. Το $F(k_1, k_2)$ περιέχει την τομή όλων των υποσωμάτων που περιέχουν τα k_2 και $F(k_1)$. Άρα, $(F(k_1))(k_2) \subseteq F(k_1, k_2)$.

Από τον ορισμό του, το $(F(k_1))(k_2)$ είναι η τομή όλων των υποσωμάτων του K που περιέχουν τα k_2 και $F(k_1)$. Άρα, τα k_2, $F(k_1)$ περιέχονται στο $(F(k_1))(k_2)$. Από τον ορισμό του, το $F(k_1)$ είναι η τομή όλων των υποσωμάτων του K που περιέχουν τα k_1 και F. Άρα, τα k_1, F περιέχονται στο $F(k_1) \subseteq (F(k_1))(k_2)$. Το $(F(k_1))(k_2)$ είναι υποσώμα του K που περιέχει τα k_1, k_2, F και συμμετέχει στην τομή όλων των υποσωμάτων του K που περιέχουν τα k_1, k_2, F. Το $(F(k_1))(k_2)$ περιέχει την τομή όλων των υποσωμάτων του K που περιέχουν τα k_1, k_2, F δηλαδή, $F(k_1, k_2) \subseteq (F(k_1))(k_2)$ και το συμπέρασμα προκύπτει.

§52. Έστω F, K σώματα με $K \supseteq F$, $k_1, k_2, \ldots, k_n \in K$. Στόχος μας τώρα είναι να προσδιορίσουμε την μορφή που έχουν τα στοιχεία του $F(k_1, k_2, \ldots, k_n)$. Για τον σκοπό αυτό προχωρούμε ως εξής. Αφού το $F(k_1, k_2, \ldots, k_n)$ είναι σώμα, περιέχει ως στοιχεία του όλες τις εκφράσεις,

$$\sum_{i_1=0}^{m_1} \sum_{i_2=0}^{m_2} \cdots \sum_{i_n=0}^{m_n} a_{i_1 i_2 \ldots i_n} \, k_1^{i_1} \, k_2^{i_2} \, \cdots \, k_n^{i_n}, \tag{29}$$

με $a_{i_1 i_2 \ldots i_n} \in F$, $m_j \in \mathbb{N}$, $j = 1, 2, \ldots, n$. Επίσης, περιέχει όλα τα κλάσματα με αριθμητή έκφραση από το (29) και παρονομαστή μη μηδενική έκφραση από το (29). Δηλαδή, αν θεωρήσουμε το σύνολο των πολυωνύμων πολλών μεταβλητών,

$$\begin{aligned} F[x_1, x_2, \ldots, x_n] \;=\; \Bigg\{ & \sum_{i_1=0}^{m_1} \sum_{i_2=0}^{m_2} \cdots \sum_{i_n=0}^{m_n} a_{i_1 i_2 \ldots i_n} \, x_1^{i_1} \, x_2^{i_2} \, \cdots \, x_n^{i_n} \; : \\ & a_{i_1 i_2 \ldots i_n} \in F, \; m_j \in \mathbb{N}, \; j = 1, 2, \ldots, n \Bigg\}, \end{aligned}$$

το $F(k_1, k_2, \ldots, k_n)$ περιέχει στοιχεία της μορφής,

$$\frac{f(k_1, k_2, \ldots, k_n)}{g(k_1, k_2, \ldots, k_n)},$$

με $f(x_1, x_2, \ldots, x_n), g(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$ και $g(k_1, k_2, \ldots, k_n) \neq 0$. Άρα,

$$\begin{aligned} F(k_1, k_2, \ldots, k_n) \;\supseteq\; \Bigg\{ & \frac{f(k_1, k_2, \ldots, k_n)}{g(k_1, k_2, \ldots, k_n)} \; : \; f(x_1, x_2, \ldots, x_n), \\ & g(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n], \end{aligned}$$

$$\left.\begin{array}{l}(x_1, x_2, \ldots, x_n) = (k_1, k_2, \ldots, k_n),\\ g(k_1, k_2, \ldots, k_n) \neq 0\end{array}\right\} = P(k_1, k_2, \ldots, k_n).$$

Είναι εμφανές ότι προσπαθούμε να δείξουμε ότι,

$$F(k_1, k_2, \ldots, k_n) = P(k_1, k_2, \ldots, k_n).$$

Για να συμβεί αυτό χρειάζεται να δείξουμε και ότι,

$$F(k_1, k_2, \ldots, k_n) \subseteq P(k_1, k_2, \ldots, k_n),$$

μιας και προηγουμένως δείξαμε ότι,

$$F(k_1, k_2, \ldots, k_n) \supseteq P(k_1, k_2, \ldots, k_n).$$

Για να δείξουμε λοιπόν $F(k_1, k_2, \ldots, k_n) \subseteq P(k_1, k_2, \ldots, k_n)$ πρέπει να δείξουμε ότι το $P(k_1, k_2, \ldots, k_n)$ έχει δύο ιδιότητες. Πρώτον ότι είναι υποσώμα του K και δεύτερον ότι περιέχει τα $k_1, k_2, \ldots, k_n$ και F. Τότε μόνο θα συμμετέχει στην τομή όλων των υποσωμάτων του K που περιέχουν τα $k_1, k_2, \ldots, k_n$ και F και άρα θα περιέχει την τομή αυτή που εξ΄ ορισμού είναι το $F(k_1, k_2, \ldots, k_n)$.

Για την πρώτη ιδιότητα. Επειδή έχουμε ήδη δείξει ότι $K \supseteq F(k_1, k_2, \ldots, k_n) \supseteq P(k_1, k_2, \ldots, k_n)$, προκύπτει αμέσως ότι το $P(k_1, k_2, \ldots, k_n) \subseteq K$. Τώρα πρέπει να δείξουμε ότι το $P(k_1, k_2, \ldots, k_n)$ εφοδιασμένο με τις πράξει του K είναι σώμα. Για να το δείξουμε αυτό θα χρειαστούμε ορισμένα ενδιάμεσα αποτελέσματα που παρουσιάζουμε στις επόμενες ενότητες.

§53. Έστω F σώμα. Το σύνολο πολυωνύμων σε n μεταβλητές,

$$\mathbf{F[x_1, x_2, \ldots, x_n]} = \left\{ \sum_{\mathbf{i_1}=\mathbf{0}}^{\mathbf{m_1}} \sum_{\mathbf{i_2}=\mathbf{0}}^{\mathbf{m_2}} \cdots \sum_{\mathbf{i_n}=\mathbf{0}}^{\mathbf{m_n}} \mathbf{a_{i_1 i_2 \ldots i_n}\, x_1^{i_1}\, x_2^{i_2} \cdots x_n^{i_n}} : \right.$$

$$\left. \mathbf{a_{i_1 i_2 \ldots i_n} \in F,\ m_j \in \mathbb{N},\ j = 1, 2, \ldots, n} \right\},$$

εφοδιασμένο με μία πράξη πρόσθεσης τέτοια ώστε το άθροισμα δύο πολυωνύμων του $\mathbf{F[x_1, x_2, \ldots, x_n]}$ να προκύπτει από την πρόσθεση των όμοιων μονωνύμων των πολυωνύμων αυτών, και μία πράξη πολλαπλασιασμού ώστε το γινόμενο των,

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

$$\mathbf{g(x)} = \sum_{\mathbf{i_1}=\mathbf{0}}^{\mathbf{k_1}} \sum_{\mathbf{i_2}=\mathbf{0}}^{\mathbf{k_2}} \cdots \sum_{\mathbf{i_n}=\mathbf{0}}^{\mathbf{k_n}} \mathbf{b_{i_1 i_2 \ldots i_n}\, x_1^{i_1}\, x_2^{i_2} \cdots x_n^{i_n}},$$

να είναι το πολυώνυμο που προκύπτει όταν κάθε μονώνυμο $\mathbf{a_{i_1 i_2 \ldots i_n}\, x_1^{i_1}\, x_2^{i_2} \cdots x_n^{i_n}}$ του $\mathbf{f(x)}$ πολλαπλασιασθεί επιμεριστικώς με κάθε μονώνυμο $\mathbf{b_{i_1 i_2 \ldots i_n}\, x_1^{i_1}\, x_2^{i_2} \cdots x_n^{i_n}}$ του $\mathbf{g(x)}$, είναι μεταθετικός δακτύλιος

με μονάδα.

Η απόδειξη ότι οι δύο πράξεις που ορίσθηκαν στο $F[x_1, x_2, \ldots, x_n]$ επαληθεύουν τις ιδιότητες (I1– I6) και τις (I8–I9) της §2 είναι επίπονη μεν αλλά άμεση εφαρμογή του ορισμού των πράξεων αυτών. Από την §8 το $F[x_1, x_2, \ldots, x_n]$ είναι μεταθετικός δακτύλιος με μονάδα.

§54. Έστω $\mathbf{F}, \mathbf{K}$ σώματα με $\mathbf{K} \supseteq \mathbf{F}$, $\mathbf{k_1}, \mathbf{k_2}, \ldots, \mathbf{k_n} \in \mathbf{K}$. Τότε το σύνολο,

$$\begin{aligned}\mathbf{F[k_1, k_2, \ldots, k_n]} &= \left\{ \sum_{\mathbf{i_1}=\mathbf{0}}^{\mathbf{m_1}} \sum_{\mathbf{i_2}=\mathbf{0}}^{\mathbf{m_2}} \cdots \sum_{\mathbf{i_n}=\mathbf{0}}^{\mathbf{m_n}} \mathbf{a_{i_1 i_2 \ldots i_n}}\, \mathbf{k_1^{i_1}}\, \mathbf{k_2^{i_2}} \cdots \mathbf{k_n^{i_n}} : \right. \\ &\qquad \left. \mathbf{a_{i_1 i_2 \ldots i_n}} \in \mathbf{F},\ \mathbf{m_j} \in \mathbb{N},\ \mathbf{j} = \mathbf{1}, \mathbf{2}, \ldots, \mathbf{n} \right\} = \\ &= \{\mathbf{f(k_1, k_2, \ldots, k_n)} : \mathbf{f(x_1, x_2, \ldots, x_n)} \in \\ &\quad \in \mathbf{F[x_1, x_2, \ldots, x_n]}, \mathbf{(x_1, x_2, \ldots, x_n)} = \\ &\quad = \mathbf{(k_1, k_2, \ldots, k_n)}\},\end{aligned}$$

είναι μεταθετικός υποδακτύλιος με μονάδα την μονάδα του $\mathbf{K}$.

Είναι εμφανές ότι το σύνολο $F[k_1, k_2, \ldots, k_n]$ προέρχεται από το σύνολο $F[x_1, x_2, \ldots, x_n]$ με αντικατάσταση των $x_1, x_2, \ldots, x_n$ με τα $k_1, k_2, \ldots, k_n$. Άρα το $F[k_1, k_2, \ldots, k_n]$ έχει την ίδια αλγεβρική δομή με αυτήν του $F[x_1, x_2, \ldots, x_n]$ μιας και η προαναφερθείσα αντικατάσταση δεν επηρεάζει την αλγεβρική συμπεριφορά των πράξεων του $F[x_1, x_2, \ldots, x_n]$. Απλώς, επειδή στην θέση των $x_1, x_2, \ldots, x_n$ έχουμε τοποθετήσει τα $k_1, k_2, \ldots, k_n$ οι πράξεις αθροισμάτων και γινομένων στις εκφράσεις $f(k_1, k_2, \ldots, k_n)$ αλλά και μεταξύ των $f(k_1, k_2, \ldots, k_n)$ είναι αυτές του K.

§55. Έστω $\mathbf{R}$ ένας μεταθετικός δακτύλιος με μονάδα με πρόσθεση $\oplus_{\mathbf{R}}$ και πολλαπλασιασμό $\odot_{\mathbf{R}}$. Συμβολίζουμε με $\mathbf{r^{-1}}$ το αντίστροφο του $\mathbf{r} \in \mathbf{R} - \{\mathbf{0}\}$, (το $\mathbf{r^{-1}}$ δεν ανήκει υποχρεωτικά στον $\mathbf{R}$ αλλά σε κάποιο σώμα που περιέχει τον $\mathbf{R}$). Το σύνολο,

$$\mathfrak{R} = \{\mathbf{a} \odot_{\mathbf{R}} \mathbf{b^{-1}} : \mathbf{a} \in \mathbf{R} \text{ και } \mathbf{b} \in \mathbf{R} - \{\mathbf{0}\}\},$$

εφοδιασμένο με τις πράξεις,

$$\begin{aligned}(\mathbf{a_1} \odot_{\mathbf{R}} \mathbf{b_1^{-1}}) \oplus_{\mathfrak{R}} (\mathbf{a_2} \odot_{\mathbf{R}} \mathbf{b_2^{-1}}) &= [(\mathbf{a_1} \odot_{\mathbf{R}} \mathbf{b_2}) \oplus_{\mathbf{R}} (\mathbf{a_2} \odot_{\mathbf{R}} \mathbf{b_1})] \odot_{\mathbf{R}} \\ &\quad \odot_{\mathbf{R}} (\mathbf{b_1} \odot_{\mathbf{R}} \mathbf{b_2})^{-\mathbf{1}}, \\ (\mathbf{a_1} \odot_{\mathbf{R}} \mathbf{b_1^{-1}}) \odot_{\mathfrak{R}} (\mathbf{a_2} \odot_{\mathbf{R}} \mathbf{b_2^{-1}}) &= (\mathbf{a_1} \odot_{\mathbf{R}} \mathbf{a_2}) \odot_{\mathbf{R}} (\mathbf{b_1} \odot_{\mathbf{R}} \mathbf{b_2})^{-\mathbf{1}},\end{aligned}$$

είναι σώμα και λέγεται το σώμα των πηλίκων του δακτυλίου $\mathbf{R}$. Εάν υιοθετήσουμε μάλιστα τον συμβολισμό, $(\mathbf{a} \odot_{\mathbf{R}} \mathbf{b^{-1}}) = \frac{\mathbf{a}}{\mathbf{b}}$, τότε οι $\oplus_{\mathfrak{R}}$ και $\odot_{\mathfrak{R}}$ μπορούν να γραφούν ως,

$$\begin{aligned}\frac{\mathbf{a_1}}{\mathbf{b_1}} \oplus_{\mathfrak{R}} \frac{\mathbf{a_2}}{\mathbf{b_2}} &= \frac{(\mathbf{a_1} \odot_{\mathbf{R}} \mathbf{b_2}) \oplus_{\mathbf{R}} (\mathbf{a_2} \odot_{\mathbf{R}} \mathbf{b_1})}{\mathbf{b_1} \odot_{\mathbf{R}} \mathbf{b_2}}, \\ \frac{\mathbf{a_1}}{\mathbf{b_1}} \odot_{\mathfrak{R}} \frac{\mathbf{a_2}}{\mathbf{b_2}} &= \frac{\mathbf{a_1} \odot_{\mathbf{R}} \mathbf{a_2}}{\mathbf{b_1} \odot_{\mathbf{R}} \mathbf{b_2}}.\end{aligned}$$

Για παράδειγμα, αν $R = \mathbb{Z}$ τότε $\mathfrak{R} = \mathbb{Q}$. Η απόδειξη ότι οι πράξεις του $\mathfrak{R}$ επαληθεύουν τις (I1–I9) είναι επίπονη μεν αλλά άμεση εφαρμογή του τρόπου ορισμού τους.

§56. Έστω $\mathbf{F, K}$ σώματα με $\mathbf{K \supseteq F}$, $\mathbf{k_1, k_2, \ldots, k_n \in K}$. Αν στην §55 θέσουμε $\mathbf{R = F[k_1, k_2, \ldots, k_n]}$ τότε από την §52 προκύπτει ότι το $\mathbf{P(k_1, k_2, \ldots, k_n)}$ είναι το σώμα των πηλίκων του $\mathbf{F[k_1, k_2, \ldots, k_n]}$ δηλαδή, σώμα και επειδή από την §52 $\mathbf{P(k_1, k_2, \ldots, k_n) \subseteq K}$ τελικώς, η πρώτη αλγεβρική ιδιότητα του $\mathbf{P(k_1, k_2, \ldots, k_n)}$ όπως απαιτήσαμε στην §52 απεδείχθη.

§57. Έστω $\mathbf{F, K}$ σώματα με $\mathbf{K \supseteq F}$, $\mathbf{k_1, k_2, \ldots, k_n \in K}$. Επειδή το $\mathbf{P(k_1, k_2, \ldots, k_n) \supseteq F[k_1, k_2, \ldots, k_n]}$ έπεται ότι το $\mathbf{P(k_1, k_2, \ldots, k_n)}$ περιέχει τα $\mathbf{k_1, k_2, \ldots, k_n}$ και $\mathbf{F}$. Και η δεύτερη αλγεβρική ιδιότητα του $\mathbf{P(k_1, k_2, \ldots, k_n)}$ όπως απαιτήσαμε στην §52 απεδείχθη. Άρα,

$$\begin{aligned}\mathbf{F(k_1, k_2, \ldots, k_n)} \;=\; \Bigg\{ & \frac{\mathbf{f(k_1, k_2, \ldots, k_n)}}{\mathbf{g(k_1, k_2, \ldots, k_n)}} \,:\, \mathbf{f(x_1, x_2, \ldots, x_n)}, \\ & \mathbf{g(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]}, \\ & \mathbf{(x_1, x_2, \ldots, x_n) = (k_1, k_2, \ldots, k_n)}, \\ & \mathbf{g(k_1, k_2, \ldots, k_n) \neq 0} \Bigg\}.\end{aligned}$$

§58. Έστω F σώμα. Όπως έχουμε ήδη αναφέρει στην §42, για κάθε πολυώνυμο του $F[x]$ υπάρχει μία επέκταση K/F η οποία περιέχει τις ρίζες του πολυωνύμου. Αυτό που μας ενδιαφέρει, είναι να προσδιορίσουμε την αλγεβρική μορφή αυτής της επέκτασης. Επίσης μας ενδιαφέρει πόσες τέτοιες επεκτάσεις υπάρχουν. Όλα αυτά μας ενδιαφέρουν γιατί τέτοιες επεκτάσεις περιέχουν τις ρίζες πολυωνύμων και εμείς ενδιαφερόμαστε για την αλγεβρική μορφή των ριζών αυτών ώστε να ξέρουμε αν το πολυώνυμο είναι επιλύσιμο δια ριζικών. Στις επόμενες ενότητες ασχολούμαστε με αυτό το ζήτημα.

§59. Έστω $\mathbf{F, K}$ σώματα, $\mathbf{K \supseteq F}$, $\mathbf{f(x) \in F[x]}$, $\mathbf{k_1, k_2, \ldots, k_n}$ οι διακεκριμένες ρίζες του $\mathbf{f(x)}$ δηλαδή, χωρίς την πολλαπλότητά τους. Αν $\mathbf{k_i \in K}$, $\mathbf{i = 1, 2, \ldots, n}$ τότε υπάρχει υποσώμα $\mathbf{M}$ του $\mathbf{K}$ ώστε,

- **το $\mathbf{M}$ είναι επέκταση του $\mathbf{F}$ και το $\mathbf{f(x)}$ να παραγοντοποιείται σε γινόμενο πρωτοβάθμιων παραγόντων του $\mathbf{M[x]}$,**
- **το $\mathbf{M}$ είναι η μικρότερη επέκταση του $\mathbf{F}$ εντός του $\mathbf{K}$ ώστε να συμβαίνει η προαναφερθείσα παραγοντοποίηση.**

Θέτουμε $M = F(k_1, k_2, \ldots, k_n)$. Το M είναι επέκταση του F και υποσώμα του K αφού το K περιέχει τα k_i και F. Το $M[x]$ περιέχει τα πολυώνυμα $x - k_i$, $i = 1, 2, \ldots, n$. Αν η πολλαπλότητα της k_1 είναι m_1, από την §21, το $(x - k_1)^{m_1}$ διαιρεί το $f(x)$ στο $M[x]$ και $f(x) = (x - k_1)^{m_1} q(x)$ με $q(x) \in M[x]$. Αν η πολλαπλότητα της k_2 είναι m_2, από την §21, το $(x - k_2)^{m_2}$ διαιρεί το $f(x)$ στο $M[x]$ και $f(x) = (x - k_2)^{m_2} p(x)$ με $p(x) \in M[x]$. Δηλαδή, $(x - k_2)^{m_2} p(x) = (x - k_1)^{m_1} q(x)$. Το $(x - k_2)^{m_2}$ διαιρεί το γινόμενο $(x - k_1)^{m_1} q(x)$

στο $M[x]$, ενώ τα $(x-k_1)^{m_1}$, $(x-k_2)^{m_2}$ είναι πρώτα μεταξύ τους. Από την §20, το $(x-k_2)^{m_2}$ διαιρεί το $q(x)$ στο $M[x]$ και $f(x)=(x-k_1)^{m_1}(x-k_2)^{m_2}a(x)$ με $a(x)\in M[x]$. Συνεχίζοντας με την ίδια λογική και μετά από πεπερασμένο πλήθος βημάτων εφ΄ όσον οι ρίζες είναι πεπερασμένου πλήθους καταλήγουμε στο ζητούμενο συμπέρασμα.

Έστω ότι υπάρχει επέκταση E/F ώστε, $F\subseteq E\subseteq F(k_1,k_2,\ldots,k_n)\subseteq K$ και το $f(x)$ παραγοντοποιείται σε γινόμενο πρωτοβάθμιων πολυωνύμων του $E[x]$. Τότε, το $E[x]$ περιέχει τα πολυώνυμα $x-k_i$, $i=1,2,\ldots,n$ και άρα το E περιέχει τα $k_1,k_2,\ldots,k_n$ και το F. Το E συμμετέχει στην τομή όλων των υποσωμάτων του K που περιέχουν τα $k_1,k_2,\ldots,k_n$ και το F. Το E περιέχει την τομή όλων των υποσωμάτων του K που περιέχουν τα $k_1,k_2,\ldots,k_n$ και το F που εξ΄ ορισμού η τομή αυτή είναι το $F(k_1,k_2,\ldots,k_n)=M$. Άρα, $E=M$.

§60. Έστω $\mathbf{F},\mathbf{K}$ σώματα, $\mathbf{K}\supseteq\mathbf{F}$, $\mathbf{f(x)}\in\mathbf{F[x]}$, $\mathbf{k_1,k_2,\ldots,k_n}\in\mathbf{K}$ οι διακεκριμένες ρίζες του $\mathbf{f(x)}$ δηλαδή, χωρίς την πολλαπλότητά τους. Το μοναδικό υποσώμα του $\mathbf{K}$, το $\mathbf{F(k_1,k_2,\ldots,k_n)}$, που όπως αποδείχθηκε στην §59 είναι η μικρότερη επέκταση του $\mathbf{F}$ που περιέχει τις ρίζες και το σώμα $\mathbf{F}$ των συντελεστών του $\mathbf{f(x)}$, λέγεται σώμα διαχωρισμού του $\mathbf{f(x)}$ στην επέκταση $\mathbf{K/F}$.

Είναι σαφές από την απόδειξη της §59 ότι όταν L/F, K/F είναι επεκτάσεις του F με $K\subseteq L$, το σώμα διαχωρισμού του $f(x)\in F[x]$ με ρίζες $k_1,k_2,\ldots,k_n\in K$ είναι το $F(k_1,k_2,\ldots,k_n)$ και ως προς την επέκταση K και ως προς την L. Πράγματι, αν στην απόδειξη της §59 στην θέση του K βάλουμε L και επαναλάβουμε τα ίδια βήματα προκύπτουν τα ίδια αποτελέσματα.

§61. Στην §39 δείξαμε ότι για κάθε ανάγωγο πολυώνυμο $p(x)$ στο $F[x]$, με F σώμα, υπάρχει σώμα $K=EF\cup F\supseteq F$, ώστε η επέκταση K/F να περιέχει μία ρίζα του $p(x)$. Από την απόδειξη αυτού του αποτελέσματος, είναι σαφές ότι αυτό το σώμα K δεν είναι μοναδικό. Αυτό γιατί, όπως προκύπτει από την §38, το σύνολο EF που περιέχει μία ρίζα του $p(x)$ και του οποίου τα στοιχεία βρίσκονται σε ένα προς ένα και επί αντιστοιχία με τα στοιχεία του $(F[x]/\langle p(x)\rangle)-FI$ δεν είναι μοναδικό.

Ένα σχετικό παράδειγμα ώστε τα πιο πάνω να γίνουν πιο σαφή είναι το εξής. Έστω $F=\mathbb{Q}$, $p(x)=x^2+1$. Τότε, $\mathbb{Q}[x]/\langle p(x)\rangle=\{(a\,x+b)+\langle p(x)\rangle\,:\,a,\,b\in\mathbb{Q}\}$. Ακολουθώντας τις §38, §39, για την δημιουργία του $EF=E\mathbb{Q}$ θα πρέπει πρώτα, να επιλέξουμε ένα στοιχείο εκτός $\mathbb{Q}$ το οποίο θα αντιστοιχηθεί στην ρίζα $x+\langle p(x)\rangle$ του $P(x)=\mathcal{F}(p(x))$ και θα είναι η ρίζα του $p(x)$ στο $E\mathbb{Q}\cup\mathbb{Q}$. Κατόπιν, θέτοντας δείκτη στο στοιχείο που επιλέξαμε τα στοιχεία του $\mathbb{Q}[x]/\langle p(x)\rangle-\mathbb{Q}I$ δημιουργούμε τα υπόλοιπα στοιχεία του $E\mathbb{Q}$.

Επειδή το στοιχείο εκτός $\mathbb{Q}$ που θα επιλέξουμε θα είναι ρίζα του $p(x)$, θα πρέπει αυτό το στοιχείο να έχει την ιδιότητα πολλαπλασιαζόμενο με τον εαυτό του να δίνει -1. Άρα, το στοιχείο εκτός $\mathbb{Q}$ που θα επιλέξουμε δεν είναι κάποιος από τους άρρητους αριθμούς.

Επιλέγουμε λοιπόν να συμβολίσουμε με I το στοιχείο αυτό δηλαδή, την ρίζα του $p(x)$ που είναι αντίστοιχη της ρίζας $x+\langle p(x)\rangle$ του $P(x)=\mathcal{F}(p(x))$. Τότε τα υπόλοιπα στοιχεία του $E\mathbb{Q}$ μπορούμε να τα συμβολίσουμε με $I_{(a\,x+b)+\langle p(x)\rangle}$, $a,b\in\mathbb{Q}$ και βρίσκονται όπως έχουμε τονίσει σε ένα προς ένα και επί αντιστοιχία με τα στοιχεία του $\mathbb{Q}[x]/\langle p(x)\rangle-\mathbb{Q}I$. Μάλιστα, για λόγους λειτουργικότητας των

συμβολισμών θα μπορούσαμε να συμφωνήσουμε ότι θα συμβολίζουμε με $i = I$ και με $a\,i + b = I_{(a\,x+b)+\langle p(x)\rangle}$, $a, b \in \mathbb{Q}$. Έτσι το $E\mathbb{Q} \cup \mathbb{Q} = \{a\,i + b \,:\, a, b \in \mathbb{Q}\}$.

Όμως, θα μπορούσαμε αντί για το I να επιλέξουμε ένα στοιχείο J εκτός $\mathbb{Q}$ για να αντιστοιχεί στο $x + \langle p(x)\rangle$ οπότε, $J_{(a\,x+b)+\langle p(x)\rangle}$, $a, b \in \mathbb{Q}$ είναι τα στοιχεία που αντιστοιχούν στα υπόλοιπα στοιχεία του $\mathbb{Q}[x]/\langle p(x)\rangle - \mathbb{Q}I$. Υιοθετώντας εκ΄ νέου συμβολισμό $j = J$, $a\,j + b = J_{(a\,x+b)+\langle p(x)\rangle}$ έχουμε ένα καινούριο σώμα, το $\{a\,j + b \,:\, a, b \in \mathbb{Q}\}$ που περιέχει μία ρίζα του $p(x)$. Το συμπέρασμα είναι το εξής,

Μία ρίζα ενός πολυωνύμου στην ουσία της παραμένει ίδια αλλά, η μορφή που λαμβάνει και με την οποία εμείς την αντιλαμβανόμαστε εξαρτάται από την επέκταση του σώματος των συντελεστών του πολυωνύμου εντός της οποίας δουλεύουμε. Η αλλαγή «εξωτερικού περιβλήματος» μίας ρίζας όμως δεν αλλάζει την αλγεβρική συμπεριφορά της.

§62. Έστω $\mathbf{F, K, L}$ σώματα, $\mathbf{K/F}$, $\mathbf{L/F}$ επεκτάσεις του $\mathbf{F}$ με $\mathbf{K \not\subseteq L}$ και $\mathbf{L \not\subseteq K}$, $\mathbf{f(x) \in F[x]}$, $\mathbf{k_1, k_2, \ldots, k_n \in K}$, $\mathbf{s_1, s_2, \ldots, s_n \in L}$, οι ρίζες του $\mathbf{f(x)}$ με την μορφή που αυτές λαμβάνουν εντός των επεκτάσεων $\mathbf{K/F}$, $\mathbf{L/F}$ αντιστοίχως. Τα σώματα διαχωρισμού του $\mathbf{f(x)}$ στις επεκτάσεις $\mathbf{K/F}$, $\mathbf{L/F}$ αντιστοίχως είναι ισομορφικά.

Από την §60 το $F(k_1, k_2, \ldots, k_n)$ είναι το μοναδικό σώμα διαχωρισμού του $f(x)$ στην επέκταση K/F και το $F(s_1, s_2, \ldots, s_n)$ είναι το μοναδικό σώμα διαχωρισμού του $f(x)$ στην επέκταση L/F. Θεωρούμε την συνάρτηση $h : F(k_1, k_2, \ldots, k_n) \mapsto F(s_1, s_2, \ldots, s_n)$ με,

$$h\left(\frac{f(k_1, k_2, \ldots, k_n)}{g(k_1, k_2, \ldots, k_n)}\right) = \frac{f(s_1, s_2, \ldots, s_n)}{g(s_1, s_2, \ldots, s_n)}\,.$$

Είναι σαφές από τον ορισμό της h ότι όλες οι αλγεβρικές ιδιότητες των στοιχείων του $F(k_1, k_2, \ldots, k_n)$ μεταφέρονται αυτούσιες σε αλγεβρικές ιδιότητες των στοιχείων του $F(s_1, s_2, \ldots, s_n)$ αφού, σε κάθε αλγεβρική ενέργεια μεταξύ στοιχείων του $F(k_1, k_2, \ldots, k_n)$ αρκεί να αντικαταστήσουμε τα $k_1, k_2, \ldots, k_n$ με τα $s_1, s_2, \ldots, s_n$ και θα έχουμε την ίδια ακριβώς αλγεβρική ενέργεια μεταξύ στοιχείων του $F(s_1, s_2, \ldots, s_n)$.

§63. Έστω $\mathbf{F, K}$ σώματα, $\mathbf{K \supseteq F}$. Η επέκταση $\mathbf{K/F}$ λέγεται αλγεβρική επέκταση του $\mathbf{F}$ αν για κάθε $\mathbf{k \in K}$ υπάρχει $\mathbf{f_k(x) \in F[x]}$ ώστε το $\mathbf{k}$ να είναι ρίζα του $\mathbf{f_k(x)}$. Σε αυτή την περίπτωση το $\mathbf{k}$ λέγεται αλγεβρικό στοιχείο του $\mathbf{K}$ επί του $\mathbf{F}$.

§64. Έστω $\mathbf{F, K}$ σώματα, $\mathbf{K \supseteq F}$, $\mathbf{K/F}$ πεπερασμένη επέκταση του $\mathbf{F}$. Θα δείξουμε ότι η $\mathbf{K/F}$ είναι αλγεβρική επέκταση του $\mathbf{F}$ και γράφεται στη μορφή $\mathbf{K = F(k_1, k_2, \ldots, k_n)}$ με $\mathbf{k_1, k_2, \ldots, k_n}$ αλγεβρικά στοιχεία του $\mathbf{K}$ επί του $\mathbf{F}$.

Έστω n η διάσταση της επέκτασης K/F. Τότε, $\{k_1, k_2, \ldots, k_n\}$ είναι μία βάση του K επί του F. Θεωρούμε τυχαίο $k \in K$. Από την §45 γνωρίζουμε ότι, το μέγιστο πλήθος γραμμικώς ανεξαρτήτων επί του F στοιχείων του K είναι n. Άρα, τα $n+1$ το πλήθος στοιχεία $1, k, k^2, \ldots, k^n$ του K είναι γραμμικώς εξαρτημένα επί του F. Υπάρχουν δηλαδή, $f_1, f_2, \ldots, f_n$ στοιχεία του F όχι όλα μηδέν

ώστε $\sum_{i=0}^{n} f_i\, k^i = 0$. Το k είναι αλγεβρικό επί του F ως ρίζα του πολυωνύμου $f(x) = \sum_{i=0}^{n} f_i\, x^i \in F[x]$.

Επειδή, το K περιέχει τα $k_1, k_2, \ldots, k_n$ και το F, το K συμμετέχει στην τομή όλων των υποσωμάτων του K που περιέχουν τα $k_1, k_2, \ldots, k_n$ και το F. Το K περιέχει την τομή όλων των υποσωμάτων του K που περιέχουν τα $k_1, k_2, \ldots, k_n$ και το F και $F(k_1, k_2, \ldots, k_n) \subseteq K$.

Κάθε στοιχείο του K είναι γραμμικός συνδυασμός επί του F των $k_1, k_2, \ldots, k_n$. Όμως το $F(k_1, k_2, \ldots, k_n)$ ως σώμα, περιέχει όλους τους γραμμικούς συνδυασμούς επί του F των $k_1, k_2, \ldots, k_n$. Άρα, και $F(k_1, k_2, \ldots, k_n) \supseteq K$. Αποδείξαμε ότι $K = F(k_1, k_2, \ldots, k_n)$ με $k_1, k_2, \ldots, k_n$ αλγεβρικά στοιχεία του K επί του F αφού η επέκταση K/F είναι αλγεβρική επί του F.

§65. Έστω $\mathbf{F}, \mathbf{K}$ σώματα, $\mathbf{K} \supseteq \mathbf{F}$ και $\mathbf{k}$ ένα αλγεβρικό στοιχείο του $\mathbf{K}$ επί του $\mathbf{F}$. Θεωρούμε τα ελαχίστου βαθμού $\mathbf{f(x)} \in \mathbf{F[x]}$ που έχουν το $\mathbf{k}$ ως ρίζα. Τα πολυώνυμα αυτά λέγονται ελάχιστα πολυώνυμα του $\mathbf{k}$ και είναι ανάγωγα στο $\mathbf{F[x]}$. Αν $\mathbf{f(x)}$, $\mathbf{g(x)}$ είναι ελάχιστα πολυώνυμα του $\mathbf{k}$ στο $\mathbf{F[x]}$, τότε υπάρχει $\mathbf{a} \in \mathbf{F} - \{\mathbf{0}\}$ ώστε $\mathbf{f(x) = a\, g(x)}$.

Έστω $f(x) \in F[x]$ ελάχιστο πολυώνυμο του k. Αν το $f(x)$ δεν είναι ανάγωγο στο $F[x]$ τότε υπάρχουν $b(x), d(x) \in F[x]$ με $1 \leq deg[b(x)], deg[d(x)] < deg[f(x)]$ ώστε $f(x) = b(x)\, d(x)$. Σε αυτή την περίπτωση, $0 = f(k) = b(k)\, d(k)$ από όπου προκύπτει ότι είτε $b(k) = 0$, είτε $d(k) = 0$ δηλαδή, το k είναι ρίζα κάποιου πολυωνύμου του $F[x]$ βαθμού μικρότερου του βαθμού του $f(x)$ άτοπο. Άρα, το $f(x)$ είναι ανάγωγο στο $F[x]$.

Έστω $f(x), g(x) \in F[x]$ δύο ελάχιστα πολυώνυμα του k. Τα $f(x)$, $g(x)$ έχουν τον ίδιο βαθμό. Η Ευκλείδεια διαίρεσή τους στο $F[x]$ μας δίνει, $f(x) = q(x)\, g(x) + r(x)$ με $q(x), r(x) \in F[x]$ και είτε $r(x) = 0$, είτε $0 \leq deg[r(x)] < deg[g(x)] = deg[f(x)]$. Αν $r(x) \neq 0$ τότε $f(k) = q(k)\, g(k) + r(k)$ έπεται $r(k) = 0$ και το k είναι ρίζα πολυωνύμου του $F[x]$ βαθμού μικρότερου του βαθμού του $f(x)$ άτοπο. Άρα, $r(x) = 0$ και $f(x) = q(x)\, g(x)$. Από την §24, $f(x) \neq 0$, $g(x) \neq 0$ και $q(x) \neq 0$ ενώ, $deg[f(x)] = deg[g(x)]$. Τα τελευταία συνεπάγονται ότι, $deg[q(x)] = 0$ και $q(x) = a \in F - \{0\}$.

§66. Έστω $\mathbf{F}, \mathbf{K}$ σώματα, $\mathbf{K} \supseteq \mathbf{F}$ και $\mathbf{k}$ ένα αλγεβρικό στοιχείο του $\mathbf{K}$ επί του $\mathbf{F}$ με βαθμό ελαχίστων πολυωνύμων $\mathbf{d}$. Θα δείξουμε ότι η επέκταση $\mathbf{F(k)}$ του $\mathbf{F}$ είναι πεπερασμένη, (και άρα αλγεβρική), με μία βάση να είναι η $\{\mathbf{1}, \mathbf{k}, \mathbf{k^2}, \ldots, \mathbf{k^{d-1}}\}$ και άρα, $\mathbf{(F(k) : F) = d}$.

Από την §57 παίρνουμε,

$$F(k) = \left\{ \frac{f(k)}{g(k)} \ : \ f(x), g(x) \in F[x],\, x = k,\, g(k) \neq 0 \right\} \supseteq F[k].$$

Στην περίπτωση που το k είναι αλγεβρικό επί του F θα δείξουμε ότι κάθε $g(k) \neq 0$ έχει αντίστροφο $1/g(k) = a(k)$ για κάποιο $a(x) \in F[x]$ οπότε, $F(k) = \{f(k)/g(k) = f(k)\, a(k) \ : \ f(x), a(x) \in F[x],\, x = k\} \subseteq F[k]$.

Έστω $p(x)$ ένα ελάχιστο πολυώνυμο του k. Από την §65 το $p(x)$ είναι ανάγωγο στο $F[x]$. Έστω $g(x) \in F[x]$ ώστε $g(k) \neq 0$. Αν $\delta(x) \in F[x]$ είναι ένας μέγιστος κοινός διαιρέτης των $g(x)$, $p(x)$ τότε είτε $deg[\delta(x)] \geq 1$, είτε $\delta(x) = \delta \in F - \{0\}$. Στην πρώτη περίπτωση, $p(x) = \delta(x)\, q_1(x)$ και $g(x) = \delta(x)\, q_2(x)$

με $q_1(x), q_2(x) \in F[x]$. Αν $deg[q_1(x)] \geq 1$, τότε το $p(x)$ δεν είναι ανάγωγο, άτοπο. Άρα $q_1(x) = q_1 \in F - \{0\}$ και $0 = p(k) = \delta(k)\, q_1$ επάγει $\delta(k) = 0$. Τότε όμως $g(k) = \delta(k)\, q_2(k) = 0$, άτοπο. Οπότε, $\delta(x) = \delta \in F - \{0\}$. Από την §15 τα $g(x)$, $p(x)$ είναι πρώτα μεταξύ τους και υπάρχουν $a(x), b(x) \in F[x]$ ώστε $a(x)\, g(x) + b(x)\, p(x) = 1$ ή $a(k)\, g(k) + b(k)\, p(k) = 1$ ή $a(k)\, g(k) = 1$ και το συμπέρασμα $F(k) \subseteq F[k]$ προκύπτει. Άρα, $F(k) \supseteq F[k]$, $F(k) \subseteq F[k]$ και $F(k) = F[k]$.

Τα στοιχεία του $F(k)$ είναι οι τιμές των πολυωνύμων του $F[x]$ όταν $x = k$. Έστω τυχαίο πολυώνυμο $f(x) \in F[x]$. Από την Ευκλείδεια διαίρεση των $f(x)$, $p(x)$ λαμβάνουμε $f(x) = p(x)\, q(x) + r(x)$ με $q(x) \in F[x]$ και είτε $r(x) = 0$ είτε $deg[r(x)] < deg[p(x)] = d$. Οπότε, $f(k) = p(k)\, q(k) + r(k) = r(k)$ και η τιμή του $f(x)$ όταν $x = k$ ισούται με $a_0 + a_1\, k + a_2\, k^2 + \cdots + a_{d-1}\, k^{d-1}$ με $a_0, a_1, \ldots, a_{d-1} \in F$ τους συντελεστές του $r(x)$. Δείξαμε λοιπόν ότι,

$$F(k) = \{a_0 + a_1\, k + a_2\, k^2 + \cdots + a_{d-1}\, k^{d-1} \,:\, a_0, a_1, \ldots, a_{d-1} \in F\},$$

δηλαδή, το σύνολο $\mathcal{K} = \{1, k, k^2, \ldots, k^{d-1}\}$ παράγει, επί του F, την επέκταση $F(k)$. Αρκεί να δείξουμε ότι τα στοιχεία του $\mathcal{K}$ είναι και γραμμικώς ανεξάρτητα επί του F. Έστω $a_0, a_1, \ldots, a_{d-1}$ στοιχεία του F όχι όλα μηδενικά. Αν $\sum_{i=0}^{d-1} a_i\, k^i = 0$, τότε το k είναι ρίζα του πολυωνύμου $\sum_{i=0}^{d-1} a_i\, x^i \in F[x]$ βαθμού μικρότερου του βαθμού των ελαχίστων πολυωνύμων του, άτοπο. Άρα, τα στοιχεία του $\mathcal{K}$ είναι γραμμικώς ανεξάρτητα επί του F και το συμπέρασμα απεδείχθη.

§67. Έστω $\mathbf{F, K}$ σώματα, $\mathbf{K \supseteq F}$, $\mathbf{k_1, k_2, \ldots, k_n \in K}$ αλγεβρικά επί του F. Η επέκταση $\mathbf{F(k_1)}$ λέγεται απλή αλγεβρική επέκταση του F. Η επέκταση $\mathbf{F(k_1, k_2, \ldots, k_n)}$ λέγεται πολλαπλή αλγεβρική επέκταση του F.

§68. Έστω $\mathbf{F, K}$ σώματα, $\mathbf{K \supseteq F}$, $\mathbf{k_1, k_2, \ldots, k_n \in K}$ αλγεβρικά επί του F. Η πολλαπλή αλγεβρική επέκταση $\mathbf{F(k_1, k_2, \ldots, k_n)}$ είναι πεπερασμένη επέκταση του F.

Θέτουμε $E_i = F(k_1, k_2, \ldots, k_i)$, $i = 1, 2, \ldots, n$. Από την §51, $E_i(k_{i+1}) = F(k_1, k_2, \ldots, k_{i+1}) = E_{i+1}$, $i = 1, 2, \ldots, n-1$. Επίσης, αν το k_{i+1} είναι αλγεβρικό επί του F, είναι αλγεβρικό και επί του E_i γιατί το πολυώνυμο $f(x) \in F[x]$ που έχει το k_{i+1} ως ρίζα, είναι και πολυώνυμο του $E_i[x]$ αφού $F \subseteq E_i$.

Από την §66 προκύπτει ότι το $E_{i+1} = E_i(k_{i+1})$ είναι πεπερασμένη επέκταση του E_i. Έστω $m_i = (E_{i+1} : E_i)$, $i = 1, 2, \ldots, n-1$. Επειδή,

$$F \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_{n-1} \subseteq E_n,$$

$$(E_n : F) \overset{\S 49}{=} (E_n : E_{n-1}) \cdots (E_2 : E_1)\, (E_1 : F) = m_{n-1} \cdots m_1\, (E_1 : F),$$

και το E_1 είναι πεπερασμένη επέκταση του F, (από §66), έπεται ότι η διάσταση της επέκτασης είναι πεπερασμένη.

§69. Έστω F σώμα. Από τις §64, §68 προκύπτει η ισοδυναμία: κάθε πεπερασμένη επέκταση του F είναι πολλαπλή αλγεβρική επέκταση του F και αντιστρόφως.

§70. Έστω F σώμα, $\mathbf{f(x), g(x) \in F[x]}$, $\mathbf{d(x) \in F[x]}$ ένας μέγιστος κοινός διαιρέτης των $\mathbf{f(x), g(x)}$. Κάθε ρίζα του $\mathbf{d(x)}$ είναι κοινή

ρίζα των $\mathbf{f(x), g(x)}$ και αντιστρόφως.

Υπάρχουν $a(x), b(x) \in F[x]$ ώστε $f(x) = d(x)\,a(x)$ και $g(x) = d(x)\,b(x)$ οπότε, όποια τιμή του x μηδενίζει το $d(x)$ μηδενίζει και τα $f(x)$, $g(x)$.

Αντιστρόφως, αν k είναι μία κοινή ρίζα των $f(x)$, $g(x)$ σε κάποιο σώμα $K \supseteq F$ τότε από την §17 το $x - k$ διαιρεί τα $f(x)$, $g(x)$ στο $K[x]$. Όπως γνωρίζουμε από την §14 το $d(x)$ είναι ένας μέγιστος κοινός διαιρέτης των $f(x)$, $g(x)$ και στο $K[x]$. Άρα, το $d(x)$ διαιρείται στο $K[x]$ από τους κοινούς διαιρέτες, στο $K[x]$, των $f(x)$, $g(x)$. Το $d(x)$ διαιρείται και από το $x - k$. Το k είναι ρίζα του $d(x)$.

§71. Έστω F σώμα, $\mathbf{p(x)} \in \mathbf{F[x]}$ ανάγωγο πολυώνυμο στο F[x]. Οι ρίζες του $\mathbf{p(x)}$ είναι διακεκριμένες δηλαδή, έχουν πολλαπλότητα ένα.

Έστω ότι η πολλαπλότητα m μίας ρίζας s του $p(x)$ είναι μεγαλύτερη ή ίση του δύο. Έστω ότι η s ανήκει σε κάποιο σώμα $K \supseteq F$. Από την §22 προκύπτει ότι η s είναι και ρίζα πολλαπλότητας $m - 1 \geq 1$ του $p'(x) \in F[x]$. Από την §70 προκύπτει ότι η s είναι ρίζα και του μέγιστου κοινού διαιρέτη, $d(x) \in F[x]$, των $p(x)$, $p'(x)$. Άρα, $deg[d(x)] \geq 1$ και $p(x) = d(x)\,a(x)$ με $a(x) \in F[x] - \{0\}$.

Αν $deg[d(x)] < deg[p(x)]$ τότε και $1 \leq deg[a(x)] < deg[p(x)]$ που σημαίνει ότι το $p(x)$ δεν είναι ανάγωγο στο $F[x]$, άτοπο. Άρα, $deg[d(x)] = deg[p(x)]$ και $deg[a(x)] = 0$ επάγοντας ότι $a(x) = a \in F - \{0\}$. Από την §11 προκύπτει ότι το $p(x)$ είναι επίσης ένας μέγιστος κοινός διαιρέτης των $p(x)$, $p'(x)$, άτοπο γιατί το $p(x)$ δεν μπορεί να διαιρεί το $p'(x)$ εφ΄ όσον $deg[p'(x)] < deg[p(x)]$.

§72. Έστω $\mathbf{F, K}$ σώματα, $\mathbf{K \supseteq F}$, $\mathbf{k_1, k_2} \in \mathbf{K}$ αλγεβρικά επί του F. Η πολλαπλή αλγεβρική επέκταση $\mathbf{F(k_1, k_2)}$ είναι απλή αλγεβρική επέκταση του F δηλαδή, υπάρχει $\mathbf{k_3} \in \mathbf{K}$ αλγεβρικό επί του F ώστε $\mathbf{F(k_1, k_2) = F(k_3)}$.

Έστω $f(x), g(x) \in F[x]$ ελάχιστα πολυώνυμα των k_1, k_2 αντιστοίχως με ρίζες του $f(x)$ τις $r_1 = k_1, r_2, \ldots, r_n$ και του $g(x)$ τις $s_1 = k_2, s_2, \ldots, s_t$ οι οποίες ανήκουν σε κάποιο σώμα $L \supseteq K \supseteq F$. Π.χ. $L = K(r_1, r_2, \ldots, r_n, s_1, s_2, \ldots, s_t)$. Από την §65 τα $f(x)$, $g(x)$ είναι ανάγωγα στο $F[x]$. Από την §71 προκύπτει ότι οι ρίζες των $f(x)$, $g(x)$ είναι διακεκριμένες μεταξύ τους αντιστοίχως.

Θεωρούμε τα $q_{ij} = \frac{r_i - r_1}{s_1 - s_j}$ με $i = 1, 2, \ldots, n$ και $j = 2, 3, \ldots, t$. Τα q_{ij} είναι πεπερασμένα το πλήθος, για την ακρίβεια $n\,(t-1)$ το πλήθος. Από τις §4, §5 προκύπτει ότι το $F_{\mathbb{Q}} \subseteq F$. Το $F_{\mathbb{Q}}$ από την κατασκευή του έχει άπειρο πλήθος στοιχείων άρα και το F έχει άπειρο πλήθος στοιχείων. Αυτό σημαίνει ότι υπάρχει $h \in F$ ώστε $h \neq q_{ij}$ για κάθε $i = 1, 2, \ldots, n$ και κάθε $j = 2, 3, \ldots, t$.

Θεωρούμε το $k_3 = k_1 + h\,k_2 \in K$. Θα δείξουμε ότι $F(k_1, k_2) = F(k_3)$. Το k_3 ανήκει στο $F(k_1, k_2)$ γιατί είναι αποτέλεσμα πράξεων στοιχείων του σώματος $F(k_1, k_2)$. Άρα, το σώμα $F(k_1, k_2)$ περιέχει το k_3 και το σώμα F. Το $F(k_1, k_2)$ συμμετέχει στην τομή όλων των υποσωμάτων του $F(k_1, k_2)$ που περιέχουν τα k_3 και F. Το $F(k_1, k_2)$ περιέχει την τομή όλων των υποσωμάτων του $F(k_1, k_2)$ που περιέχουν τα k_3 και F. Άρα, $F(k_1, k_2) \supseteq F(k_3)$.

Για να δείξουμε την σχέση $F(k_3) \supseteq F(k_1, k_2)$ αρκεί να δείξουμε ότι $k_1, k_2 \in F(k_3)$. Επειδή και $F \subseteq F(k_3)$, το $F(k_3)$ θα περιέχει την τομή όλων των υποσωμάτων του $F(k_3)$ που περιέχουν τα k_1, k_2 και F και το συμπέρασμα θα προκύψει. Για να δείξουμε ότι $k_1, k_2 \in F(k_3)$ αρκεί να δείξουμε ότι $k_2 \in F(k_3)$ γιατί τότε,

και το $k_1 = k_3 - h\,k_2 \in F(k_3)$ ως αποτέλεσμα πράξεων στοιχείων του σώματος $F(k_3)$.

Το ελάχιστο πολυώνυμο $g(x)$ του k_2 είναι και πολυώνυμο του $(F(k_3))[x]$ γιατί, $F[x] \subseteq (F(k_3))[x]$. Το πολυώνυμο $\tau(x) = f(k_3 - h\,x) \in (F(k_3))[x]$ ως σύνθεση, του ελαχίστου πολυωνύμου $f(x)$ του k_1 και του πολυωνύμου $k_3 - h\,x \in (F(k_3))[x]$. Τα $g(x)$, $\tau(x)$ έχουν το k_2 ως κοινή τους ρίζα αφού, $g(k_2) = g(s_1) = 0$ και $\tau(k_2) = f(k_3 - h\,k_2) = f(k_1) = f(r_1) = 0$.

Έστω $d(x) \in (F(k_3))[x]$ ένας μέγιστος κοινός διαιρέτης των $g(x)$, $\tau(x)$. Από την §70, το k_2 είναι ρίζα και του $d(x)$. Αν το $d(x)$ έχει και άλλες ρίζες πέραν της k_2, από την §70 προκύπτει ότι αυτές είναι κοινές ρίζες των $g(x)$ και $\tau(x)$. Οι κοινές ρίζες των $g(x)$ και $\tau(x)$ είναι εκείνες οι ρίζες s_j του $g(x)$ που επαληθεύουν και το $\tau(x)$. Ήδη γνωρίζουμε ότι η $s_1 = k_2$ είναι μία κοινή ρίζα των $g(x)$ και $\tau(x)$. Έστω s_j για κάποιο $j = 2, 3, \ldots, t$, μία άλλη κοινή ρίζα των $g(x)$ και $\tau(x)$. Τότε, $0 = \tau(s_j) = f(k_3 - h\,s_j)$ και το $k_3 - h\,s_j$ είναι ρίζα του $f(x)$ δηλαδή, $k_3 - h\,s_j \in \{r_1, r_2, \ldots, r_n\}$.

Έστω $k_3 - h\,s_j = r_i$ για κάποιο $i = 1, 2, \ldots, n$. Τότε,

$$k_3 - h\,s_j = r_i \Leftrightarrow k_1 + h\,k_2 - h\,s_j = r_i \Leftrightarrow r_1 + h\,(s_1 - s_j) = r_i \Leftrightarrow h = \frac{r_i - r_1}{s_1 - s_j}\,,$$

για κάποια $i \in \{1, 2, \ldots, n\}$, $j \in \{2, 3, \ldots, t\}$. Το τελευταίο επάγει ότι $h = q_{ij}$ για κάποια $i \in \{1, 2, \ldots, n\}$, $j \in \{2, 3, \ldots, t\}$, άτοπο από την επιλογή του h.

Άρα, τα $g(x)$, $\tau(x)$ δεν έχουν άλλες κοινές ρίζες παρά μόνο το k_2. Ως επακόλουθο, το $d(x)$ έχει μόνο μία ρίζα το k_2 και από την §42 μπορούμε να γράψουμε $d(x) = b\,(x - k_2)$, $b \in F(k_3) - \{0\}$ και $k_2 \in K \subseteq L$. Όμως $d(x) \in (F(k_3))[x]$. Αυτό σημαίνει ότι οι συντελεστές του $d(x)$ ανήκουν στο $F(k_3)$ οπότε, $b\,k_2 = z \in F(k_3)$. Τελικά, $k_2 = b^{-1}\,z \in F(k_3)$ και το ζητούμενο συμπέρασμα ότι $F(k_3) \supseteq F(k_1, k_2)$ προκύπτει.

Από την §68, η επέκταση $F(k_1, k_2)$ είναι πεπερασμένη. Από την §64, η επέκταση $F(k_1, k_2)$ είναι αλγεβρική. Άρα, το $F(k_3) = F(k_1, k_2)$ είναι αλγεβρική επέκταση του F και το $k_3 \in K$ είναι αλγεβρικό επί του F. Το τελικό συμπέρασμα αποδείχθη.

§73. Έστω $\mathbf{F, K}$ σώματα, $\mathbf{K \supseteq F}$, $\mathbf{k_1, k_2, \ldots, k_n \in K}$ αλγεβρικά επί του $\mathbf{F}$. Η πολλαπλή αλγεβρική επέκταση $\mathbf{F(k_1, k_2, \ldots, k_n)}$ είναι απλή αλγεβρική επέκταση του $\mathbf{F}$ δηλαδή, υπάρχει $\mathbf{k \in K}$ αλγεβρικό επί του $\mathbf{F}$ ώστε $\mathbf{F(k_1, k_2, \ldots, k_n) = F(k)}$.

Θα αποδείξουμε το αποτέλεσμα εφαρμόζοντας επαγωγή στο n. Για $n = 1$, το $F(k_1)$ είναι απλή αλγεβρική επέκταση του F από τις §66, §67. Υποθέτουμε το συμπέρασμα για n δηλαδή, υποθέτουμε ότι υπάρχει $k \in K$ αλγεβρικό επί του F ώστε $F(k_1, k_2, \ldots, k_n) = F(k)$. Θα αποδείξουμε το συμπέρασμα για $n + 1$. Από την §51,

$$F(k_1, k_2, \ldots, k_n, k_{n+1}) = (F(k_1, k_2, \ldots, k_n))(k_{n+1}). \tag{30}$$

Από την υπόθεση της επαγωγής, υπάρχει $k \in K$ αλγεβρικό επί του F ώστε

$$(F(k_1, k_2, \ldots, k_n))(k_{n+1}) = (F(k))(k_{n+1}). \tag{31}$$

Από την §51,

$$(F(k))(k_{n+1}) = F(k, k_{n+1}). \tag{32}$$

Από την §72 για $k_1 = k$, $k_2 = k_{n+1}$ υπάρχει $w \in K$ αλγεβρικό επί του F ώστε,

$$F(k, k_{n+1}) = F(w). \tag{33}$$

Από τις (30)–(33) το συμπέρασμα ισχύει και για $n+1$.

§74. Έστω $\mathbf{F}, \mathbf{K}$ σώματα, $\mathbf{K} \supseteq \mathbf{F}$, $\mathbf{k} \in \mathbf{K}$ αλγεβρικό επί του $\mathbf{F}$. Το $\mathbf{F(k)}$ είναι είναι μία πολλαπλή αλγεβρική επέκταση $\mathbf{F(k_1, k_2, \ldots, k_n)}$ του $\mathbf{F}$, με $\mathbf{k_1, k_2, \ldots, k_n} \in \mathbf{K}$ αλγεβρικά επί του $\mathbf{F}$.

Από την §66, το $F(k)$ είναι πεπερασμένη επέκταση του F. Από την §64 το $F(k)$ είναι πολλαπλή αλγεβρική επέκταση του F όπως απαιτεί το συμπέρασμα.

§75. Έστω $\mathbf{F}$ σώμα. Από τις §69, §73, §74 προκύπτουν οι ακόλουθες ισοδυναμίες.

- **Το $\mathbf{K}$ είναι πεπερασμένη επέκταση του $\mathbf{F}$.**

$$\Updownarrow$$

- **Το $\mathbf{K}$ είναι πολλαπλή αλγεβρική επέκταση του $\mathbf{F}$ δηλαδή, $\mathbf{K = F(k_1, k_2, \ldots, k_n)}$ με $\mathbf{k_1, k_2, \ldots, k_n} \in \mathbf{K}$ αλγεβρικά επί του $\mathbf{F}$.**

$$\Updownarrow$$

- **Το $\mathbf{K}$ είναι απλή αλγεβρική επέκταση του $\mathbf{F}$ δηλαδή, $\mathbf{K = F(k)}$ με $\mathbf{k} \in \mathbf{K}$ αλγεβρικό επί του $\mathbf{F}$.**

§76. Από την εμπειρία μας στην επίλυση πολυωνυμικών εξισώσεων με σώμα προέλευσης των συντελεστών του πολυωνύμου είτε το $\mathbb{Q}$, είτε το $\mathbb{R}$ προκύπτει ότι, οι τέσσερις πράξεις της αριθμητικής μεταξύ των συντελεστών του πολυωνύμου, δίνουν αποτέλεσμα εντός του σώματος προέλευσής τους και μόνο η εξαγωγή ρίζας κάποιας τάξης μπορεί να δώσει αποτέλεσμα εκτός του $\mathbb{Q}$ ή του $\mathbb{R}$.

Σε αυτή την περίπτωση, πρέπει το καινούριο στοιχείο που προέκυψε, και δεν ανήκει στο σώμα προέλευσης των συντελεστών του πολυωνύμου, να το προσαρτήσουμε στο σώμα προέλευσης των συντελεστών του πολυωνύμου ώστε να δημιουργήσουμε μία επέκταση αυτού και να μπορέσουμε να προχωρήσουμε περαιτέρω. Άρα, αν F είναι γενικά το σώμα προέλευσης των συντελεστών του πολυωνύμου μίας πολυωνυμικής εξίσωσης, χρειάζεται να αναφέρουμε την περίπτωση επεκτάσεων του F που προέρχονται από προσάρτηση στο F ριζών στοιχείων του F, οι οποίες ρίζες δεν ανήκουν στο F.

§77. Έστω $\mathbf{F}$ σώμα, $\mathbf{a} \in \mathbf{F}$, $\mathbf{d} \in \mathbb{N} - \{\mathbf{0}\}$. Από την §42 γνωρίζουμε ότι υπάρχει σώμα $\mathbf{A} \supseteq \mathbf{F}$ ώστε το $\mathbf{A}$ να περιέχει τις ρίζες του $\mathbf{f(x) = x^d - a}$ δηλαδή τις $\mathbf{d}$-οστές ρίζες του $\mathbf{a}$. Έστω $\sqrt[\mathbf{d}]{\mathbf{a}}$ μία από αυτές. Αφού υπάρχει πολυώνυμο του $\mathbf{F[x]}$ που έχει την $\sqrt[\mathbf{d}]{\mathbf{a}}$ ως ρίζα, υπάρχει και ελαχίστου βαθμού πολυώνυμο του $\mathbf{F[x]}$ που έχει την $\sqrt[\mathbf{d}]{\mathbf{a}}$ ως ρίζα και που από την §65 είδαμε ότι είναι ανάγωγο στο $\mathbf{F[x]}$. Από την §66 το σύνολο $\mathbf{F}(\sqrt[\mathbf{d}]{\mathbf{a}})$ είναι σώμα. Αν $\mathbf{d}$ είναι πρώτος αριθμός και η $\sqrt[\mathbf{d}]{\mathbf{a}}$ δεν ανήκει στο $\mathbf{F}$, το σώμα $\mathbf{F}(\sqrt[\mathbf{d}]{\mathbf{a}})$ λέγεται ριζική επέκταση του $\mathbf{F}$ ύψους 1.

Κατ' αναλογία λέμε ότι το σώμα $\mathbf{B}$ είναι ριζική επέκταση του σώματος $\mathbf{F}$ ύψους $\mathbf{n} \in \mathbb{N} - \{\mathbf{0}\}$ αν υπάρχει σειρά σωμάτων,

$$\mathbf{F = R_0 \subset R_1 \subset R_2 \subset \cdots \subset R_n = B},$$

ώστε για $\mathbf{i = 0, 1, \ldots, n-1}$ το σώμα $\mathbf{R_{i+1}}$ να είναι ριζική επέκταση ύψους 1 του σώματος $\mathbf{R_i}$ δηλαδή, $\mathbf{R_{i+1} = R_i(\sqrt[d_i]{a_i})}$ για κάποιο πρώτο αριθμό $\mathbf{d_i \in \mathbb{N} - \{0\}}$ και κάποιο $\mathbf{a_i \in R_i}$ ώστε $\mathbf{\sqrt[d_i]{a_i}}$ δεν ανήκει στο $\mathbf{R_i}$.

Τέλος λέμε ότι το σώμα F είναι ριζική επέκταση του εαυτού του ύψους 0. Όταν λέμε ότι ένα σώμα B είναι ριζική επέκταση του σώματος F θα εννοείται ριζική επέκταση κάποιου ύψους $\mathbf{n \in \mathbb{N}}$.

§78. Ο πιο πάνω ορισμός της ριζικής επέκτασης ενός σώματος F, μας επιτρέπει να διατυπώσουμε με αυστηρή Μαθηματική ορολογία, τι εννοούμε όταν λέμε ότι μία πολυωνυμική εξίσωση με συντελεστές από το F είναι επιλύσιμη δια ριζικών.

Λέμε ότι, μία πολυωνυμική εξίσωση με συντελεστές από ένα σώμα F είναι επιλύσιμη δια ριζικών όταν, κάθε λύση της εξίσωσης αυτής ανήκει σε σώμα B το οποίο είναι ριζική επέκταση του F δηλαδή, όταν υπάρχει ριζική επέκταση B του F ώστε το σώμα διαχωρισμού του πολυωνύμου της εξίσωσης να περιέχεται στο B.

§79. Από την §42 είναι σαφές ότι, κάθε συντελεστής του πολυωνύμου μίας πολυωνυμικής εξίσωσης μπορεί να εκφρασθεί συναρτήσει των ριζών του πολυωνύμου. Δηλαδή, υπάρχουν ευθείες συναρτησιακές σχέσεις ανάμεσα στους συντελεστές και τις ρίζες ενός πολυωνύμου. Στην περίπτωση των πολυωνύμων του $\mathbb{C}[x]$, οι σχέσεις αυτές μας είναι γνωστές ως τύποι του Viéte.

Οι τύποι αυτοί, παρουσιάζουν το ιδιαίτερο γνώρισμα να μένουν αμετάβλητοι όταν μεταθέσουμε τις ρίζες του πολυωνύμου. Στις επόμενες ενότητες ασχολούμαστε με αλγεβρικές παραστάσεις που παρουσιάζουν το ίδιο γνώρισμα με τους τύπους του Viéte. Αυτές οι παραστάσεις και η σύνδεσή τους με τις ρίζες πολυωνύμων είναι σημαντικές στην διαδικασία επίλυσης πολυωνυμικών εξισώσεων δια ριζικών.

Στοιχεία από την Θεωρία Συμμετρικών Πολυωνύμων και Συμμετρικών Ρητών Συναρτήσεων

§80. Έστω $\mathbf{n \in \mathbb{N} - \{0\}}$, $\mathcal{X} = \{\mathbf{x_1, x_2, \ldots, x_n}\}$. Κάθε μία, ένα προς ένα και επί συνάρτηση από το $\mathcal{X}$ στον εαυτό του λέγεται μετάθεση των $\mathbf{x_1, x_2, \ldots, x_n}$. Ο κανόνας μίας μετάθεσης $\sigma : \mathcal{X} \mapsto \mathcal{X}$ είναι της μορφής,

$$\begin{pmatrix} \mathbf{x_1} & \mathbf{x_2} & \cdots & \mathbf{x_n} \\ \sigma(\mathbf{x_1}) & \sigma(\mathbf{x_2}) & \cdots & \sigma(\mathbf{x_n}) \end{pmatrix} = \begin{pmatrix} \mathbf{x_1} & \mathbf{x_2} & \cdots & \mathbf{x_n} \\ \mathbf{x_{i_1}} & \mathbf{x_{i_2}} & \cdots & \mathbf{x_{i_n}} \end{pmatrix},$$

με $\mathbf{\{i_1, i_2, \ldots, i_n\} = \{1, 2, \ldots, n\}}$. Όταν,

$$\sigma(\mathbf{x_{i_1}}) = \mathbf{x_{i_2}}, \sigma(\mathbf{x_{i_2}}) = \mathbf{x_{i_3}}, \ldots, \sigma(\mathbf{x_{i_{m-1}}}) = \mathbf{x_{i_m}}, \sigma(\mathbf{x_{i_m}}) = \mathbf{x_{i_1}},$$

ενώ $\sigma(\mathbf{x_{i_j}}) = \mathbf{x_{i_j}}$, $\mathbf{i_j \in \{1, 2, \ldots, n\} - \{i_1, i_2, \ldots, i_m\}}$, συμβολίζουμε τον κανόνα της μετάθεσης με $(\mathbf{x_{i_1}\, x_{i_2} \cdots x_{i_m}})$ και την λέμε m κύκλο.

Αν γνωρίζουμε την αντιστοίχιση $\mathbf{1 \mapsto i_1}$, $\mathbf{2 \mapsto i_2}$, ..., $\mathbf{n \mapsto i_n}$ τότε γνωρίζουμε πλήρως και την αντιστοίχιση $\mathbf{x_j \mapsto x_{i_j}}$, $\mathbf{j = 1, 2, \ldots, n}$

και αντιστρόφως. Γι΄ αυτό, μπορούμε χωρίς βλάβη της γενικότητας, να θεωρούμε ως μετάθεση κάθε μία ένα προς ένα και επί συνάρτηση από το σύνολο $\mathbf{\Sigma_n = \{1, 2, \ldots, n\}}$ στον εαυτό του.

Πρακτικά, μία μετάθεση n το πλήθος στοιχείων είναι ένα «ανακάτεμα» μία επανατοποθέτησή τους σε διαφορετική σειρά. Από την Συνδυαστική γνωρίζουμε ότι υπάρχουν n! το πλήθος μεταθέσεις n στοιχείων.

§81. Το σύνολο $\mathbf{S_n}$ των μεταθέσεων n στοιχείων εφοδιασμένο με την πράξη της σύνθεσης συναρτήσεων είναι ομάδα.

Έστω $\sigma_1, \sigma_2 \in S_n$. Τότε από την §80 οι $\sigma_i : \Sigma_n \mapsto \Sigma_n$, $i = 1, 2$ είναι ένα προς ένα και επί. Οπότε και η σύνθεση $\sigma_1 \circ \sigma_2 : \Sigma_n \mapsto \Sigma_n$ και $\sigma_2 \circ \sigma_1 : \Sigma_n \mapsto \Sigma_n$ είναι ένα προς ένα και επί. Το S_n είναι κλειστό ως προς την σύνθεση μεταθέσεων.

Ουδέτερο στοιχείο είναι η συνάρτηση $id : \Sigma_n \mapsto \Sigma_n$ με $id(i) = i$. Κάθε στοιχείο του S_n ως ένα προς ένα και επί συνάρτηση αντιστρέφεται και η αντίστροφη συνάρτηση είναι επίσης ένα προς ένα και επί. Τέλος η σύνθεση μεταθέσεων είναι προσεταιριστική γιατί η σύνθεση συναρτήσεων είναι προσεταιριστική.

§82. Έστω F σώμα. Θα λέμε ότι το πολυώνυμο $\mathbf{f(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]}$ είναι συμμετρικό, (ως προς τα $\mathbf{x_1, x_2, \ldots, x_n}$), αν παραμένει αμετάβλητο όταν μεταθέσουμε τα $\mathbf{x_1, x_2, \ldots, x_n}$ καθ΄ οιονδήποτε τρόπο δηλαδή,

$$\begin{aligned} \mathbf{f}(\sigma(\mathbf{x_1}), \sigma(\mathbf{x_2}), \ldots, \sigma(\mathbf{x_n})) &\equiv \mathbf{f}(\mathbf{x}_{\sigma(1)}, \mathbf{x}_{\sigma(2)}, \ldots, \mathbf{x}_{\sigma(n)}) = \\ &= \mathbf{f}(\mathbf{x_1, x_2, \ldots, x_n}),\ \forall \sigma \in \mathbf{S_n}. \end{aligned}$$

Για παράδειγμα, το πολυώνυμο,

$$f(x_1, x_2, x_3) = x_1 + x_2 + x_3 + x_1\,x_2 + x_1\,x_3 + x_2\,x_3 + x_1\,x_2\,x_3 \in \mathbb{Q}[x_1, x_2, x_3],$$

είναι συμμετρικό γιατί,

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

§83. α). Έστω $\mathbf{(i_1, i_2, \ldots, i_n)}$, $\mathbf{(j_1, j_2, \ldots, j_n) \in \mathbb{N}^n}$. Ορίζουμε την σχέση διάταξης $\mathbf{\succ}$ στο $\mathbf{\mathbb{N}^n}$ με,

$$\mathbf{(i_1, i_2, \ldots, i_n) \succ (j_1, j_2, \ldots, j_n) \Leftrightarrow i_1 = j_1, \ldots, i_k = j_k, i_{k+1} > j_{k+1}},$$

με $\mathbf{k \in \{0, 1, \ldots, n-1\}}$ και λέμε ότι η n–άδα $\mathbf{(i_1, i_2, \ldots, i_n)}$ είναι μεγαλύτερη από την n–άδα $\mathbf{(j_1, j_2, \ldots, j_n)}$. Για $\mathbf{n = 1}$, η $(\succ)$ ταυτίζεται με την συνήθη σχέση διάταξης $(>)$.

β). Είναι προφανές από τον ορισμό της $\mathbf{\succ}$ ότι, αν $\mathbf{(i_1, i_2, \ldots, i_n) \succ (j_1, j_2, \ldots, j_n)}$ και $\mathbf{i_1 = j_1, \ldots, i_k = j_k, i_{k+1} > j_{k+1}}$ με $\mathbf{k \in \{1, \ldots, n-1\}}$ τότε, $\mathbf{(i_{k+1}, i_{k+2}, \ldots, i_n) \succ (j_{k+1}, j_{k+2}, \ldots, j_n)}$.

γ). Θα δείξουμε ότι, δεν υπάρχει ακολουθία $\mathbf{(a_m)_{m=1}^{\infty}}$ στοιχείων του $\mathbf{\mathbb{N}^n}$ που να είναι γνησίως φθίνουσα ως προς την $(\succ)$.

Εφαρμόζουμε επαγωγή στο n. Για $n = 1$, το $\mathbb{N}^n = \mathbb{N}$ και έστω $(a_m)_{m=1}^{\infty}$ ακολουθία στοιχείων του $\mathbb{N}$ που να είναι γνησίως φθίνουσα. Τότε, $a_1 > a_2 > \cdots >$

$a_m > \cdots$ με a_1 φυσικό αριθμό. Όμως, επειδή οι φυσικοί κατέρχονται ανά ένα, ξεκινώντας από τον a_1 και μετά από a_1+1 το πλήθος όρους θα έχουμε φτάσει στο μηδέν και πιο κάτω δεν θα μπορούμε να πάμε. Άρα η ακολουθία a_m δεν μπορεί να έχει άπειρους όρους και το συμπέρασμα ισχύει για $n = 1$.

Υποθέτουμε το συμπέρασμα για $n-1$, $n \geq 2$. Θα το αποδείξουμε και για $n \geq 2$. Έστω $(a_m)_{m=1}^{\infty}$ ακολουθία στοιχείων του $\mathbb{N}^n$ που να είναι γνησίως φθίνουσα ως προς την $(\succ)$. Τότε, $a_m = (i_{m1}, i_{m2}, \ldots, i_{mn})$ και $a_1 \succ a_2 \succ \cdots \succ a_m \succ \cdots$. Από τον ορισμό της $(\succ)$ αυτό σημαίνει ότι, $i_{11} \geq i_{21} \geq \cdots \geq i_{m1} \geq \cdots$. Όμως, στην ακολουθία φυσικών αριθμών $i_{11}, i_{21}, \ldots, i_{m1}, \ldots$ δεν μπορεί να υπάρχουν άπειροι το πλήθος όροι που να συγκροτούν γνησίως φθίνουσα υποακολουθία. Άρα, από έναν δείκτη $M \in \mathbb{N} - \{0\}$ και μετά έχουμε $i_{M1} = i_{(M+1)1} = \cdots = i_{m1} = \cdots$ δηλαδή, όλοι οι i_{m1} είναι ίσοι μεταξύ τους για $m = M, M+1, \ldots$.

Εφόσον έχουμε υποθέσει ότι η ακολουθία $(a_m)_{m=1}^{\infty}$ είναι γνησίως φθίνουσα, και η ακολουθία $(a_m)_{m=M}^{\infty}$ είναι γνησίως φθίνουσα γιατί αποτελείται από όλους τους όρους της $(a_m)_{m=1}^{\infty}$ χωρίς $M-1$ το, (πεπερασμένο), πλήθος αρχικούς όρους. Οπότε, $a_M \succ a_{M+1} \succ \cdots \succ a_m \succ \cdots$ με $i_{M1} = i_{(M+1)1} = \cdots = i_{m1} = \cdots$. Από το (β).) προκύπτει ότι, η ακολουθία $(b_m)_{m=M}^{\infty}$ στοιχείων του $\mathbb{N}^{n-1}$, με $b_m = (i_{m2}, i_{m3}, \ldots, i_{mn})$, είναι γνησίως φθίνουσα ως προς την $(\succ)$ άτοπο, από την υπόθεση της επαγωγής. Το συμπέρασμα προκύπτει.

§84. Έστω F σώμα, $\mathbf{f(x)} = \sum_{\mathbf{i_1=0}}^{\mathbf{m_1}} \sum_{\mathbf{i_2=0}}^{\mathbf{m_2}} \cdots \sum_{\mathbf{i_n=0}}^{\mathbf{m_n}} \mathbf{a_{i_1 i_2 \ldots i_n}}\, \mathbf{x_1^{i_1}}\, \mathbf{x_2^{i_2}} \cdots \mathbf{x_n^{i_n}}$ $\in \mathbf{F[x_1, x_2, \ldots, x_n]}$. Ορίζουμε βαθμό του $\mathbf{f(x)}$ ως προς την σχέση $(\succ)$ την μεγαλύτερη n–άδα $\mathbf{(i_1, i_2, \ldots, i_n)}$.

§85. Έστω F σώμα. Τα πολυώνυμα,

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

είναι προφανώς συμμετρικά και λέγονται στοιχειώδη συμμετρικά πολυώνυμα, (επί του F). Είναι προφανές ότι,

$$\begin{aligned}
\mathbf{deg}[\mathbf{e_1(x_1, x_2, \ldots, x_n)}] &= (\mathbf{1, 0, 0, \ldots, 0}), \\
\mathbf{deg}[\mathbf{e_2(x_1, x_2, \ldots, x_n)}] &= (\mathbf{1, 1, 0, \ldots, 0}), \\
&\vdots \quad \vdots \quad \vdots \\
\mathbf{deg}[\mathbf{e_k(x_1, x_2, \ldots, x_n)}] &= (\underbrace{\mathbf{1, \ldots, 1}}_{\mathbf{k-\text{όροι}}}, \mathbf{0, \ldots, 0}), \\
&\vdots \quad \vdots \quad \vdots \\
\mathbf{deg}[\mathbf{e_n(x_1, x_2, \ldots, x_n)}] &= (\mathbf{1, 1, \ldots, 1}),
\end{aligned}$$

§86. Έστω F σώμα, $\mathbf{f(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]}$ συμμετρικό πολυώνυμο. Υπάρχει πολυώνυμο $\mathbf{g(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]}$ ώστε,

$$\mathbf{f(x_1, x_2, \ldots, x_n) = g(e_1(x_1, \ldots, x_n), e_2(x_1, \ldots, x_n), \ldots, e_n(x_1, \ldots, x_n)),}$$

δηλαδή το $\mathbf{f(x_1, x_2, \ldots, x_n)}$ μπορεί να εκφρασθεί ως πολυώνυμο με συντελεστές από το F, των στοιχειωδών συμμετρικών πολυωνύμων.

Έστω ότι $deg[f(x_1, x_2, \ldots, x_n)] = (i_1, i_2, \ldots, i_n)$. Ο μεγιστοβάθμιος όρος του $f(x_1, x_2, \ldots, x_n)$, ως προς την $(\succ)$, είναι το μονώνυμο $a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$. Ως συμμετρικό, το $f(x_1, x_2, \ldots, x_n)$ περιέχει και όλα τα μονώνυμα που προκύπτουν από το μεγιστοβάθμιο, μέσω όλων των δυνατών μεταθέσεων των $x_1, x_2, \ldots, x_n$ ή ισοδυνάμως όλων των δυνατών μεταθέσεων των $i_1, i_2, \ldots, i_n$.

Ο βαθμός $(i_1, i_2, \ldots, i_n)$ είναι η μεγαλύτερη n–άδα, ως προς την $(\succ)$, ανάμεσα σε όλες τις n–άδες εκθετών των μονωνύμων του $f(x_1, x_2, \ldots, x_n)$ άρα και η μεγαλύτερη n–άδα, ως προς την $(\succ)$, ανάμεσα σε όλες τις n–άδες που προκύπτουν από τις δυνατές μεταθέσεις των $i_1, i_2, \ldots, i_n$.

Αυτό συνεπάγεται ότι, για τα i_j, $j = 1, 2, \ldots, n$ της $(i_1, i_2, \ldots, i_n)$ ισχύει $i_1 \geq i_2 \geq \cdots \geq i_n$. Γιατί, οποιαδήποτε άλλη μετάθεση των $i_1, i_2, \ldots, i_n$, στην πρώτη θέση θα έχει είτε το i_1 είτε μικρότερο του i_1. Αν έχει το i_1 στην δεύτερη θέση θα έχει είτε το i_2 είτε μικρότερο του i_2 και ούτω καθ' εξής.

Για την μεγαλύτερη n–άδα $(i_1, i_2, \ldots, i_n)$, θεωρούμε το πολυώνυμο $h(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$ με,

$$\begin{aligned} h(x_1, x_2, \ldots, x_n) &= [e_1(x_1, \ldots, x_n)]^{i_1 - i_2} [e_2(x_1, \ldots, x_n)]^{i_2 - i_3} \cdots \\ &\quad [e_{n-1}(x_1, \ldots, x_n)]^{i_{n-1} - i_n} [e_n(x_1, \ldots, x_n)]^{i_n}. \end{aligned}$$

Για $k = 1, 2, \ldots, n-1$ από την §85 προκύπτει ότι,

$$\begin{aligned} deg[e_k(x_1, \ldots, x_n)]^{i_k - i_{k+1}} &= \sum_{j=1}^{i_k - i_{k+1}} deg[e_k(x_1, \ldots, x_n)] = \\ &= \sum_{j=1}^{i_k - i_{k+1}} (\underbrace{1, \ldots, 1}_{k-\text{όροι}}, 0, \ldots, 0) = \\ &= (\underbrace{i_k - i_{k+1}, \ldots, i_k - i_{k+1}}_{k-\text{όροι}}, 0, \ldots, 0), \end{aligned}$$

$$deg[e_n(x_1, \ldots, x_n)]^{i_n} = \sum_{j=1}^{i_n} (1, 1, \ldots, 1) = (i_n, i_n, \ldots, i_n),$$

$$\begin{aligned} deg[h(x_1, \ldots, x_n)] &= (i_1 - i_2, 0, \ldots, 0) + (i_2 - i_3, i_2 - i_3, 0, \ldots, 0) + \\ &\quad + \ldots + (i_{n-1} - i_n, i_{n-1} - i_n, \ldots, i_{n-1} - i_n, 0) + \\ &\quad + (i_n, i_n, \ldots, i_n) = (i_1, i_2, \ldots, i_n). \end{aligned}$$

Από τον ορισμό των $e_k(x_1, x_2, \ldots, x_n)$ ο συντελεστής του μεγιστοβάθμιου όρου τους είναι 1. Άρα και ο συντελεστής του μεγιστοβάθμιου όρου του $h(x_1, x_2, \ldots, x_n)$ είναι 1. Οπότε, μπορούμε να γράψουμε,

$$h(x_1, x_2, \ldots, x_n) = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} + \text{ όροι μικρότερου βαθμού.}$$

Θεωρούμε το πολυώνυμο,

$$q_1(x_1,\ldots,x_n)=f(x_1,\ldots,x_n)-a_{i_1i_2\ldots i_n}\,h(x_1,\ldots,x_n)\in F[x_1,x_2,\ldots,x_n].$$

Είτε $q_1(x_1,x_2,\ldots,x_n)=0$ και το συμπέρασμα προκύπτει αμέσως αφού τότε $f(x_1,x_2,\ldots,x_n)=a_{i_1i_2\ldots i_n}\,h(x_1,x_2,\ldots,x_n)$ και το $h(x_1,x_2,\ldots,x_n)$ είναι πολυώνυμο με συντελεστές από το F, των στοιχειωδών συμμετρικών πολυωνύμων.

Είτε, $q_1(x_1,x_2,\ldots,x_n)\neq 0$ με $deg[q_1(x_1,x_2,\ldots,x_n)]\prec deg[f(x_1,x_2,\ldots,x_n)]$. Το $q_1(x_1,x_2,\ldots,x_n)$ είναι συμμετρικό πολυώνυμο ως διαφορά συμμετρικών πολυωνύμων. Επαναλαμβάνοντας την προηγηθείσα διαδικασία με το $q_1(x_1,x_2,\ldots,x_n)$ στην θέση του $f(x_1,x_2,\ldots,x_n)$ προκύπτει συμμετρικό πολυώνυμο $q_2(x_1,x_2,\ldots,x_n)$ για το οποίο ισχύει,

$$q_2(x_1,x_2,\ldots,x_n)=q_1(x_1,\ldots,x_n)-h_1(x_1,\ldots,x_n)\in F[x_1,x_2,\ldots,x_n],$$

με $h_1(x_1,\ldots,x_n)$ πολυώνυμο με συντελεστές από το F, των στοιχειωδών συμμετρικών πολυωνύμων και μεγιστοβάθμιο όρο, ως προς την $(\succ)$, τον μεγιστοβάθμιο όρο, ως προς την $(\succ)$, του $q_1(x_1,\ldots,x_n)$.

Είτε $q_2(x_1,x_2,\ldots,x_n)=0$ και το συμπέρασμα προκύπτει αμέσως αφού τότε $f(x_1,x_2,\ldots,x_n)=a_{i_1i_2\ldots i_n}\,h(x_1,x_2,\ldots,x_n)+h_1(x_1,x_2,\ldots,x_n)$ είναι άθροισμα πολυωνύμων με συντελεστές από το F, των στοιχειωδών συμμετρικών πολυωνύμων. Είτε, $q_2(x_1,x_2,\ldots,x_n)\neq 0$ με $deg[q_2(x_1,x_2,\ldots,x_n)]\prec deg[q_1(x_1,x_2,\ldots,x_n)]$.

Επαναλαμβάνοντας την διαδικασία με το $q_2(x_1,x_2,\ldots,x_n)$ στην θέση του $q_1(x_1,x_2,\ldots,x_n)$ και ούτω καθ΄ εξής, μετά από πεπερασμένο πλήθος βημάτων θα καταλήξουμε ότι το $f(x_1,x_2,\ldots,x_n)$ είναι άθροισμα πολυωνύμων με συντελεστές από το F, των στοιχειωδών συμμετρικών πολυωνύμων. Το ότι η επαναληπτική διαδικασία θα ολοκληρωθεί μετά από πεπερασμένο πλήθος βημάτων εξασφαλίζεται από την §83 (γ).). Αυτό γιατί το συμπέρασμα της §83 (γ).) μας λέει ότι η ακολουθία $deg[f(x_1,x_2,\ldots,x_n)]\succ deg[q_1(x_1,x_2,\ldots,x_n)]\succ\cdots$ δεν μπορεί να είναι άπειρη.

§87. Έστω $\mathbf{F},\mathbf{K},\mathbf{M}$ σώματα, με $\mathbf{K}\supseteq\mathbf{F}$, $\mathbf{M}\supseteq\mathbf{F}$, $\mathbf{p}(\mathbf{x_1},\mathbf{x_2},\ldots,\mathbf{x_n})\in\mathbf{F}[\mathbf{x_1},\mathbf{x_2},\ldots,\mathbf{x_n}]$, $\mathbf{q}(\mathbf{x_1},\mathbf{x_2},\ldots,\mathbf{x_n})\in\mathbf{F}[\mathbf{x_1},\mathbf{x_2},\ldots,\mathbf{x_n}]-\{\mathbf{0}\}$. Η συνάρτηση $\mathbf{f}:\mathbf{K}\mapsto\mathbf{M}$ με τύπο,

$$\mathbf{f}(\mathbf{x_1},\mathbf{x_2},\ldots,\mathbf{x_n})=\frac{\mathbf{p}(\mathbf{x_1},\mathbf{x_2},\ldots,\mathbf{x_n})}{\mathbf{q}(\mathbf{x_1},\mathbf{x_2},\ldots,\mathbf{x_n})},$$

λέγεται ρητή επί του σώματος $\mathbf{F}$. Το σύνολο των ρητών συναρτήσεων επί του σώματος $\mathbf{F}$ συμβολίζεται με $\mathbf{F}(\mathbf{x_1},\mathbf{x_2},\ldots,\mathbf{x_n})$ και εφοδιασμένο με την συνήθη πρόσθεση και τον συνήθη πολλαπλασιασμό ρητών αλγεβρικών παραστάσεων είναι σώμα.

Μία ρητή συνάρτηση είναι συμμετρική αν μένει αμετάβλητη σε όλες τις δυνατές μεταθέσεις των $\mathbf{x_1},\mathbf{x_2},\ldots,\mathbf{x_n}$.

§88. Έστω $\mathbf{F}$ σώμα, $\mathbf{f}(\mathbf{x_1},\mathbf{x_2},\ldots,\mathbf{x_n})\in\mathbf{F}(\mathbf{x_1},\mathbf{x_2},\ldots,\mathbf{x_n})$ μία συμμετρική ρητή συνάρτηση. Τότε υπάρχει ρητή συνάρτηση $\mathbf{g}(\mathbf{x_1},\mathbf{x_2},\ldots,\mathbf{x_n})\in\mathbf{F}(\mathbf{x_1},\mathbf{x_2},\ldots,\mathbf{x_n})$ ώστε,

$$\mathbf{f}(\mathbf{x_1},\mathbf{x_2},\ldots,\mathbf{x_n})=\mathbf{g}(\mathbf{e_1}(\mathbf{x_1},\ldots,\mathbf{x_n}),\mathbf{e_2}(\mathbf{x_1},\ldots,\mathbf{x_n}),\ldots,\mathbf{e_n}(\mathbf{x_1},\ldots,\mathbf{x_n})),$$

Από την §87 προκύπτει ότι,

$$f(x_1, x_2, \ldots, x_n) = \frac{p(x_1, x_2, \ldots, x_n)}{q(x_1, x_2, \ldots, x_n)},$$

με $p(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$, $q(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n] - \{0\}$. Αν το $q(x_1, x_2, \ldots, x_n)$ είναι συμμετρικό πολυώνυμο τότε και το $p(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_n)\, q(x_1, x_2, \ldots, x_n)$ είναι συμμετρικό πολυώνυμο ως γινόμενο συμμετρικών εκφράσεων. Από την §86 τα $p(x_1, x_2, \ldots, x_n)$, $q(x_1, x_2, \ldots, x_n)$ εκφράζονται ως πολυώνυμα με συντελεστές από το F των στοιχειωδών συμμετρικών πολυωνύμων και άρα ο λόγος τους είναι μία ρητή συνάρτηση $g(x_1, x_2, \ldots, x_n)$ με την ζητούμενη ιδιότητα.

Αν το $q(x_1, x_2, \ldots, x_n)$ δεν είναι συμμετρικό τότε οι διάφορες μεταθέσεις των $x_1, x_2, \ldots, x_n$ δημιουργούν τα διακεκριμένα μεταξύ τους και με το $q(x_1, x_2, \ldots, x_n)$ μη μηδενικά, (αφού το $q(x_1, x_2, \ldots, x_n) \neq 0$), πολυώνυμα του $F[x_1, x_2, \ldots, x_n]$, $q_1(x_1, x_2, \ldots, x_n)$, $q_2(x_1, x_2, \ldots, x_n)$, …, $q_m(x_1, x_2, \ldots, x_n)$. Το

$$Q(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)\, q_1(x_1, \ldots, x_n) \cdots q_m(x_1, \ldots, x_n),$$

είναι συμμετρικό πολυώνυμο ως προς τα $x_1, \ldots, x_n$ αφού κάθε μετάθεσή τους απλώς αλλάζει θέση στην σειρά των παραγόντων του $Q(x_1, \ldots, x_n)$. Τότε,

$$\begin{aligned} f(x_1, \ldots, x_n) &= \frac{p(x_1, \ldots, x_n)\, q_1(x_1, \ldots, x_n) \cdots q_m(x_1, \ldots, x_n)}{q(x_1, \ldots, x_n)\, q_1(x_1, \ldots, x_n) \cdots q_m(x_1, \ldots, x_n)} = \\ &= \frac{P(x_1, \ldots, x_n)}{Q(x_1, \ldots, x_n)}. \end{aligned}$$

Το $P(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)\, Q(x_1, \ldots, x_n)$ είναι συμμετρικό πολυώνυμο ως γινόμενο συμμετρικών εκφράσεων. Από την §86 τα $P(x_1, x_2, \ldots, x_n)$, $Q(x_1, x_2, \ldots, x_n)$ εκφράζονται ως πολυώνυμα με συντελεστές από το F των στοιχειωδών συμμετρικών πολυωνύμων και άρα ο λόγος τους είναι μία ρητή συνάρτηση $g(x_1, x_2, \ldots, x_n)$ με την ζητούμενη ιδιότητα.

Επιλυσιμότητα δια Ριζικών–Αναγκαία και Ικανή Συνθήκη Εισαγωγή στην Θεωρία Galois–Κίνητρα

§89. Στις επόμενες ενότητες, παρουσιάζουμε την απόδειξη της αναγκαίας και ικανής συνθήκης που πρέπει να ικανοποιείται, ώστε μία πολυωνυμική εξίσωση να είναι επιλύσιμη δια ριζικών. Θα παραθέσουμε πρώτα ένα παράδειγμα, μέσω του οποίου, γίνεται εμφανής η σκοπιμότητα της μετάβασης από την μελέτη της αλγεβρικής δομής πεπερασμένων επεκτάσεων του σώματος προέλευσης των συντελεστών του πολυωνύμου της εξίσωσης, στη μελέτη της αλγεβρικής δομής ομάδων αυτομορφισμών των προαναφερθέντων επεκτάσεων.

Θεωρούμε το πολυώνυμο $f(x) = x^5 - x^4 - 5\,x^3 + 5\,x^2 + 6\,x - 6 \in \mathbb{Q}[x]$. Είναι άμεσο να επαληθεύσουμε ότι οι ρίζες του είναι,

$$r_1 = 1,\ r_2 = \sqrt{2},\ r_3 = -\sqrt{2},\ r_4 = \sqrt{3},\ r_5 = -\sqrt{3}.$$

Η πολυωνυμική εξίσωση $f(x) = 0$ είναι επιλύσιμη δια ριζικών εφ' όσον, οι ρίζες του $f(x)$ έχουν την ζητούμενη, από τις απαιτήσεις της επιλυσιμότητας δια ριζικών, μορφή. Το σώμα διαχωρισμού του $f(x)$ εντός της επέκταση $\mathbb{R}/\mathbb{Q}$ είναι

το $\mathbb{Q}(\sqrt{2},-\sqrt{2},\sqrt{3},-\sqrt{3})=\mathbb{Q}(\sqrt{2},\sqrt{3})$ γιατί, όταν τα $\sqrt{2}$, $\sqrt{3}$ ανήκουν σε ένα σώμα τότε και τα αντίθετά τους ανήκουν στο σώμα αυτό.

Από την §51, $\mathbb{Q}(\sqrt{2},\sqrt{3})=(\mathbb{Q}(\sqrt{3}))(\sqrt{2})$ και η σειρά επεκτάσεων,

$$\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{3})\subseteq(\mathbb{Q}(\sqrt{3}))(\sqrt{2})=\mathbb{Q}(\sqrt{2},\sqrt{3}),\tag{34}$$

πληρεί τις απαιτήσεις των §77, §78. Πράγματι, το $\mathbb{Q}(\sqrt{3})$ είναι ριζική επέκταση του $\mathbb{Q}$ ύψους 1 και το $(\mathbb{Q}(\sqrt{3}))(\sqrt{2})$ είναι ριζική επέκταση του $\mathbb{Q}(\sqrt{3})$ επίσης ύψους 1 άρα, το $\mathbb{Q}(\sqrt{2},\sqrt{3})$ είναι ριζική επέκταση του $\mathbb{Q}$ ύψους 2 και το σώμα διαχωρισμού του $f(x)$ εντός της επέκτασης $\mathbb{R}/\mathbb{Q}$ περιέχεται σε αυτό.

Είναι λογικό, να σκεφτούμε να μελετήσουμε την αλγεβρική δομή της σειράς επεκτάσεων (34) αφού, η σειρά αυτή ικανοποιεί τις απαιτήσεις της επιλυσιμότητας δια ριζικών. Όμως, κάθε στοιχείο της σειράς αυτής είναι σώμα με απείρου πλήθους στοιχεία. Οι αλγεβρική δομή του κάθε σώματος, προκύπτει από τον συνδυασμό των τεσσάρων πράξεων, που ορίζονται σε αυτό, μεταξύ των απείρου πλήθους στοιχείων του. Η πολυπλοκότητα της έρευνας είναι μεγάλη.

Αν όμως καταφέρναμε, να περάσουμε τις πληροφορίες σχετικά με την αλγεβρική δομή των όρων της (34), σε αντίστοιχες πληροφορίες συνόλων σχετιζόμενων μεν με την (34), αλλά με πεπερασμένου πλήθους στοιχεία και μία μόνο πράξη να ορίζεται μεταξύ τους, τότε η διερεύνηση του τι είναι αυτό που καθιστά μία πολυωνυμική εξίσωση επιλύσιμη δια ριζικών θα ήταν ευκολότερη. Την δυνατότητα μετάβασης, από την μελέτη πιο πολύπλοκων αλγεβρικών δομών, όπως οι επεκτάσεις σωμάτων, σε πιο απλές, σε σχέση πάντα με την επιλυσιμότητα δια ριζικών, μας δίνει η έννοια των αυτομορφισμών επεκτάσεων σωμάτων.

Έστω συνάρτηση $\tau:\mathbb{Q}(\sqrt{2},\sqrt{3})\mapsto\mathbb{Q}(\sqrt{2},\sqrt{3})$ ώστε η τ να είναι ένα προς ένα και επί, $\tau(a+b)=\tau(a)+\tau(b)$, $\tau(a\,b)=\tau(a)\,\tau(b)$ για κάθε $a,b\in\mathbb{Q}(\sqrt{2},\sqrt{3})$, $\tau(g)=g$ για κάθε $g\in\mathbb{Q}$. Κάθε τέτοια συνάρτηση που είναι ισομορφισμός από το $\mathbb{Q}(\sqrt{2},\sqrt{3})$ στον εαυτό του και ο περιορισμός της στο $\mathbb{Q}$ είναι ταυτοτικός θα λέγεται αυτομορφισμός της επέκτασης $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$. Από τις ιδιότητες του τ παίρνουμε, $\tau(0)=\tau(0+0)=\tau(0)+\tau(0)$ οπότε, $\tau(0)=0$. Επίσης,

$$\begin{aligned}0 &= \tau(0)=\tau(f(r_i))=\tau(r_i^5-r_i^4-5\,r_i^3+5\,r_i^2+6\,r_i-6)=\\ &= \tau(r_i)^5-\tau(r_i)^4-5\,\tau(r_i)^3+5\,\tau(r_i)^2+6\,\tau(r_i)-6,\end{aligned}$$

με $i=1,2,3,4,5$. Ο τ απεικονίζει τις ρίζες του $f(x)$ εκ΄ νέου σε ρίζες του $f(x)$. Δηλαδή, ο τ μεταθέτει τις ρίζες του $f(x)$. Κάθε αυτομορφισμός της επέκτασης $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ αντιστοιχεί σε μία μετάθεση των ριζών του $f(x)$. Το αντίστροφο όμως δεν είναι αληθές. Κάθε μετάθεση των ριζών του $f(x)$ δεν αντιστοιχεί υποχρεωτικά σε έναν αυτομορφισμό της επέκτασης $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$.

Για παράδειγμα, αν η μετάθεση των r_i, $i=1,2,3,4,5$,

$$\begin{pmatrix} r_1 & r_2 & r_3 & r_4 & r_5\\ r_1 & r_4 & r_3 & r_2 & r_5\end{pmatrix}=\begin{pmatrix} 1 & \sqrt{2} & -\sqrt{2} & \sqrt{3} & -\sqrt{3}\\ 1 & \sqrt{3} & -\sqrt{2} & \sqrt{2} & -\sqrt{3}\end{pmatrix}$$

αντιστοιχούσε σε αυτομορφισμό της επέκτασης $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ τότε,

$$\tau(r_1)=r_1,\ \tau(r_2)=r_4,\ \tau(r_3)=r_3,\ \tau(r_4)=r_2,\ \tau(r_5)=r_5,$$

και, επειδή μία βάση της επέκτασης $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ είναι η $\{1,r_2,r_4,r_2\,r_4\}$, για τα στοιχεία $(a_1\,r_2+a_2\,r_4)$, $(b_1\,r_2+b_2\,r_4)$ του $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(r_2,r_4)$, $a_1,a_2,b_1,b_2\in$

$\mathbb{Q}$ θα είχαμε,

$$\begin{aligned} \tau((a_1\,r_2+a_2\,r_4)\,(b_1\,r_2+b_2\,r_4)) &= \\ =\tau((2\,a_1\,b_1+3\,a_2\,b_2)+(a_1\,b_2+a_2\,b_1)\,r_2\,r_4) &= \\ =\tau(2\,a_1\,b_1+3\,a_2\,b_2)+\tau(a_1\,b_2+a_2\,b_1)\,\tau(r_2)\,\tau(r_4) &= \\ =(2\,a_1\,b_1+3\,a_2\,b_2)+(a_1\,b_2+a_2\,b_1)\,r_4\,r_2, & \quad (35) \\ \tau(a_1\,r_2+a_2\,r_4)\,\tau(b_1\,r_2+b_2\,r_4) &= \\ (a_1\,r_4+a_2\,r_2)\,(b_1\,r_4+b_2\,r_2) &= \\ (3\,a_1\,b_1+2\,a_2\,b_2)+(a_1\,b_2+a_2\,b_1)\,r_4\,r_2. & \quad (36) \end{aligned}$$

Οι (35), (36) επάγουν,

$$\tau((a_1\,r_2+a_2\,r_4)\,(b_1\,r_2+b_2\,r_4)) \neq \tau(a_1\,r_2+a_2\,r_4)\,\tau(b_1\,r_2+b_2\,r_4),$$

άτοπο αφού υποθέσαμε ότι ο τ είναι αυτομορφισμός της επέκτασης $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$. Με αντίστοιχο έλεγχο μπορούμε να βρούμε ότι, από τις 5! μεταθέσεις των r_i, $i=1,2,3,4,5$ οι,

$$\tau_1 = Id = \begin{pmatrix} r_1 & r_2 & r_3 & r_4 & r_5 \\ r_1 & r_2 & r_3 & r_4 & r_5 \end{pmatrix} \quad , \quad \tau_2 = \begin{pmatrix} r_1 & r_2 & r_3 & r_4 & r_5 \\ r_1 & r_2 & r_3 & r_5 & r_4 \end{pmatrix},$$

$$\tau_3 = \begin{pmatrix} r_1 & r_2 & r_3 & r_4 & r_5 \\ r_1 & r_3 & r_2 & r_4 & r_5 \end{pmatrix} \quad , \quad \tau_4 = \begin{pmatrix} r_1 & r_2 & r_3 & r_4 & r_5 \\ r_1 & r_3 & r_2 & r_5 & r_4 \end{pmatrix},$$

αντιστοιχούν σε αυτομορφισμούς τ της επέκτασης $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$.

Το σύνολο $H=\{\tau_1,\tau_2,\tau_3,\tau_4\}$ εφοδιασμένο με την πράξη της σύνθεσης συναρτήσεων είναι μία ομάδα. Πράγματι, όπως προκύπτει από τον πιο κάτω πίνακα που παρουσιάζει τα αποτελέσματα $\tau_i\circ\tau_j$ για $(i,j)\in\{1,2,3,4\}\times\{1,2,3,4\}$,

$\circ$	τ_1	τ_2	τ_3	τ_4
τ_1	τ_1	τ_2	τ_3	τ_4
τ_2	τ_2	τ_1	τ_4	τ_3
τ_3	τ_3	τ_4	τ_1	τ_2
τ_4	τ_4	τ_3	τ_2	τ_1

το σύνολο H είναι κλειστό ως προς την πράξη $\circ$ και στην προκείμενη περίπτωση μάλιστα, η πράξη είναι μεταθετική. Το H περιέχει ουδέτερο στοιχείο ως προς την πράξη, τον $\tau_1=Id$. Κάθε στοιχείο του H είναι αντιστρέψιμο με $\tau_j^{-1}=\tau_j$, $j=1,2,3,4$. Η πράξη είναι προσετεριστική στο H γιατί γενικώς η σύνθεση συναρτήσεων είναι προσετεριστική πράξη.

Έστω K μία υποομάδα της ομάδας H. Επειδή η πράξη $\circ$ είναι μεταθετική προκύπτει ότι, για κάθε $\tau_i\in H$, $i=1,2,3,4$ και $\tau_j\in K$, $j=1,2,3,4$,

$$\tau_i\circ\tau_j\circ\tau_i^{-1}=\tau_j\circ\tau_i\circ\tau_i^{-1}=\tau_j\in K. \quad (37)$$

Υποομάδες μίας ομάδας με την ιδιότητα (37) λέγονται κανονικές. Άρα, κάθε υποομάδα της H είναι κανονική. Θεωρούμε τις υποομάδες $H_1=\{\tau_1,\tau_2\}$, $H_2=\{\tau_1\}$ της $H_0=H$. Κάθε H_{i+1} είναι κανονική υποομάδα της H_i, $i=0,1$. Αυτές μαζί με την H, συγκροτούν μία κανονική σειρά υποομάδων της H την,

$$\{Id\}=\{\tau_1\}\subset\{\tau_1,\tau_2\}\subset H \Leftrightarrow H_2\subset H_1\subset H_0, \quad (38)$$

Αν με $|A|$ συμβολίσουμε το πλήθος των στοιχείων που περιέχει ένα σύνολο A παίρνουμε ότι οι $|H_{i-1}|/|H_i|$, $i = 1, 2$ είναι πρώτοι αριθμοί. Πράγματι, $|H_0|/|H_1| = |H_1|/|H_2| = 2$.

Ανακεφαλαιώνοντας τα όσα προέκυψαν κατά την πορεία παρουσίασης του παραδείγματος έχουμε ότι,

- Η πολυωνυμική εξίσωση $f(x) = x^5 - x^4 - 5\,x^3 + 5\,x^2 + 6\,x - 6 = 0$ είναι επιλύσιμη δια ριζικών.

- Στο πολυώνυμο $f(x)$ της εξίσωσης, αντιστοιχεί η σειρά ριζικών επεκτάσεων του $\mathbb{Q}$,
$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq (\mathbb{Q}(\sqrt{3}))(\sqrt{2}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}),$$
όπου $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ είναι το σώμα διαχωρισμού του $f(x)$.

- Στην προαναφερθείσα σειρά ριζικών επεκτάσεων του $\mathbb{Q}$, αντιστοιχεί η κανονική σειρά,
$$H_2 \subset H_1 \subset H_0,$$
της ομάδας $H_0 = H$ των αυτομορφισμών του σώματος διαχωρισμού του $f(x)$ που είναι ταυτοτικοί στο $\mathbb{Q}$. Οι όροι της κανονικής σειράς, βρίσκονται σε ένα προς ένα αντιστοιχία με τους όρους της σειράς ριζικών επεκτάσεων.

Έτσι, αντί να ασχολούμαστε με αλγεβρικές δομές, όπως οι όροι μίας σειράς ριζικών επεκτάσεων, που έχουν απείρου πλήθους στοιχεία και τέσσερις πράξεις, μπορούμε να ασχολούμαστε με αλγεβρικές δομές, όπως οι όροι μίας κανονικής σειράς, που έχουν πεπερασμένου πλήθους στοιχεία και μία πράξη.

Όταν μία ομάδα με πεπερασμένου πλήθους στοιχεία διαθέτει μία κανονική σειρά με τις αλγεβρικές ιδιότητες της (38) λέγεται επιλύσιμη. Το παράδειγμα μας προδιαθέτει, για το ποια μπορεί να είναι η αναγκαία και ικανή συνθήκη ώστε μία πολυωνυμική εξίσωση να είναι επιλύσιμη δια ριζικών.

Έστω E, F σώματα, $f(x) \in F[x]$, E/F επέκταση του F τέτοια ώστε το E να περιέχει τις ρίζες του $f(x)$, L το σώμα διαχωρισμού του $f(x)$ στην επέκταση E/F, H η ομάδα αυτομορφισμών του σώματος L που είναι ταυτοτικοί στο F. Το παράδειγμα που εξετάσαμε σε αυτή την ενότητα μας προδιαθέτει για την επόμενη διατύπωση. Η πολυωνυμική εξίσωση $f(x) = 0$ είναι επιλύσιμη δια ριζικών αν και μόνο αν η ομάδα H είναι επιλύσιμη.

Στις επόμενες ενότητες θα αποδείξουμε αυτή την πρόταση αφού πρώτα, όπως προέκυψε μέσα από την εξέλιξη του παραδείγματος, αναφέρουμε αποτελέσματα από την θεωρεία ομάδων που είναι απαραίτητα.

Στοιχεία από την Θεωρία Ομάδων.

§90. Για λόγους απλοποίησης σε σχέση με τον ορισμό της §28 στα επόμενα θα συμβολίζουμε την πράξη $*$ μεταξύ των στοιχείων $\mathbf{a}, \mathbf{b}$ μίας ομάδας $\mathbf{G}$ ως $\mathbf{ab}$ αντί για $\mathbf{a} * \mathbf{b}$. Θα καλούμε την πράξη αυτή «γινόμενο». Θα συμβολίζουμε με $\mathbf{1}$ το ουδέτερο στοιχείο $\mathbf{e}$ της πράξης της ομάδας. Θα συμβολίζουμε με $\mathbf{a^{-1}}$ το στοιχείο της $\mathbf{G}$ για το οποίο ισχύει $\mathbf{a\,a^{-1} = a^{-1}\,a = 1}$ και θα το λέμε αντίστροφο

του a. Επίσης, όταν $\mathbf{n} \in \mathbb{Z}$ και $\mathbf{a} \in \mathbf{G}$ θα συμβολίζουμε με,

$$\mathbf{a^n} = \begin{cases} \underbrace{\mathbf{a\,a} \cdots \mathbf{a}}_{n \text{ παράγοντες}} & , \ \mathbf{n} \in \mathbb{N} - \{\mathbf{0}\}, \\ \mathbf{1} & , \ \mathbf{n} = \mathbf{0}, \\ \underbrace{\mathbf{a^{-1}\,a^{-1}} \cdots \mathbf{a^{-1}}}_{|n| \text{ παράγοντες}} & , \ -\mathbf{n} \in \mathbb{N} - \{\mathbf{0}\}. \end{cases}$$

Αν για κάθε $\mathbf{a, b} \in \mathbf{G}$ ισχύει $\mathbf{a\,b = b\,a}$ η ομάδα G θα λέγεται μεταθετική η Αβελιανή.

Συμβολίζουμε με $|\mathbf{G}|$ την τάξη δηλαδή, το πλήθος των στοιχείων που περιέχει μία ομάδα G.

Έστω τώρα, G ομάδα με πεπερασμένου πλήθους στοιχεία και H μία υποομάδα της G. Αν $H = G$, τότε η τάξη της υποομάδας H διαιρεί την τάξη της G. Αν $H \subset G$, τότε έστω $g_1 \in G - H$ και $g_1\,H = \{g_1\,h \,:\, h \in G\}$. Αν $g_1\,h \in H$ για κάποιο $h \in H$, τότε $g_1\,h = k$ για κάποιο $k \in H$ και $g_1 = k\,h^{-1} \in H$, άτοπο.

Αν $G = H \cup (g_1\,H)$, τότε τα στοιχεία της G κατανέμονται σε δύο ξένα μεταξύ τους σύνολα τα H και $g_1\,H$ που έχουν όμως το ίδιο πλήθος στοιχείων. Άρα, $|G| = 2\,|H|$ και εκ΄ νέου η τάξη της υποομάδας H διαιρεί την τάξη της G.

Αν $H \cup (g_1\,H) \subset G$ θεωρούμε $g_2 \in G - (H \cup (g_1\,H))$ και όπως πιο πάνω καταλήγουμε ότι, ανά δύο τα σύνολα H, $g_1\,H$, $g_2\,H$ δεν έχουν κοινά στοιχεία αλλά έχουν το ίδιο πλήθος στοιχείων. Οπότε, είτε $G = H \cup g_1\,H \cup g_2\,H$ και $|G| = 3\,|H|$, είτε $H \cup g_1\,H \cup g_2\,H \subset G$. Επειδή όμως η G έχει πεπερασμένου πλήθους στοιχεία, η πιο πάνω επαναλαμβανόμενη διαδικασία δεν μπορεί να συνεχίζεται επ΄ άπειρον και μετά από πεπερασμένο πλήθος βημάτων καταλήγουμε στην $G = H \cup (g_1\,H) \cup \cdots \cup (g_n\,H)$ με $g_i \in G - (H \cup (g_1\,H) \cup \cdots \cup (g_{i-1}\,H))$, $i = 1, 2, \ldots, n$, $g_0 = 1$ και ανά δύο τα $H, g_1\,H, \cdots, g_n\,H$ δεν έχουν κοινά στοιχεία ενώ έχουν το ίδιο πλήθος στοιχείων. Άρα, $|G| = (n+1)\,|H|$. Έχουμε αποδείξει το γνωστό από την Άλγεβρα θεώρημα Lagrange.

Έστω G ομάδα πεπερασμένης τάξης, H υποομάδα της G. Η τάξη της H διαιρεί την τάξη της G. Το πηλίκο της διαίρεσης $|\mathbf{G}|/|\mathbf{H}|$ λέγεται δείκτης της H στην G και συμβολίζεται με $[\mathbf{G} : \mathbf{H}]$.

§91. Μία ομάδα G θα λέγεται κυκλική με γεννήτορα το στοιχείο της a αν για κάθε στοιχείο $\mathbf{b} \in \mathbf{G}$ υπάρχει $\mathbf{n} \in \mathbb{Z}$ ώστε $\mathbf{b} = \mathbf{a^n}$. Σε αυτή την περίπτωση γράφουμε $\mathbf{G} = \langle \mathbf{a} \rangle$ και λέμε ότι η G παράγεται από το a.

§92. Κάθε υποομάδα μίας κυκλικής ομάδας $\mathbf{G} = \langle \mathbf{a} \rangle$ με πεπερασμένη τάξη είναι κυκλική.

Έστω H μία υποομάδα της G. Αν η H περιέχει ένα μόνο στοιχείο, αυτό είναι το ουδέτερο 1 και η H είναι κυκλική παραγόμενη από το 1. Αν η H περιέχει περισσότερα του ενός στοιχεία, αυτά θα είναι δυνάμεις του γεννήτορα a γιατί τα στοιχεία της G είναι δυνάμεις του γεννήτορα a και $H \subseteq G$. Έστω $a^k \neq 1$ ένα από τα στοιχεία της H. Επειδή η H είναι ομάδα και το a^{-k} είναι στοιχείο της. Άρα οπωσδήποτε υπάρχει στοιχείο της H με θετικό εκθέτη. Έστω m ο μικρότερος θετικός φυσικός αριθμός για τον οποίο ισχύει $a^m \in H$. Η κυκλική ομάδα $\langle a^m \rangle$ αποτελείται από δυνάμεις του a^m. Οι δυνάμεις a^m ανήκουν στην H γιατί αυτή

είναι ομάδα. Άρα, $\langle a^m\rangle \subseteq H$.

Έστω a^d ένα στοιχείο της H. Η Ευκλείδεια διαίρεση των d, m δίνει $d = m\,q + u$ με $q \in \mathbb{Z}$ και είτε $u = 0$ είτε $0 < u < m$. Αν $0 < u < m$ προκύπτει $a^d = (a^m)^q\,a^u$ που επάγει ότι $a^u = a^d\,(a^m)^{-q} \in H$ άτοπο γιατί δεν υπάρχει θετικός φυσικός u μικρότερος του m ώστε $a^u \in H$. Άρα $u = 0$ και $a^d = (a^m)^q$ που επάγει ότι $a^d \in \langle a^m\rangle$ δηλαδή, $H \subseteq \langle a^m\rangle$. Τελικώς $H = \langle a^m\rangle$ και το συμπέρασμα προκύπτει.

§93. Έστω ομάδα G. Ο μικρότερος θετικός φυσικός n, (αν υπάρχει), για τον οποίο ισχύει $\mathbf{a^n = 1}$ λέγεται τάξη του a. Αν τέτοιος n δεν υπάρχει λέμε ότι το a είναι άπειρης τάξης.

§94. Έστω ομάδα G και $\mathbf{g \in G}$ τάξης n. Τότε και $\mathbf{g^k = 1}$ για κάποιο $\mathbf{k \in \mathbb{N} - \{0\}}$ αν και μόνο αν ο n διαιρεί τον k.

Έστω $g^k = 1$ για κάποιο $k \in \mathbb{N} - \{0\}$. Από την Ευκλείδεια διαίρεση των k, n λαμβάνουμε, $k = n\,q + u$ με $q \in \mathbb{Z}$ και είτε $u = 0$ είτε $0 < u < n$. Αν $0 < u < n$ τότε, $1 = g^k = (g^n)^q\,g^u = g^u$ άτοπο γιατί ο n είναι ο μικρότερος θετικός φυσικός ώστε $g^n = 1$. Άρα $u = 0$ και ο n διαιρεί τον k. Έστω ότι ο n διαιρεί τον k. Τότε $k = n\,m$ με $m \in \mathbb{N} - \{0\}$ και $g^k = (g^n)^m = 1$.

§95. Αν $\mathbf{G = \langle a\rangle}$ είναι μία κυκλική ομάδα τάξης $\mathbf{n \in \mathbb{N} - \{0\}}$, (δηλαδή με n το πλήθος στοιχεία), τότε η τάξη του a είναι n.

Η G περιέχει το a άρα ως ομάδα περιέχει τα στοιχεία $1 = a^0, a, a^2, \ldots, a^{n-1}$. Αν υπάρχουν $m_1, m_2 \in \mathbb{N} - \{0\}$ ώστε $0 \le m_1 < m_2 \le n - 1$ και $a^{m_2} = a^{m_1}$ έπεται ότι $a^{m_2 - m_1} = 1$ με $0 < m_2 - m_1 < n$. Το a είναι γεννήτορας της G. Κάθε στοιχείο της G είναι δύναμη του a. Έστω $d \in \mathbb{Z}$. Η Ευκλείδεια διαίρεση των $d, m_2 - m_1$ δίνει $d = (m_2 - m_1)\,q + u$ με $q \in \mathbb{Z}$ και είτε $u = 0$ είτε $0 < u < m_2 - m_1$.

Αν $u = 0$ έπεται $a^d = (a^{m_2 - m_1})^q\,a^u = 1$. Αν $0 < u < m_2 - m_1$ έπεται $a^d = (a^{m_2 - m_1})^q\,a^u = a^u$. Σε κάθε περίπτωση, οι μόνες δυνάμεις του a εντός της G είναι οι $1, a, a^2, \ldots, a^{m_2 - m_1 - 1}$ δηλαδή, η G περιέχει ακριβώς $m_2 - m_1 \le n - 1$ στοιχεία άτοπο. Άρα οι n το πλήθος δυνάμεις $1, a, a^2, \ldots, a^{n-1}$ είναι διακεκριμένες και η $G = \{1, a, a^2, \ldots, a^{n-1}\}$.

Το $a^n \in G$. Αν $a^n \neq 1$ τότε $a^n = a^k$ για κάποιο $k \in \{1, 2, \ldots, n - 1\}$. Οπότε, $a^{n-k} = 1$ με $0 < n - k \le n - 1$. Αν εφαρμόσουμε για την περίπτωση αυτή λογική ίδια με αυτή της περίπτωσης $m_2 - m_1$, (θέτοντας $n - k$ στην θέση του $m_2 - m_1$), καταλήγουμε εκ΄ νέου σε άτοπο. Άρα, $a^n = 1$ και ο $n \in \mathbb{N}$ είναι ο μικρότερος για τον οποίο συμβαίνει αυτό.

§96. Αν $\mathbf{G = \langle a\rangle}$ είναι μία κυκλική ομάδα τάξης $\mathbf{n \in \mathbb{N}}$ τότε το $\mathbf{a^k}$ με $\mathbf{k \in \mathbb{N} - \{0\}}$ είναι γεννήτορας της G αν και μόνο αν ο μέγιστος κοινός διαιρέτης $\mathbf{(k, n)}$ των $\mathbf{k, n}$ είναι 1.

Αν το a^k είναι γεννήτορας της G τότε υπάρχει $m \in \mathbb{N} - \{0\}$ ώστε $a = (a^k)^m = a^{k\,m}$ από όπου έπεται $a^{k\,m-1} = 1$. Από την §95 προκύπτει ότι η τάξη του a είναι n και από την §94 ότι ο n διαιρεί τον $k\,m - 1$ δηλαδή, $k\,m - 1 = n\,t$ με $t \in \mathbb{Z}$ ή $m\,k + (-t)\,n = 1$. Είναι γνωστό από την Θεωρία Αριθμών ότι το τελευταίο συμπέρασμα επάγει το ζητούμενο αποτέλεσμα.

Έστω ότι ο $(k, n) = 1$. Από την Θεωρία Αριθμών είναι γνωστό ότι υπάρχουν

ακέραιοι m, h ώστε $m\,k + h\,n = 1$. Άρα, $a = a^{m\,k+h\,n} = a^{m\,k}\,(a^n)^h = (a^k)^m$ και ο γεννήτορας της G ανήκει στην κυκλική ομάδα $\langle a^k\rangle$. Όλες οι δυνάμεις του a ανήκουν στην $\langle a^k\rangle$ γιατί αυτή είναι ομάδα. Οπότε, $G \subseteq \langle a^k\rangle$. Όμως το a^k ανήκει στην G. Άρα και όλες οι δυνάμεις του a^k ανήκουν στην G γιατί αυτή είναι ομάδα. Οπότε, $\langle a^k\rangle \subseteq G$. Τελικώς $G = \langle a^k\rangle$ και το συμπέρασμα προκύπτει.

§97. Έστω $\mathbf{G = \langle a\rangle}$ μία κυκλική ομάδα. Αν η τάξη του a είναι $\mathbf{n \in \mathbb{N} - \{0\}}$, τότε η G περιέχει n το πλήθος στοιχεία δηλαδή, $\mathbf{G = \{1, a, a^2, \ldots, a^{n-1}\}}$.

Η G ως ομάδα περιέχει τα στοιχεία $1, a, a^2, \ldots, a^{n-1}$. Αν υπάρχουν $m_1, m_2 \in \mathbb{N} - \{0\}$ ώστε $0 \leq m_1 < m_2 \leq n-1$ και $a^{m_2} = a^{m_1}$ έπεται ότι $a^{m_2-m_1} = 1$ άτοπο γιατί ο n είναι ο μικρότερος θετικός φυσικός ώστε $a^n = 1$. Άρα τα $1, a, a^2, \ldots, a^{n-1}$ είναι n το πλήθος διακεκριμένα μεταξύ τους στοιχεία της G. Για κάθε άλλο στοιχείο a^d της G με $d \in \mathbb{Z}$ από την Ευκλείδεια διαίρεση των d, n ισχύει $a^d = (a^n)^q\,a^u = a^u$ με $q \in \mathbb{Z}$ και είτε $u = 0$ είτε $0 < u < n$. Άρα όλες οι δυνάμεις του a ανήκουν στο σύνολο $\{1, a, a^2, \ldots, a^{n-1}\}$ και η G ισούται με το σύνολο αυτό αφού αποτελείται από όλες τις δυνάμεις του a.

§98. Έστω $\mathbf{G = \langle a\rangle}$ μία κυκλική ομάδα τάξης $\mathbf{n \in \mathbb{N} - \{0\}}$ και $\mathbf{d \in \mathbb{N} - \{0\}}$ ένας διαιρέτης του n. Υπάρχει μοναδική υποομάδα της G με τάξη d. Η υποομάδα αυτή είναι κυκλική.

Αφού ο d είναι διαιρέτης του n, υπάρχει $m \in \mathbb{N} - \{0\}$ ώστε, $n = d\,m$. Θα δείξουμε ότι η κυκλική ομάδα $\langle a^m\rangle$ είναι η μόνη υποομάδα της G τάξης d. Από την §95 έπεται $a^n = 1$ και άρα $(a^m)^d = a^n = 1$. Αν υπάρχει $r \in \mathbb{N} - \{0\}$ ώστε $r < d$ και $(a^m)^r = a^{m\,r} = 1$, από την §94 ο n διαιρεί το $m\,r$ δηλαδή, $m\,r = n\,k = m\,d\,k$ με $k \in \mathbb{N} - \{0\}$. Άρα $r = d\,k$ άτοπο γιατί $0 < r < d$. Οπότε, d είναι ο μικρότερος θετικός φυσικός για τον οποίο ισχύει $(a^m)^d = 1$ και η τάξη του a^m είναι d.

Από την §97 προκύπτει ότι η ομάδα $\langle a^m\rangle = \{1, a^m, a^{2\,m}, \ldots, a^{(d-1)\,m}\}$ έχει τάξη d. Είναι προφανές ότι η ομάδα $\langle a^m\rangle$ είναι υποομάδα της G. Έστω $H \neq \langle a^m\rangle$ μία άλλη υποομάδα της G ώστε η τάξη της να είναι επίσης d. Από την §92 προκύπτει ότι η H είναι κυκλική άρα υπάρχει στοιχείο $a^t \in G$ με $t \in \mathbb{Z}$ ώστε $H = \langle a^t\rangle$. Από την §95 η τάξη του a^t είναι d δηλαδή, $1 = (a^t)^d = a^{t\,d}$ και από την §94 ο n διαιρεί το $t\,d$. Άρα $t\,d = n\,p = m\,d\,p$ με $p \in \mathbb{N} - \{0\}$. Οπότε, $t = m\,p$ και $H = \langle a^t\rangle = \langle (a^m)^p\rangle \subseteq \langle a^m\rangle$ δηλαδή, η H είναι υποσύνολο της $\langle a^m\rangle$ με ίδια τάξη με την $\langle a^m\rangle$. Αυτό σημαίνει ότι $H = \langle a^m\rangle$ και η $\langle a^m\rangle$ είναι η μοναδική υποομάδα της G τάξης d και είναι και κυκλική.

§99. Θεωρούμε την συνάρτηση $\phi : \mathbb{N} - \{0\} \mapsto \mathbb{N} - \{0\}$ ώστε $\phi(1) = 1$ και $\phi(\mathbf{n}) = |\{\mathbf{k} \in \mathbb{N} - \{0\} : 1 \leq \mathbf{k} < \mathbf{n}$ και $(\mathbf{k}, \mathbf{n}) = 1\}|$ δηλαδή, το πλήθος των θετικών φυσικών μικρότερων του n που είναι πρώτοι ως προς τον n. Η ϕ λέγεται συνάρτηση του Euler. Αν $\mathbf{n} \in \mathbb{N} - \{0\}$ τότε, $\mathbf{n} = \sum_{\mathbf{d|n}} \phi(\mathbf{d})$, $\mathbf{d > 0}$ όπου d|n σημαίνει ότι το d διαιρεί το n.

Έστω G μία ομάδα με πεπερασμένο πλήθος στοιχείων $n \in \mathbb{N} - \{0, 1\}$. Κάθε στοιχείο $a \neq 1$ της G έχει πεπερασμένη τάξη γιατί αλλιώς αν το a έχει άπειρη τάξη, η G σαν ομάδα θα περιέχει κάθε δύναμη του a άρα και τις δυνάμεις $1, a, a^2, \ldots, a^n, a^{n+1}, \ldots$ άτοπο γιατί η G έχει μόνο n το πλήθος στοιχεία. Έστω λοιπόν $k_a \in \mathbb{N} - \{0\}$ η τάξη του στοιχείου $a \neq 1$ της G. Από την §97 η κυκλική ομάδα $\langle a\rangle$ έχει k_a το πλήθος στοιχεία και επειδή η G σαν ομάδα περιέχει όλες τις

δυνάμεις του a προκύπτει ότι η $\langle a\rangle$ είναι υποομάδα της.

Ορίζουμε την σχέση $(\sim)$ μεταξύ των στοιχείων της G ως εξής, $a \sim b$ αν $\langle a\rangle = \langle b\rangle$. Για την σχέση αυτή ισχύει,

- $a \sim a$ γιατί $\langle a\rangle = \langle a\rangle$. Η $(\sim)$ είναι αυτοπαθής.
- Αν $a \sim b$ τότε $\langle a\rangle = \langle b\rangle$ και $\langle b\rangle = \langle a\rangle$ οπότε $b \sim a$. Η $(\sim)$ είναι συμμετρική.
- Αν $a \sim b$ και $b \sim g$ τότε $\langle a\rangle = \langle b\rangle$ και $\langle b\rangle = \langle g\rangle$ οπότε και $\langle a\rangle = \langle g\rangle$ άρα $a \sim g$. Η $(\sim)$ είναι μεταβατική.

Από τα πιο πάνω προκύπτει ότι η $(\sim)$ είναι σχέση ισοδυναμίας και διαμερίζει την G σε ξένες μεταξύ τους κλάσεις ισοδυναμίας. Συμβολίζουμε με $g(\langle a\rangle)$ την κλάση ισοδυναμίας της G που περιέχει όλα τα στοιχεία της που παράγουν την ίδια κυκλική υποομάδα $\langle a\rangle$. Άρα $G = \cup g(\langle a\rangle)$ όπου η ένωση λαμβάνεται στο πλήθος των κυκλικών υποομάδων $\langle a\rangle$ της G.

Έστω τώρα ότι η ομάδα G που επιλέξαμε είναι κυκλική με γεννήτορα h. Τότε όλα τα στοιχεία της είναι δυνάμεις του h. Από την θεωρία ομάδων γνωρίζουμε ότι η τάξη μίας υποομάδας διαιρεί την τάξη της G. Άρα σε κάθε υποομάδα της G αντιστοιχεί ένας διαιρέτης της τάξης $|G| = n$. Και από την §98 σε κάθε διαιρέτη του n αντιστοιχεί μία μοναδική κυκλική υποομάδα της G. Άρα, όλες οι υποομάδες της G είναι κυκλικές και τόσες όσοι οι θετικοί διαιρέτες του n. Έστω d ένας θετικός διαιρέτης της τάξης $|G| = n$. Από την §98 σε αυτό το d αντιστοιχεί μία κυκλική υποομάδα, η $\langle a\rangle_d$, της G τάξης d. Όλοι οι γεννήτορες της $\langle a\rangle_d$, ως στοιχεία της G που είναι, είναι της μορφής h^k με $(k, d) = 1$ από την §96. Άρα η τάξη $|g(\langle a\rangle_d)| = \phi(d)$. $G = \cup_{d|n} g(\langle a\rangle_d)$ οπότε $n = |G| = \sum_{d|n} |g(\langle a\rangle_d)| = \sum_{d|n} \phi(d)$.

§100. Έστω G μία ομάδα τάξης $\mathbf{n} \in \mathbb{N} - \{0\}$. Η G είναι κυκλική αν και μόνο αν σε κάθε θετικό διαιρέτη d του n αντιστοιχεί το πολύ μία κυκλική υποομάδα τάξης d.

Έστω ότι η G είναι κυκλική. Από την §98, σε κάθε θετικό διαιρέτη d του n αντιστοιχεί ακριβώς μία κυκλική υποομάδα τάξης d. Άρα το πολύ μία και το συμπέρασμα προκύπτει.

Έστω ότι σε κάθε θετικό διαιρέτη d του n αντιστοιχεί το πολύ μία κυκλική υποομάδα τάξης d. Στην απόδειξη της §99 είδαμε ότι $G = \cup g(\langle a\rangle)$ όπου η ένωση λαμβάνεται στο πλήθος των κυκλικών υποομάδων $\langle a\rangle$ της G. Τότε $n = |G| = \sum |g(\langle a\rangle)|$ όπου το άθροισμα λαμβάνεται στο πλήθος των κυκλικών υποομάδων $\langle a\rangle$ της G. Αφού σε κάθε θετικό διαιρέτη d του n αντιστοιχεί το πολύ μία κυκλική υποομάδα $\langle a\rangle$ τάξης d, σε κάθε θετικό διαιρέτη d του n αντιστοιχεί μία το πολύ κλάση ισοδυναμίας $g(\langle a\rangle)$ τάξης $\phi(d)$. Άρα $n = |G| = \sum |g(\langle a\rangle)| \leq \sum_{d|n} \phi(d) \overset{(\S 99)}{=} n$. Οπότε $\sum |g(\langle a\rangle)| = \sum_{d|n} \phi(d)$ όπου το άθροισμα το πρώτου μέλους λαμβάνεται στο πλήθος των κυκλικών υποομάδων $\langle a\rangle$ της G.

Τελικώς, αν υπάρχει θετικός διαιρέτης d του n στον οποίο δεν αντιστοιχεί κυκλική υποομάδα τάξης d τότε και η αντίστοιχη κλάση ισοδυναμίας είναι το κενό σύνολο και η τελευταία ισότητα παραβιάζεται, άτοπο. Άρα σε κάθε θετικό διαιρέτη d του n αντιστοιχεί ακριβώς μία κυκλική υποομάδα και στον θετικό διαιρέτη n του n αντιστοιχεί ακριβώς μία κυκλική υποομάδα τάξης n η G.

§101. Έστω a μη μηδενικό στοιχείο του σώματος F, $\mathbf{n} \in \mathbb{N} - \{0\}$.

Το πολυώνυμο $\mathbf{x^n - a}$ έχει n το πλήθος διακεκριμένες ρίζες σε κάποιο σώμα $\mathbf{K \supseteq F}$.

Από την §42 προκύπτει ότι υπάρχει σώμα $K \supseteq F$ που περιέχει όλες τις ρίζες του $a(x) = x^n - a$. Το $a(x) \in F[x] \subseteq K[x]$. Θεωρούμε την πρώτη παράγωγο του $a(x)$ το $a'(x) = n\,x^{n-1} \in F[x] \subseteq K[x]$. Από την μορφή τους, τα $a(x)$, $a'(x)$ είναι πρώτα μεταξύ τους στο $K[x]$. Έστω ότι μία τυχαία ρίζα του $a(x)$ π.χ. η $s \in K$ έχει πολλαπλότητα $m > 1$. Από την §22 η s είναι και ρίζα του $a'(x)$ πολλαπλότητας $m - 1 > 0$. Από την §21 προκύπτει ότι τα πολυώνυμα $(x-s)^m$ και $(x-s)^{m-1}$ του $K[x]$ διαιρούν τα $a(x)$, $a'(x)$ αντιστοίχως δηλαδή, το $x - s \in K[x]$ είναι κοινός παράγοντας των $a(x)$, $a'(x)$, άτοπο γιατί όπως αναφέραμε πιο πάνω αυτά είναι πρώτα μεταξύ τους στο $K[x]$. Άρα οι n ρίζες του $a(x)$ στο σώμα K είναι διακεκριμένες.

§102. Έστω F ένα σώμα, $\mathbf{F^* = F - \{0\}}$ η πολλαπλασιαστική του ομάδα, (εξαιρούμε το 0 γιατί δεν έχει πολλαπλασιαστικό αντίστροφο). Κάθε πεπερασμένη υποομάδα G της $\mathbf{F^*}$ είναι κυκλική.

Έστω $|G| = n \in \mathbb{N} - \{0\}$. Θα δείξουμε ότι σε κάθε θετικό διαιρέτη d του n αντιστοιχεί το πολύ μία κυκλική υποομάδα της G. Έστω d θετικός διαιρέτης του n στον οποίο αντιστοιχούν δύο διακεκριμένες κυκλικές υποομάδες της G οι K_1, K_2. Από την §98 έχουν τάξη d. Αυτό σημαίνει ότι $d > 1$ αλλιώς $d = 1$ έπεται $|K_1| = |K_2| = 1$ και $K_1 = K_2 = \{1\}$ το ουδέτερο πολλαπλασιαστικό στοιχείο του F, άτοπο γιατί οι K_1, K_2 είναι διακεκριμένες. Αφού $|K_1| = d > 1$ έπεται ότι ένας γεννήτορας της K_1 ο k_1 είναι διαφορετικός του 1. Από τις §95, §97 έπεται ότι $K_1 = \{1, k_1, k_1^2, \ldots, k_1^{d-1}\}$ που σημαίνει ότι τα $1, k_1, k_1^2, \ldots, k_1^{d-1}$ είναι διακεκριμένα μεταξύ τους.

Επίσης, από την §95 το k_1 έχει τάξη d άρα $(k_1^i)^d = (k_1^d)^i = 1$, $i = 0, 1, \ldots, d-1$ και οι $1, k_1, k_1^2, \ldots, k_1^{d-1}$ είναι d το πλήθος διακεκριμένες ρίζες του πολυωνύμου $f(x) = x^d - 1 \in F[x]$. Αφού οι K_1, K_2 είναι διακεκριμένες υπάρχει $k_2 \in K_2$ ώστε $k_2 \neq k_1^i$, $i = 0, 1, \ldots, d-1$. Αν h είναι ένας γεννήτορας της K_2 από την §95 το h έχει τάξη d αφού $|K_2| = d$. Οπότε, $k_2 = h^m$ με $m \in \mathbb{Z}$ και $k_2^d = (h^m)^d = (h^d)^m = 1$ επάγοντας ότι και το k_2 είναι μία ρίζα του $f(x)$ διαφορετική από τις προαναφερθείσες d το πλήθος. Τότε όμως το $f(x)$ θα έχει $d+1$ διακεκριμένες ρίζες, άτοπο από την §101. Άρα στον θετικό διαιρέτη d του n δεν αντιστοιχούν δύο διακεκριμένες κυκλικές υποομάδες της G τάξης d αλλά το πολύ μία. Από την §100 η G είναι κυκλική.

§103. Έστω F σώμα, $\mathbf{n \in \mathbb{N} - \{0\}}$, $\boldsymbol{\zeta_1, \zeta_2, \ldots, \zeta_n \in K}$ οι διακεκριμένες ρίζες του πολυωνύμου $\mathbf{a(x) = x^n - 1 \in F[x]}$ στο σώμα $\mathbf{K \supseteq F}$. Το σύνολο $\mathbf{\mathcal{Z} = \{\zeta_1, \zeta_2, \ldots, \zeta_n\} \subseteq K}$ εφοδιασμένο με τον πολλαπλασιασμό του σώματος K είναι κυκλική πολλαπλασιαστική υποομάδα της πολλαπλασιαστικής ομάδας $\mathbf{K^*}$ του K.

Για κάθε $\zeta_i, \zeta_j \in \mathcal{Z}$ προκύπτει ότι $(\zeta_i\,\zeta_j)^n - 1 = \zeta_i^n\,\zeta_j^n - 1 = 1 - 1 = 0$ που επάγει ότι $\zeta_i, \zeta_j \in \mathcal{Z}$ και το $\mathcal{Z}$ είναι κλειστό ως προς τον πολλαπλασιασμό. $1^n - 1 = 0$ και το 1 είναι ρίζα του $a(x)$ άρα το πολλαπλασιαστικό ουδέτερο ανήκει στο $\mathcal{Z}$. Ο πολλαπλασιασμός ανάμεσα στα στοιχεία του $\mathcal{Z}$ είναι προσετεριστικός γιατί το $\mathcal{Z}$ είναι υποσύνολο του K^* και ο πολλαπλασιασμός στο K^* είναι προσετεριστικός. Έστω

$\zeta_i \in \mathcal{Z}$. Αν $\zeta_i = 1$ τότε το ζ_i είναι αντιστρέψιμο και το αντίστροφο στοιχείο του είναι ο εαυτός του. Έστω $\zeta_i \neq 1$. Επειδή $(\zeta_i^m)^n - 1 = (\zeta_i^n)^m - 1 = 1^m - 1 = 0$ με $m \in \mathbb{N} - \{0\}$ έπεται ότι και τα ζ_i^m είναι ρίζες του $a(x)$ με $m \in \mathbb{N} - \{0\}$.

Όμως, το $a(x)$ έχει πεπερασμένο πλήθος ριζών άρα τα ζ_i^m δεν μπορεί να είναι διακεκριμένα για κάθε $m \in \mathbb{N} - \{0\}$. Άρα υπάρχουν $m_1, m_2 \in \mathbb{N} - \{0\}$ ώστε $m_1 > m_2$ και $\zeta_i^{m_1} = \zeta_i^{m_2}$ ή $\zeta_i^{m_1 - m_2} = 1$ ή $\zeta_i \zeta_i^{m_1 - m_2 - 1} = 1$ και το ζ_i είναι αντιστρέψιμο με αντίστροφο το $\zeta_i^{m_1 - m_2 - 1}$ το οποίο είναι στοιχείο του $\mathcal{Z}$ αφού όπως δείξαμε πιο πάνω τα ζ_i^m είναι ρίζες του $a(x)$ για κάθε $m \in \mathbb{N} - \{0\}$. Οπότε το $\mathcal{Z}$ είναι πολλαπλασιαστική υποομάδα της K^*. Επειδή η υποομάδα $\mathcal{Z}$ της K^* είναι πεπερασμένη από την §102 προκύπτει ότι η $\mathcal{Z}$ είναι κυκλική.

§104. Μία n–οστή ρίζα της μονάδας, (του πολλαπλασιαστικού ουδέτερου ενός σώματος), λέγεται πρωταρχική όταν, είναι γεννήτορας της κυκλικής ομάδας $\mathcal{Z}$ των n–οστών ριζών της μονάδας.

§105. Έστω p πρώτος αριθμός, G ομάδα τάξης p. Η G είναι κυκλική.

Η τάξη p της G έχει μόνο δύο διαιρέτες. Το 1 και το p. Υπάρχει μόνο μία υποομάδα της G τάξης ένα, αυτή που περιέχει το ουδέτερο 1 της πράξης της G και είναι κυκλική κατά τετριμμένο τρόπο. Υπάρχει μόνο μία υποομάδα της G τάξης p, η ίδια η G. Άρα, σε κάθε θετικό διαιρέτη d της τάξης της G, αντιστοιχεί το πολύ μία κυκλική υποομάδα της G τάξης d. Από την §100 προκύπτει το συμπέρασμα.

Μία άλλη απόδειξη του ίδιου αποτελέσματος χωρίς την χρήση της §100 είναι η εξής. Εφ΄ όσον ο p είναι πρώτος αριθμός, είναι μεγαλύτερος ή ίσος του 2. Άρα, η G έχει τουλάχιστον 2 διαφορετικά στοιχεία. Έστω $g \in G - \{1\}$. Τότε, τα $g, g^2, g^3, \ldots$ είναι στοιχεία της G. Επειδή η G έχει πεπερασμένη τάξη, δεν μπορεί τα $g, g^2, g^3, \ldots$ να είναι διακεκριμένα μεταξύ τους για κάθε εκθέτη. Υπάρχουν εκθέτες $1 \leq i < j$ ώστε $g^j = g^i$ ή $g^{j-i} = 1$. Έστω k ο μικρότερος θετικός ακέραιος ώστε $g^k = 1$ δηλαδή, η τάξη του g είναι k.

Από την §97 η κυκλική ομάδα $H = \langle g \rangle$ ισούται με $\{1, g, g^2, \ldots, g^{k-1}\}$ και είναι υποομάδα της G. Από την §90, και το θεώρημα Lagrange, η τάξη k της H διαιρεί την τάξη p της G. Αυτό σημαίνει ότι είτε $k = 1$ είτε $k = p$. $k = 1$ σημαίνει $1 = g^k = g$, άτοπο. Άρα, $k = p$ και $H = \{1, g, g^2, \ldots, g^{p-1}\}$. Η H είναι μία υποομάδα της G με ίδιου πλήθους στοιχεία. Η $H = G$ και το συμπέρασμα προκύπτει.

§106. Έστω G ομάδα, H υποομάδα της G. Θα λέμε ότι η H είναι κανονική υποομάδα της G αν για κάθε $\mathbf{g \in G}$ και κάθε $\mathbf{h \in H}$ ισχύει $\mathbf{g^{-1} h g \in H}$. Η τελευταία σχέση είναι ισοδύναμη με την $\mathbf{g h g^{-1} \in H}$ αφού στην θέση του g μπορούμε να θέσουμε $\mathbf{g^{-1}}$.

Έστω G ομάδα, $\mathbf{g \in G}$, H υποομάδα της G. Το σύνολο $\mathbf{g^{-1} H g = \{g^{-1} h g : h \in H\}}$ είναι υποομάδα της G και λέγεται συζυγής ομάδα της H. Από τον προηγούμενο ορισμό προκύπτει ότι, όταν η H είναι κανονική υποομάδα της G, ισούται με όλες τις συζυγής της ομάδες δηλαδή, $\mathbf{g^{-1} H g = H}$ για κάθε $\mathbf{g \in G}$ και αντιστρόφως.

Έστω $g^{-1} h_1 g$, $g^{-1} h_2 g$ στοιχεία της $g^{-1} H g$. $(g^{-1} h_1 g)(g^{-1} h_2 g) = g^{-1} h_1 h_2 g$ είναι στοιχείο της $g^{-1} H g$.

Το $1 \in H$ οπότε $g^{-1}\,1\,g = 1 \in g^{-1}\,H\,g$.
Για κάθε $g^{-1}\,h\,g \in g^{-1}\,H\,g$ το $g^{-1}\,h^{-1}\,g \in g^{-1}\,H\,g$ και $(g^{-1}\,h\,g)\,(g^{-1}\,h^{-1}\,g) = 1$.
Το $g^{-1}\,h^{-1}\,g \in g^{-1}\,H\,g$ είναι το αντίστροφο του $g^{-1}\,h\,g \in g^{-1}\,H\,g$.
Τέλος, η προσετεριστικότητα ισχύει για τα στοιχεία της $g^{-1}\,H\,g$ γιατί είναι στοιχεία της G.

§107. Έστω G ομάδα. Η G θα λέγεται επιλύσιμη αν υπάρχει, (κανονική), σειρά υποομάδων $\mathbf{G_i}$, $\mathbf{i = 0, 1, 2, \ldots, n}$ της G ώστε,

- $\mathbf{\{1\} = G_n \subseteq G_{n-1} \subseteq \cdots \subseteq G_0 = G}$,
- **Η $\mathbf{G_{i+1}}$ είναι κανονική υποομάδα της $\mathbf{G_i}$, $\mathbf{i = 0, 1, \ldots, n-1}$,**
- **Οι δείκτες $\mathbf{[G_i : G_{i+1}] = \frac{|G_i|}{|G_{i+1}|}}$, $\mathbf{i = 0, 1, \ldots, n-1}$ είναι πρώτοι αριθμοί.**

Θεωρούμε την τετριμμένη ομάδα $\mathbf{G = \{1\}}$ τετριμμένως επιλύσιμη.

§108. Έστω G κυκλική ομάδα πεπερασμένης τάξης. Η G είναι αβελιανή.

Από τον ορισμό της η $G = \{1, g, g^2, \ldots, g^{n-1}\}$. Έστω g^m, g^k δύο στοιχεία της G. Από την §90 $g^m\,g^k = g^{m+k} = g^{k+m} = g^k\,g^m$ και η G είναι αβελιανή.

§109. Έστω G αβελιανή ομάδα. Κάθε υποομάδα της G είναι κανονική.

Έστω H μία υποομάδα της G. Για κάθε $g \in G$ και $h \in H$ και λόγω της μεταθετικότητας των στοιχείων της G παίρνουμε $g^{-1}\,h\,g = h\,g^{-1}\,g = h \in H$ και η H είναι κανονική.

§110. Έστω G κυκλική ομάδα πεπερασμένης τάξης. Η G είναι επιλύσιμη.

Έστω n η τάξη της G και $n = p_1\,p_2\,\cdots\,p_m$ η ανάλυση του n σε γινόμενο πρώτων παραγόντων, (όχι όλων υποχρεωτικά διακεκριμένων). Αν $n = 1$, τότε $G = \{1\}$ και από την §107 η G είναι τετριμμένως επιλύσιμη.

Αν $n \geq 2$, από τις §95, §97 προκύπτει ότι, $G = \{1, g, g^2, \ldots, g^{n-1}\}$ για κάποιο $g \in G - \{1\}$. Θέτουμε $k_j = p_1\,p_2\,\cdots\,p_j$, $q_j = p_{j+1}\,\cdots\,p_m$, $j = 1, 2, \ldots, m$, $q_m = 1$. Τα q_j διαιρούν το n με πηλίκο k_j. Από την απόδειξη της §98 προκύπτει ότι, σε κάθε διαιρέτη q_j του n αντιστοιχεί μοναδική κυκλική υποομάδα $G_j = \langle g^{k_j} \rangle$ της G τάξης q_j.

Επειδή, $g^{k_{j+1}} = (g^{k_j})^{p_{j+1}}$ ο γεννήτορας, (άρα και κάθε στοιχείο), της G_{j+1} ανήκει στην G_j. Η G_{j+1} είναι υποομάδα της G_j, $j = 1, 2, \ldots, m-1$. Έχουμε λοιπόν μία σειρά υποομάδων της G την,

$$\{1\} = G_m \subset G_{m-1} \subset \cdots \subset G_2 \subset G_1 \subset G_0 = G,$$

με,

$$[G_j : G_{j+1}] = \begin{cases} \frac{|G_0|}{|G_1|} &= p_1, \\ \frac{|G_j|}{|G_{j+1}|} &= \frac{q_j}{q_{j+1}} = p_{j+1},\ j = 1, 2, \ldots, m-2, \\ \frac{|G_{m-1}|}{|G_m|} &= p_m, \end{cases}$$

πρώτους. Από την §108, η G είναι αβελιανή. Αυτό σημαίνει ότι όλα τα στοιχεία της G μετατίθενται μεταξύ τους. Άρα, και όλα τα στοιχεία κάθε υποομάδας της G, (ως στοιχεία της G), μετατίθενται μεταξύ τους. Κάθε υποομάδα της G είναι αβελιανή. Οι υποομάδες G_j της G, $j = 1, 2, \ldots, m$ είναι αβελιανές. Από την §109, η G_{j+1} είναι κανονική υποομάδα της G_j, $j = 0, 1, \ldots, m-1$. Δείξαμε ότι η G είναι επιλύσιμη.

§111. Έστω $(\mathbf{i_1\, i_2 \ldots i_n})$ ένας n κύκλος, $(\mathbf{j_1\, j_2 \ldots j_m})$ ένας m κύκλος. Οι κύκλοι λέγονται ξένοι αν $\{\mathbf{i_1\, i_2 \ldots i_n}\} \cap \{\mathbf{j_1\, j_2 \ldots j_m}\} = \emptyset$.

Έστω $(\mathbf{i_1\, i_2 \ldots i_n})$ ένας n κύκλος. $(\mathbf{i_1\, i_2 \ldots i_n})^{-1} = (\mathbf{i_n\, i_{n-1} \ldots i_1})$.

Κάθε 2 κύκλος λέγεται αντιμετάθεση.

Για λόγους απλοποίησης των συμβολισμών και της ορολογίας και κατ΄ αναλογία των όσον αναφέραμε στην §90, θα συμβολίζουμε την πράξη της σύνθεσης $\sigma \circ \tau$ των στοιχείων της ομάδας $\mathbf{S_n}$ με $\sigma\,\tau$ και θα την καλούμε «γινόμενο» των σ, τ.

§112. Κάθε μετάθεση γράφεται κατά μοναδικό τρόπο ως «γινόμενο» ξένων κύκλων.

Έστω $\sigma \in S_n$. Αν $n = 1$, τότε η σ γράφεται κατά τετριμμένο μοναδικό τρόπο ως 1 κύκλος αφού, το $\Sigma_1 = \{1\}$ και η μόνη μετάθεση των στοιχείων του Σ_1 είναι ο 1 κύκλος (1).

Έστω $n \geq 2$. Αν η $\sigma = id$, τότε γράφεται κατά μοναδικό τρόπο ως 1 κύκλος αφού,

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} = (1).$$

Αν $\sigma \in S_n - \{id\}$, τότε για $i_1 \in \Sigma_n$, τα $\sigma(i_1), \sigma^2(i_1), \ldots, \sigma^k(i_1), \ldots$ είναι στοιχεία του Σ_n. Όμως το Σ_n έχει πεπερασμένου πλήθους στοιχεία. Άρα, τα $\sigma(i_1), \sigma^2(i_1), \ldots, \sigma^k(i_1), \ldots$ δεν μπορεί να είναι διακεκριμένα για κάθε εκθέτη k και υπάρχουν $1 \leq t < d$ ώστε, $\sigma^d(i_1) = \sigma^t(i_1)$ ή $\sigma^{d-t}(i_1) = i_1$. Έστω r_1 ο μικρότερος θετικός ακέραιος ώστε $\sigma^{r_1}(i_1) = i_1$, . Τότε,

$$\sigma(i_1) = i_2,\ \sigma(i_2) = \sigma^2(i_1) = i_3,\ \ldots,\ \sigma(i_{r_1-1}) = \sigma^{r_1-1}(i_1) = i_{r_1},$$
$$\sigma(i_{r_1}) = \sigma^{r_1}(i_1) = i_1.$$

και ο περιορισμός της σ στο σύνολο $I_{r_1} = \{i_1, i_2, \ldots, i_{r_1}\}$ είναι ο r_1 κύκλος $\kappa_{r_1} = (i_1\, i_2 \ldots i_{r_1})$.

Παίρνουμε $j_1 \in \Sigma_n - I_{r_1}$. Ομοίως όπως προηγουμένως, υπάρχει θετικός ακέραιος r_2 και κύκλος $\kappa_{r_2} = (j_1\, j_2 \ldots j_{r_2})$ ώστε ο περιορισμός της σ στο σύνολο $I_{r_2} = \{j_1, j_2, \ldots, j_{r_2}\}$ να είναι ο r_2 κύκλος κ_{r_2}. Αν οι κ_{r_1}, κ_{r_2} δεν είναι ξένοι, τότε υπάρχουν $i_\mu \in I_{r_1}$ και $j_\nu \in I_{r_2}$ ώστε $i_\mu = j_\nu$ ή $\sigma^{\mu-1}(i_1) = \sigma^{\nu-1}(j_1)$. Χωρίς βλάβη της γενικότητας θεωρούμε $\mu \geq \nu$. Τότε, $\sigma^{\mu-\nu}(i_1) = j_1$. Από την Ευκλείδεια διαίρεση των $\mu - \nu$ και r_1 λαμβάνουμε, $\mu - \nu = r_1\, q + u$, $0 \leq u < r_1$. Σε κάθε περίπτωση,

$$j_1 = \sigma^{\mu-\nu}(i_1) = (\sigma^u\,(\sigma^{r_1})^q)(i_1) = (\sigma^u\, \underbrace{\sigma^{r_1} \cdots \sigma^{r_1}}_{q\ \text{όροι}})(i_1) = \sigma^u(i_1) \in I_{r_1},$$

άτοπο, γιατί επιλέξαμε το $j_1 \in \Sigma_n - I_{r_1}$. Οι κ_{r_1}, κ_{r_2} είναι ξένοι. Επειδή, το Σ_n έχει πεπερασμένου πλήθους στοιχεία, επαναλαμβάνοντας την πιο πάνω διαδικασία,

προκύπτει ότι υπάρχουν δείκτες r_ℓ, $\ell = 1, 2, \ldots, m$, σύνολα I_{r_ℓ} ξένα ανά δύο ώστε $\sum_n = \cup_{\ell=1}^m I_{r_\ell}$ και r_ℓ κύκλοι κ_{r_ℓ} ξένοι ανά δύο ώστε ο περιορισμός της σ στο I_{r_ℓ} να είναι ο κ_{r_ℓ}. Το «γινόμενο» των ξένων κύκλων κ_{r_ℓ} ισούται με την σ. Έχουμε λοιπόν ότι $\sigma = \Pi_{\ell=1}^m \kappa_{r_\ell}$.

Έστω ότι υπάρχει και δεύτερη ανάλυση της σ σε «γινόμενο» ξένων η_ω κύκλων c_{η_ω}, η $\sigma = \Pi_{\omega=1}^\theta c_{\eta_\omega}$. Επιλέγουμε ένα τυχαίο στοιχείο i_γ του κύκλου κ_{r_1}. Το i_γ ως στοιχείο του Σ_n το βρίσκουμε και σε κάποιο από τους κύκλους c_{η_ω} αφού, τα στοιχεία του Σ_n κατανέμονται στους κύκλους στους οποίους αναλύεται η σ. Αν ο κύκλος c_{η_ω} που περιέχει το i_γ είναι ίδιος με τον κ_{r_1} συνεχίζουμε επιλέγοντας άλλο στοιχείο του κ_{r_1}. Αν σε κάθε επιλογή στοιχείου από τον κ_{r_1} ο κύκλος c_{η_ω}, από την δεύτερη ανάλυση της σ, που το περιέχει είναι ίδιος με τον κ_{r_1} συνεχίζουμε με τον επόμενο κύκλο κ_{r_2}. Επειδή, οι δύο αναλύσεις της σ υποτέθησαν διαφορετικές, δεν μπορεί σε κάθε επιλογή στοιχείου από κάθε κ_{r_ℓ}, ο κύκλος c_{η_ω} από την δεύτερη ανάλυση της σ που το περιέχει να είναι ίδιος με τον κ_{r_ℓ}.

Άρα, θα υπάρχει κάποιο i_δ από κάποιο r_ℓ κύκλο κ_{r_ℓ} της πρώτης ανάλυσης της σ, που να περιέχεται σε κάποιο η_ω κύκλο c_{η_ω}, από την δεύτερη ανάλυση της σ και οι δύο αυτοί κύκλοι να μην είναι ίδιοι. Έστω $\eta_\omega > r_\ell$. Επειδή το i_δ είναι στοιχείο και των δύο κύκλων, τα $\sigma^b(i_\delta)$, $b = 1, 2, \ldots, r_\ell$ είναι στοιχεία και των δύο κύκλων. Ο κύκλος c_{η_ω} έχει επιπλέον τα στοιχεία $\sigma^\pi(i_\delta)$, $\pi = r_\ell + 1, \ldots, \eta_\omega$. Όμως, από την Ευκλείδεια διαίρεση των π, r_ℓ παίρνουμε, $\pi = r_\ell\, q_\ell + a_\ell$, $0 \le a_\ell < r_\ell$. Τότε τα,

$$\sigma^\pi(i_\delta) = (\sigma^{a_\ell}\,(\sigma^{r_\ell})^{q_\ell})(i_\delta) = (\sigma^{a_\ell}\,\underbrace{\sigma^{r_\ell}\,\cdots\,\sigma^{r_\ell}}_{q_\ell\ \text{όροι}})(i_\delta) = \sigma^{a_\ell}(i_\delta),$$

είναι στοιχεία του κύκλου κ_{r_ℓ}. Δηλαδή, ο κύκλος c_{η_ω} αποτελείται από στοιχεία του κ_{r_ℓ} που ορισμένα εμφανίζονται δύο φορές άτοπο, από τον ορισμό ενός κύκλου στην §80. Ομοίως απορρίπτεται η περίπτωση $\eta_\omega < r_\ell$. Τελικά μένει $\eta_\omega = r_\ell$. Αλλά από το γεγονός ότι τα $\sigma^b(i_\delta)$, $b = 1, 2, \ldots, r_\ell$ είναι στοιχεία και των δύο κύκλων προκύπτει ότι οι δύο κύκλοι είναι ίδιοι άτοπο, από την υπόθεσή μας.

Άρα, η σ γράφεται κατά μοναδικό τρόπο ως «γινόμενο» ξένων κύκλων.

§113. Κάθε μετάθεση γράφεται ως «γινόμενο» αντιμεταθέσεων.

Έστω ο κύκλος $(i_1\, i_2\, \ldots\, i_k)$. Είναι άμεσο να επαληθεύσουμε ότι,

$$(i_1\, i_2\, \ldots\, i_k) = (i_1\, i_k)\,(i_1\, i_{k-1})\,\cdots\,(i_1\, i_3)\,(i_1\, i_2).$$

Από την §112, κάθε μετάθεση γράφεται ως «γινόμενο» κύκλων. Από το προηγούμενο αποτέλεσμα, κάθε κύκλος γράφεται ως «γινόμενο» αντιμεταθέσεων. Συνδυάζοντας τα προαναφερθέντα το συμπέρασμα προκύπτει.

§114. Έστω G ομάδα, X ένα σύνολο. Αν υπάρχει πράξη, $(\cdot) : \mathbf{G} \times \mathbf{X} \mapsto \mathbf{X}$ ώστε,

- $\mathbf{1 \cdot x = x}$ για κάθε $\mathbf{x \in X}$,
- $\mathbf{(g_1\, g_2) \cdot x = g_1 \cdot (g_2 \cdot x)}$ για κάθε $\mathbf{g_1, g_2 \in G}$,

λέμε ότι η ομάδα G δρα στο X από αριστερά ή ότι είναι μία από αριστερά δράση στο X.

Αν υπάρχει πράξη, $(\cdot) : \mathbf{X} \times \mathbf{G} \mapsto \mathbf{X}$ **ώστε,**

- $\mathbf{x \cdot 1 = x}$ **για κάθε** $\mathbf{x \in X}$**,**
- $\mathbf{x \cdot (g_1\, g_2) = (x \cdot g_1) \cdot g_2}$ **για κάθε** $\mathbf{g_1, g_2 \in G}$**,**

λέμε ότι η ομάδα G δρα στο X από δεξιά ή ότι είναι μία από δεξιά δράση στο X.

§115. Λέμε ότι η ομάδα G δρα μεταβατικά από αριστερά στο σύνολο X αν για κάθε $\mathbf{x_1, x_2 \in X}$ **υπάρχει** $\mathbf{g \in G}$ **ώστε** $\mathbf{g \cdot x_1 = x_2}$**.**

Λέμε ότι η ομάδα G δρα μεταβατικά από δεξιά στο σύνολο X αν για κάθε $\mathbf{x_1, x_2 \in X}$ **υπάρχει** $\mathbf{g \in G}$ **ώστε** $\mathbf{x_1 \cdot g = x_2}$**.**

§116. Έστω G ομάδα, $\mathbf{a, b \in G}$**. Το** $\mathbf{[a, b]_r = a^{-1}\, b^{-1}\, a\, b}$ **λέγεται από δεξιά μεταθέτης των a, b γιατί,** $\mathbf{b\, a\, [a, b]_r = a\, b}$**.**

Αντιστοίχως, το $\mathbf{[a, b]_l = a\, b\, a^{-1}\, b^{-1}}$ **λέγεται από αριστερά μεταθέτης των a, b γιατί,** $\mathbf{[a, b]_l\, b\, a = a\, b}$**.**

§117. Έστω G ομάδα πεπερασμένης τάξης, H κανονική υποομάδα της G με δείκτη $\mathbf{[G : H] = p}$ **πρώτο αριθμό. Για κάθε** $\mathbf{a, b \in G}$**, οι από δεξιά και αριστερά μεταθέτες** $\mathbf{[a, b]_r}$**,** $\mathbf{[a, b]_l}$ **αντιστοίχως ανήκουν στην H.**

Έστω $a, b \in G$. Αν το $a \in H$, τότε $b^{-1}\, a\, b \in H$ από την κανονικότητα της H. Ο $[a, b]_r = a^{-1}\, (b^{-1}\, a\, b) \in H$ ως «γινόμενο» στοιχείων της H.

Αν $a \notin H$, θεωρούμε το σύνολο $\mathcal{H} = \{a^k\, h \,:\, h \in H,\, k \in \mathbb{Z}\}$. Το $\mathcal{H}$ είναι υποσύνολο της G. Επί πλέον, για τα $a^{k_1}\, h_1$, $a^{k_2}\, h_2$ ισχύουν,

- $a^{-k_2}\, h_1\, a^{k_2} \in H$ από την κανονικότητα της H. Οπότε, $a^{-k_2}\, h_1\, a^{k_2} = h_3 \in H$ ή $h_1\, a^{k_2} = a^{k_2}\, h_3$.
- $(a^{k_1}\, h_1)\, (a^{k_2}\, h_2) = a^{k_1}\, ((h_1\, a^{k_2})\, h_2) = a^{k_1}\, ((a^{k_2}\, h_3)\, h_2) = (a^{k_1}\, a^{k_2})\, (h_3\, h_2)$ είναι στοιχείο του $\mathcal{H}$.
- $a^0\, 1 = 1$ είναι στοιχείο του $\mathcal{H}$.
- $a^{k_1}\, h_1^{-1}\, a^{-k_1} \in H$ από την κανονικότητα της H. Οπότε, $a^{k_1}\, h_1^{-1}\, a^{-k_1} = h_4 \in H$ ή $h_1^{-1}\, a^{-k_1} = a^{-k_1}\, h_4$ είναι στοιχείο του $\mathcal{H}$.
- $(a^{k_1}\, h_1)\, (h_1^{-1}\, a^{-k_1}) = 1 = (h_1^{-1}\, a^{-k_1})\, (a^{k_1}\, h_1)$.
- Ισχύει η προσετεριστικότητα για τα στοιχεία του $\mathcal{H}$ γιατί είναι και στοιχεία της ομάδας G.

Αποδείξαμε ότι το $\mathcal{H}$ είναι υποομάδα της G. Για $k = 0$ κάθε στοιχείο της H είναι και στοιχείο της $\mathcal{H}$ δηλαδή, η H είναι υποομάδα της $\mathcal{H}$. Άρα, $|G| = p\, |H|$, $|\mathcal{H}| = \beta\, |H|$, $|G| = d\, |\mathcal{H}|$ ή $p\, |H| = \beta\, d\, |H|$ ή $\beta\, d = p$. Αυτό σημαίνει ότι είτε $\beta = 1$, είτε $\beta = p$. Αν $\beta = 1$, τότε $|\mathcal{H}| = |H|$. Όμως, για $k = 1$ το ουδέτερο του $\mathbb{Z}$ και $h = 1$ το ουδέτερο της H το $a \in \mathcal{H}$ ενώ έχουμε υποθέσει ότι $a \notin H$. Άρα, το H είναι γνήσια υποομάδα του $\mathcal{H}$ και δεν έχει το ίδιο πλήθος στοιχείων με την $\mathcal{H}$.

Τελικά, $\beta = p$ και $|\mathcal{H}| = \beta\, |H| = p\, |H| = |G|$. Η $\mathcal{H}$ σαν υποομάδα της G είτε είναι γνήσια δηλαδή, περιέχει λιγότερα στοιχεία από αυτά της G, είτε ισούται με την G. Το συμπέρασμα $|\mathcal{H}| = |G|$ επάγει ότι $\mathcal{H} = G$. Εφ' όσον από την αρχική

μας υπόθεση $b \in G$, υπάρχουν $k \in \mathbb{Z}$ και $h \in H$ ώστε $b = a^k\, h$. Άρα, $[a,b]_r = a^{-1}\, b^{-1}\, a\, b \;=\; a^{-1}\, (a^k\, h)^{-1}\, a\, (a^k\, h) \;=\; a^{-1}\, h^{-1}\, a^{-k}\, a^{k+1}\, h \;=\; a^{-1}\, h^{-1}\, a\, h$. Το $a^{-1}\, h^{-1}\, a \in H$ από την κανονικότητα της H. Ο $[a,b]_r \in H$ ως «γινόμενο» στοιχείων της H και το συμπέρασμα προκύπτει για τους από δεξιά μεταθέτες.

Έστω $a, b \in G$. Ο από αριστερά μεταθέτης $[a,b]_l = [a^{-1}, b^{-1}]_r \in H$ γιατί και τα $a^{-1}, b^{-1} \in G$ και το συμπέρασμα προκύπτει για τους από αριστερά μεταθέτες.

§118. Η ομάδα $\mathbf{S_n}$ για $\mathbf{n \geq 5}$ δεν είναι επιλύσιμη.

Έστω ότι η S_n είναι επιλύσιμη. Τότε υπάρχει σειρά $\{Id\} = G_m \subset \cdots G_1 \subset G_0 = S_n$ υποομάδων της S_n ώστε, G_{i+1} είναι κανονική υποομάδα της G_i και ο $[G_i : G_{i+1}]$ είναι πρώτος αριθμός, $i = 0, 1, \ldots, m-1$. Η $G_0 = S_n$ περιέχει όλους τους 3 κύκλους αφού, κάθε 3 κύκλος $(i_1\, i_2\, i_3)$ είναι η μετάθεση n στοιχείων,

$$\begin{pmatrix} i_1 & i_2 & i_3 & i_4 & \cdots & i_n \\ i_2 & i_3 & i_1 & i_4 & \cdots & i_n \end{pmatrix},$$

με $\{i_1, i_2, i_3, i_4, \ldots, i_n\} = \{1, 2, \ldots, n\}$. Υποθέτουμε ότι η ομάδα G_i περιέχει όλους τους 3 κύκλους. Έστω $(i_1\, i_2\, i_3)$ ένας τυχαίος 3 κύκλος. Ορίζουμε, $a = (i_4\, i_2\, i_1)$, $b = (i_1\, i_5\, i_3)$ που είναι εφικτό γιατί $n \geq 5$. Τα $a, b \in G_i$ από την υπόθεση και ο μεταθέτης $[a,b]_r \in G_{i+1}$ από την §117 επειδή η G_{i+1} είναι κανονική υποομάδα της G_i. Όμως,

$$[a,b]_r = a^{-1}\, b^{-1}\, a\, b = (i_1\, i_2\, i_4)\, (i_3\, i_5\, i_1)\, (i_4\, i_2\, i_1)\, (i_1\, i_5\, i_3) = (i_1\, i_2\, i_3),$$

είναι στοιχείο της G_{i+1}. Συμπεραίνουμε ότι και η G_{i+1} περιέχει όλους τους 3 κύκλους. Αποδείξαμε λοιπόν, με επαγωγή στο m ότι κάθε όρος της σειράς $\{Id\} = G_m \subset \cdots G_1 \subset G_0 = S_n$ περιέχει όλους τους 3 κύκλους, άτοπο γιατί η $G_m = \{id\}$ περιέχει μόνο τους 1 κύκλους.

Επιλυσιμότητα δια Ριζικών–Αναγκαία και Ικανή Συνθήκη

Εισαγωγή στην Θεωρία Galois–Συνέχεια

§119. Μετά την παράθεση αναγκαίων για την συνέχεια εννοιών από την Θεωρεία Ομάδων, προχωρούμε στην λεπτομερή εισαγωγή και επεξεργασία των αλγεβρικών εργαλείων που το παράδειγμα της §89 μας προδιέθεσε ότι είναι απαραίτητα για την απόδειξη της ικανής και αναγκαίας συνθήκης ώστε μία πολυωνυμική εξίσωση να είναι επιλύσιμη δια ριζικών.

Έστω $\mathbf{E}, \mathbf{F}$ σώματα, $\mathbf{E/F}$ επέκταση του $\mathbf{F}$. Το σύνολο $\mathcal{G}(\mathbf{E/F})$ των συναρτήσεων $\tau : \mathbf{E} \mapsto \mathbf{E}$ ώστε,

i. **η τ να είναι ένα προς ένα και επί,**

ii. **για κάθε $\mathbf{a}, \mathbf{b} \in \mathbf{E}$ να ισχύει $\tau(\mathbf{a} + \mathbf{b}) = \tau(\mathbf{a}) + \tau(\mathbf{b})$ και $\tau(\mathbf{a}\, \mathbf{b}) = \tau(\mathbf{a})\, \tau(\mathbf{b})$,**

iii. **για κάθε $\mathbf{a} \in \mathbf{F}$ να ισχύει $\tau(\mathbf{a}) = \mathbf{a}$,**

εφοδιασμένο με την πράξη της σύνθεσης συναρτήσεων που για λόγους απλότητας, και κατ΄ αναλογία των αναφερθέντων στις §90, §111 θα συμβολίζουμε με κενό και θα την λέμε «γινόμενο», είναι ομάδα και καλείται ομάδα Galois της επέκτασης $\mathbf{E/F}$.

Τα στοιχεία της $\mathcal{G}(\mathbf{E/F})$ λέγονται αυτομορφισμοί του E που είναι ταυτοτικοί στο F.

Έστω $\tau, \psi \in \mathcal{G}(E/F)$. Επειδή οι τ, ψ είναι ένα προς ένα και επί, και το «γινόμενό» τους είναι συνάρτηση ένα προς ένα και επί. Επιπλέον, για κάθε $a \in F$, $(\tau\,\psi)(a) = \tau(\psi(a)) = \tau(a) = a$. Επίσης, για κάθε $a, b \in E$ παίρνουμε $(\tau\,\psi)(a+b) = \tau(\psi(a+b)) = \tau(\psi(a)+\psi(b)) = \tau(\psi(a)) + \tau(\psi(b)) = (\tau\,\psi)(a) + (\tau\,\psi)(b)$, $(\tau\,\psi)(a\,b) = \tau(\psi(a\,b)) = \tau(\psi(a)\,\psi(b)) = \tau(\psi(a))\,\tau(\psi(b)) = (\tau\,\psi)(a)\,(\tau\,\psi)(b)$.

Η ταυτοτική συνάρτηση id είναι το ουδέτερο στοιχείο του «γινομένου» των στοιχείων του $\mathcal{G}(E/F)$.

Κάθε στοιχείο του $\mathcal{G}(E/F)$ ως ένα προς ένα και επί συνάρτηση, διαθέτει αντίστροφο στοιχείο την αντίστροφή του συνάρτηση, η οποία είναι επίσης ένα προς ένα και επί και επιπλέον, για κάθε $a \in F$, $\tau(a) = a$ έπεται $\tau^{-1}(a) = a$. Επίσης, για κάθε $a, b \in E$ υπάρχουν $g, d \in E$ ώστε $\tau(g) = a$ και $\tau(d) = b$. Τότε, $\tau^{-1}(a+b) = \tau^{-1}(\tau(g)+\tau(d)) = \tau^{-1}(\tau(g+d)) = g+d = \tau^{-1}(a) + \tau^{-1}(b)$ και $\tau^{-1}(a\,b) = \tau^{-1}(\tau(g)\,\tau(d)) = \tau^{-1}(\tau(g\,d)) = g\,d = \tau^{-1}(a)\,\tau^{-1}(b)$.

Άρα η τ^{-1} είναι στοιχείο του $\mathcal{G}(E/F)$.

Έστω $\tau, \psi, \omega \in \mathcal{G}(E/F)$. Είναι άμεσο από τις ιδιότητες του «γινομένου», (σύνθεσης), συναρτήσεων ότι $\tau\,(\psi\,\omega) = (\tau\,\psi)\,\omega$.

Αποδείξαμε ότι το σύνολο $\mathcal{G}(E/F)$ εφοδιασμένο με την πράξη «γινόμενο» συναρτήσεων είναι ομάδα.

§120. Εδώ, τονίζουμε κάτι που σιωπηρά έχουμε υποθέσει και στα προηγούμενα δηλαδή ότι, όταν λέμε ότι τα $\mathbf{k_1, k_2, \ldots, k_n}$ είναι οι ρίζες ενός πολυωνύμου θα θεωρούμε τα $\mathbf{k_i}$ διακεκριμένα χωρίς δηλαδή, να λαμβάνεται υπόψιν η πολλαπλότητα εκάστου των $\mathbf{k_i}$ εκτός αν άλλως αναφέρεται.

Π.χ. στα προηγούμενα, όταν αναφερόμασταν στο σώμα διαχωρισμού $\mathbf{F(k_1, k_2, \ldots, k_n)}$ ενός πολυωνύμου με ρίζες $\mathbf{k_1, k_2, \ldots, k_n}$, ήταν προφανές από την αλγεβρική δομή του $\mathbf{F(k_1, k_2, \ldots, k_n)}$ ότι, $\mathbf{F(k_1, k_2, \ldots, k_n) = F(k_1, k_1, \ldots, k_1, k_2, \ldots, k_n)}$ οπότε, η πολλαπλότητα της κάθε ρίζας $\mathbf{k_i}$ δεν λαμβάνετω υπόψιν εκτός αν άλλως αναφερόταν.

§121. Έστω F σώμα, $\mathbf{f(x) \in F[x]}$, $\mathbf{k_1, k_2, \ldots, k_n}$ οι ρίζες του $\mathbf{f(x)}$, $\mathbf{K \supseteq F}$ σώμα που περιέχει τις ρίζες του $\mathbf{f(x)}$, $\mathbf{E = F(k_1, k_2, \ldots, k_n)}$ το σώμα διαχωρισμού του $\mathbf{f(x)}$ στην επέκταση $\mathbf{K/F}$. Η $\mathcal{G}(\mathbf{E/F})$ λέγεται ομάδα Galois του $\mathbf{f(x)}$ στην επέκταση $\mathbf{E/F}$.

§122. Έστω $\mathbf{F, K, L}$ σώματα, $\mathbf{K/F}$, $\mathbf{L/F}$ επεκτάσεις του F με $\mathbf{K \not\subseteq L}$ και $\mathbf{L \not\subseteq K}$, $\mathbf{f(x) \in F[x]}$, $\mathbf{k_1, k_2, \ldots, k_n \in K}$, $\mathbf{s_1, s_2, \ldots, s_n \in L}$, οι ρίζες του $\mathbf{f(x)}$ με την μορφή που αυτές λαμβάνουν εντός των επεκτάσεων $\mathbf{K/F}$, $\mathbf{L/F}$ αντιστοίχως, $\mathbf{E_K = F(k_1, k_2, \ldots, k_n)}$, $\mathbf{E_L = F(s_1, s_2, \ldots, s_n)}$ τα σώματα διαχωρισμού του $\mathbf{f(x)}$ στις επεκτάσεις $\mathbf{K/F}$, $\mathbf{L/F}$ αντιστοίχως. Οι $\mathcal{G}(\mathbf{E_K/F})$, $\mathcal{G}(\mathbf{E_L/F})$ είναι ισομορφικές δηλαδή, υπάρχει $\mathbf{g : \mathcal{G}(E_K/F) \mapsto \mathcal{G}(E_L/F)}$ ώστε,

- **η g να είναι ένα προς ένα και επί,**
- **για κάθε $\tau_1, \tau_2 \in \mathcal{G}(\mathbf{E_K/F})$, $\mathbf{g(\tau_1\,\tau_2) = g(\tau_1)\,g(\tau_2)}$.**

Λόγο αυτής της ιδιότητας, οι διάφορες $\mathcal{G}(\mathbf{E_K/F})$ του $\mathbf{f(x)}$ στις διάφορες επεκτάσεις $\mathbf{E_K/F}$, είναι αλγεβρικώς η ίδια ομάδα γιατί, όπως έχουμε αναφέρει και προγενέστερα, ένας ισομορφισμός μεταφέρει αυτούσιες τις αλγεβρικές ιδιότητες και δομή από το ένα σύνολο στο άλλο. Γι΄ αυτό, στον ορισμό της §121 μπορούμε να αντικαταστήσουμε την φράση «η $\mathcal{G}(\mathbf{E/F})$ λέγεται ομάδα Galois του $\mathbf{f(x)}$ στην επέκταση $\mathbf{E/F}$» με την φράση «η $\mathcal{G}(\mathbf{E/F})$ λέγεται ομάδα Galois του $\mathbf{f(x)}$ στο $\mathbf{F}$».

Από την §62 υπάρχει ισομορφισμός $h : E_K \mapsto E_L$ με $h(a) = a$ για κάθε $a \in F$. Έστω $\tau \in \mathcal{G}(E_K/F)$, $\psi \in \mathcal{G}(E_L/F)$. Τότε, το πιο κάτω διάγραμμα είναι μεταθετικό, (δηλαδή, $h\,\tau = \psi\,h$),

$$\begin{array}{ccc} E_K & \stackrel{\tau}{\longrightarrow} & E_K \\ h\downarrow\uparrow h^{-1} & & h\downarrow\uparrow h^{-1} \\ E_L & \stackrel{\psi}{\longrightarrow} & E_L \end{array}$$

Θεωρούμε την συνάρτηση $g : \mathcal{G}(E_K/F) \mapsto \mathcal{G}(E_L/F)$ με $g(\tau) = h\,\tau\,h^{-1}$. Θα δείξουμε ότι η g είναι ο ζητούμενος ισομορφισμός.

Πρώτον δείχνουμε ότι η g είναι επί. Έστω $\psi \in \mathcal{G}(E_L/F)$. Η συνάρτηση $h^{-1}\,\psi\,h$ είναι ισομορφισμός από το E_K στο E_K ως «γινόμενο», (σύνθεση), ισομορφισμών, και $(h^{-1}\,\psi\,h)(a) = h^{-1}(\psi(h(a))) = h^{-1}(\psi(a)) = h^{-1}(a) = a$, για κάθε $a \in F$. Οπότε, η συνάρτηση $\tau = h^{-1}\,\psi\,h$ είναι αυτομορφισμός του E_K που είναι ταυτοτικός στο F. Η $\tau \in \mathcal{G}(E_K/F)$ και $g(\tau) = h\,(h^{-1}\,\psi\,h)\,h^{-1} = \psi$.

Δεύτερον δείχνουμε ότι η g είναι ένα προς ένα. Έστω $\tau_1, \tau_2 \in \mathcal{G}(E_K/F)$ με $g(\tau_1) = g(\tau_2)$. Τότε, $h\,\tau_1\,h^{-1} = h\,\tau_2\,h^{-1}$ ή $h^{-1}\,h\,\tau_1\,h^{-1}\,h = h^{-1}\,h\,\tau_2\,h^{-1}\,h$ ή $\tau_1 = \tau_2$.

Τρίτον δείχνουμε ότι για κάθε $\tau_1, \tau_2 \in \mathcal{G}(E_K/F)$, $g(\tau_1\,\tau_2) = g(\tau_1)\,g(\tau_2)$. Έχουμε, $g(\tau_1\,\tau_2) = h\,\tau_1\,\tau_2\,h^{-1} = h\,\tau_1\,h^{-1}\,h\,\tau_2\,h^{-1} = g(\tau_1)\,g(\tau_2)$.

Το συμπέρασμα απεδείχθη.

§123. Έστω $\mathbf{E, F}$ σώματα με $\mathbf{E/F}$ επέκταση του $\mathbf{F}$, $\tau \in \mathcal{G}(\mathbf{E/F})$. Ισχύει ότι,

- $\tau(\mathbf{0}) = \mathbf{0}$, **(0 το προσθετικό ουδέτερο του E),**
- $\tau(\mathbf{1}) = \mathbf{1}$, **(1 το πολλαπλασιαστικό ουδέτερο του E),**
- $\tau(-\mathbf{a}) = -\tau(\mathbf{a})$, **για κάθε** $\mathbf{a} \in \mathbf{E} - \{\mathbf{0}\}$,
- $\tau(\mathbf{a^{-1}}) = (\tau(\mathbf{a}))^{-\mathbf{1}}$, **για κάθε** $\mathbf{a} \in \mathbf{E} - \{\mathbf{0}\}$.

$\tau(0) = \tau(0+0) = \tau(0) + \tau(0)$ επάγει $\tau(0) = 0$.
$\tau(1) = \tau(1\,1) = \tau(1)\,\tau(1)$ επάγει $\tau(1) = 1$.
Για κάθε $a \in E - \{0\}$, $0 = \tau(0) = \tau(a + (-a)) = \tau(a) + \tau(-a)$ επάγει $\tau(-a) = -\tau(a)$.
Για κάθε $a \in E - \{0\}$, $1 = \tau(1) = \tau(a\,a^{-1}) = \tau(a)\,\tau(a^{-1})$ επάγει $\tau(a^{-1}) = (\tau(a))^{-1}$.

§124. Έστω $\mathbf{F}$ σώμα, $\mathbf{f(x)} \in \mathbf{F[x]}$, $\mathbf{k_1, k_2, \ldots, k_n}$ οι ρίζες του $\mathbf{f(x)}$, $\mathbf{K} \supseteq \mathbf{F}$ σώμα που περιέχει τις ρίζες του $\mathbf{f(x)}$, $\mathbf{E} = \mathbf{F(k_1, k_2, \ldots, k_n)}$

το σώμα διαχωρισμού του $\mathbf{f(x)}$ στην επέκταση $\mathbf{K/F}$. Η $\mathcal{G}(\mathbf{E/F})$ είναι υποομάδα της $\mathbf{S_n}$.

Έστω $\tau \in \mathcal{G}(E/F)$, $f(x) = \sum_{j=0}^{m} a_j\, x^j \in F[x]$. Από την §123,

$$0 = \tau(0) = \tau(f(k_i)) = \tau\left(\sum_{j=0}^{m} a_j\, k_i^j\right) = \sum_{j=0}^{m} \tau(a_j)\, \tau(k_i)^j = \sum_{j=0}^{m} a_j\, \tau(k_i)^j.$$

Για κάθε $\tau \in \mathcal{G}(E/F)$, το $\tau(k_i) \in \mathcal{K} = \{k_1, k_2, \ldots, k_n\}$ δηλαδή, $\tau(\mathcal{K}) \subseteq \mathcal{K}$.

Έστω $k_i \in \mathcal{K}$. Επειδή η τ είναι επί του E, υπάρχει $b \in E$ ώστε $\tau(b) = k_i$ ή, $b = \tau^{-1}(k_i)$. Τότε,

$$\begin{aligned}\sum_{j=0}^{m} a_j\, b^j &= \sum_{j=0}^{m} a_j\, (\tau^{-1}(k_i))^j = \sum_{j=0}^{m} \tau^{-1}(a_j)\, \tau^{-1}(k_i^j) = \tau^{-1}\left(\sum_{j=0}^{m} a_j\, k_i^j\right) = \\ &= \tau^{-1}(0) = 0.\end{aligned}$$

Το b είναι στοιχείο του $\mathcal{K}$. Κάθε ρίζα του $f(x)$ είναι εικόνα μέσω του τ μιας ρίζας του $f(x)$. Άρα, $\tau(\mathcal{K}) = \mathcal{K}$. Δείξαμε ότι κάθε $\tau \in \mathcal{G}(E/F)$ είναι επί του $\mathcal{K}$.

Κάθε στοιχείο της $\mathcal{G}(E/F)$ είναι μία ένα προς ένα συνάρτηση από το E στο E άρα και μία ένα προς ένα συνάρτηση από το υποσύνολο $\mathcal{K}$, του E, στο $\mathcal{K}$. Κάθε στοιχείο της $\mathcal{G}(E/F)$ είναι μία ένα προς ένα και επί συνάρτηση από το $\mathcal{K}$ στο $\mathcal{K}$ δηλαδή, μία μετάθεση των n στοιχείων $\{k_1, k_2, \ldots, k_n\}$ ή ισοδυνάμως όπως έχουμε τονίσει στην §80 μία μετάθεση των στοιχείων του $\Sigma_n = \{1, 2, \ldots, n\}$. Άρα, η ομάδα $\mathcal{G}(E/F)$ είναι υποομάδα της S_n που επίσης μας λέει ότι,

Η ομάδα Galois ενός πολυωνύμου σε ένα σώμα $\mathbf{F}$ έχει πεπερασμένη τάξη.

Όπως είδαμε στο παράδειγμα §89, κάθε στοιχείο της S_n δεν είναι υποχρεωτικά στοιχείο μίας ομάδας Galois ενός πολυωνύμου. Στην πορεία θα δούμε ότι, υπάρχουν πολυώνυμα των οποίων η ομάδα Galois είναι η S_n για κάποιο n.

§125. Έστω $\mathbf{E, F}$ σώματα, $\mathbf{k \in E}$ αλγεβρικό επί του $\mathbf{F}$, $\mathbf{p(x) \in F[x]}$ ένα ελάχιστο πολυώνυμο του $\mathbf{k}$ και $\mathbf{k_1 = k, k_2, \ldots, k_n}$ οι ρίζες του $\mathbf{p(x)}$. Τότε, το $\mathbf{p(x)}$ είναι ένα ελάχιστο πολυώνυμο και για τα $\mathbf{k_2, \ldots, k_n}$.

Από την §65 το $p(x)$ είναι ανάγωγο στο $F[x]$. Έστω $k_i \in \{k_2, \ldots, k_n\}$. Αν υπάρχει ελάχιστο πολυώνυμο $g(x) \in F[x]$ του k_i με $deg[g(x)] < deg[p(x)]$, τότε από την Ευκλείδεια διαίρεση των $p(x)$, $g(x)$ έπεται, $p(x) = g(x)\, q(x) + u(x)$ με $q(x), u(x) \in F[x]$ και είτε $u(x) = 0$ είτε $0 \leq deg[u(x)] < deg[g(x)]$.

Αν $0 \leq deg[u(x)] < deg[g(x)]$, τότε $0 = p(k_i) = g(k_i)\, q(k_i) + u(k_i) = u(k_i)$, άτοπο από την υπόθεση ότι το $g(x)$ είναι ελάχιστο πολυώνυμο για το k_i. Άρα, $u(x) = 0$ και $p(x) = g(x)\, q(x)$. Επειδή το $p(x)$ είναι ανάγωγο στο $F[x]$ το τελευταίο ισχύει μόνο αν $q(x) = q \in F - \{0\}$ που σημαίνει ότι $deg[g(x)] = deg[p(x)]$, άτοπο. Οπότε, δεν υπάρχει ελάχιστο πολυώνυμο του k_i στο $F[x]$ βαθμού μικρότερου του $p(x)$ και το συμπέρασμα προκύπτει.

§126. Έστω $\mathbf{E, F}$ σώματα, $\mathbf{k \in E}$ αλγεβρικό επί του $\mathbf{F}$ ώστε $\mathbf{E = F(k)}$, $\mathcal{K} = \{\mathbf{k_1 = k, k_2, \ldots, k_n}\}$ το σύνολο των ριζών ενός ελαχίστου

πολυωνύμου $\mathbf{q(x)}$ του $\mathbf{k}$ στο $\mathbf{F[x]}$, $\mathbf{k_{i_1}, k_{i_2}, \ldots, k_{i_m}}$ τα στοιχεία του $\mathcal{K}$ που ανήκουν στο $\mathbf{E}$. Τότε, $|\mathcal{G}(\mathbf{E/F})| = \mathbf{m}$.

Έστω $\tau \in \mathcal{G}(E/F)$. Από την §124 είδαμε ότι η εικόνα μέσω του τ μίας ρίζας ενός πολυωνύμου του $F[x]$ είναι εκ΄ νέου ρίζα του πολυωνύμου αυτού. Άρα, επειδή το k είναι ρίζα του $q(x) \in F[x]$, το $\tau(k)$ είναι επίσης ρίζα του πολυωνύμου αυτού. Επιπλέον, το $\tau(k) \in E$ δηλαδή, $\tau(k) \in \{k_{i_1}, k_{i_2}, \ldots, k_{i_m}\}$.

Έστω $\psi \in \mathcal{G}(E/F)$ με $\tau \neq \psi$ και $\tau(k) = \psi(k)$. Από την §66 για κάθε $b \in E$, $b = \sum_{j=0}^{n-1} a_j\, k^j$ όπου $n = deg[q(x)]$, $a_j \in F$. Τότε,

$$\begin{aligned} \tau(b) &= \tau\left(\sum_{j=0}^{n-1} a_j\, k^j\right) = \sum_{j=0}^{n-1} \tau(a_j)\, \tau(k)^j = \sum_{j=0}^{n-1} a_j\, \psi(k)^j = \\ &= \sum_{j=0}^{n-1} \psi(a_j)\, \psi(k)^j = \psi\left(\sum_{j=0}^{n-1} a_j\, k^j\right) = \psi(b), \end{aligned}$$

που συνεπάγεται $\tau = \psi$, άτοπο. Άρα, κάθε στοιχείο του $\{k_{i_1}, k_{i_2}, \ldots, k_{i_m}\}$ έχει διαφορετική εικόνα μέσω διαφορετικών στοιχείων της $\mathcal{G}(E/F)$.

Έστω $k_\mu \in \{k_{i_1}, k_{i_2}, \ldots, k_{i_m}\}$. Θεωρούμε την συνάρτηση $\omega : E \mapsto E$ με $\omega(b) = \omega\left(\sum_{j=0}^{n-1} a_j\, k^j\right) = \sum_{j=0}^{n-1} a_j\, k_\mu^j$. Θα δείξουμε ότι η ω είναι στοιχείο της $\mathcal{G}(E/F)$. Έστω $\omega(b_1) = \omega(b_2)$ με $b_1 = \sum_{j=0}^{n-1} a_j\, k^j$ και $b_2 = \sum_{j=0}^{n-1} g_j\, k^j$. Τότε,

$$\sum_{j=0}^{n-1} a_j\, k_\mu^j = \sum_{j=0}^{n-1} g_j\, k_\mu^j \Rightarrow \sum_{j=0}^{n-1} (a_j - g_j)\, k_\mu^j = 0,$$

επάγοντας είτε ότι υπάρχει πολυώνυμο $h(x)$ του $F[x]$ με βαθμό μικρότερο του n που να έχει την k_μ ως ρίζα, άτοπο από την §125, είτε ότι $a_j = g_j$ οπότε, $b_1 = b_2$ και η ω είναι ένα προς ένα.

Επειδή, $k_\mu \in F(k)$ έπεται $F \subseteq F(k_\mu) \subseteq F(k)$. Από την υπόθεση και την §125, ένα ελάχιστο πολυώνυμο της k_μ στο $F[x]$ είναι το $q(x)$. Από την §66, $(F(k) : F) = (F(k_\mu) : F) = n$. Από την §49,

$$n = (F(k) : F) = (F(k) : F(k_\mu))\, (F(k_\mu) : F) = (F(k) : F(k_\mu))\, n$$

οπότε, $(F(k) : F(k_\mu)) = 1$ και τελικά $F(k) = F(k_\mu)$. Έστω $z = \sum_{j=0}^{n-1} a_j\, k^j \in E = F(k) = F(k_\mu)$. Τότε, το z ως στοιχείο και του $F(k_\mu)$ γράφεται $z = \sum_{j=0}^{n-1} b_j\, k_\mu^j$. Θεωρούμε το στοιχείο $g = \sum_{j=0}^{n-1} b_j\, k^j \in F(k) = E$. Έπεται $\omega(g) = z$ και η ω είναι επί.

Έστω $b_1 = \sum_{j=0}^{n-1} a_j\, k^j$ και $b_2 = \sum_{j=0}^{n-1} g_j\, k^j$ στοιχεία του E.

$$\begin{aligned} \omega(b_1 + b_2) &= \omega\left(\sum_{j=0}^{n-1} (a_j + g_j)\, k^j\right) = \sum_{j=0}^{n-1} (a_j + g_j)\, k_\mu^j = \\ &= \sum_{j=0}^{n-1} a_j\, k_\mu^j + \sum_{j=0}^{n-1} g_j\, k_\mu^j = \omega(b_1) + \omega(b_2), \\ \omega(b_1\, b_2) &= \omega\left(\sum_{i=0}^{2n-2} \left(\sum_{j=0}^{i} a_{i-j}\, g_j\right) k^i\right) = \sum_{i=0}^{2n-2} \left(\sum_{j=0}^{i} a_{i-j}\, g_j\right) k_\mu^i = \end{aligned}$$

$$= \left(\sum_{j=0}^{n-1} a_j\, k_\mu^j\right)\left(\sum_{j=0}^{n-1} g_j\, k_\mu^j\right) = \omega(b_1)\,\omega(b_2).$$

Για κάθε $b \in F$, $b = b\,1 + 0\,k + \cdots + 0\,k^{n-1}$ οπότε, $\omega(b) = b\,1 + 0\,k_\mu + \cdots + 0\,k_\mu^{n-1} = b$. Αποδείξαμε ότι η ω είναι ένας αυτομορφισμός του E που είναι ταυτοτικός στο F δηλαδή, $\omega \in \mathcal{G}(E/F)$.

Άρα, σε κάθε στοιχείο k_μ του $\{k_{i_1}, k_{i_2}, \ldots, k_{i_m}\}$ αντιστοιχεί ένα στοιχείο ω της $\mathcal{G}(E/F)$ με κανόνα $\omega(b) = \omega\left(\sum_{j=0}^{n-1} a_j\, k^j\right) = \sum_{j=0}^{n-1} a_j\, k_\mu^j$ για κάθε $b = \sum_{j=0}^{n-1} a_j\, k^j \in E$. Αν αντιστοιχεί και δεύτερο στοιχείο τ της $\mathcal{G}(E/F)$ τότε, λόγο του κανόνα ορισμού του, $\tau(b) = \tau\left(\sum_{j=0}^{n-1} a_j\, k^j\right) = \sum_{j=0}^{n-1} a_j\, k_\mu^j$ για κάθε $b = \sum_{j=0}^{n-1} a_j\, k^j \in E$ θα έπεται $\omega = \tau$. Οπότε, σε κάθε στοιχείο k_μ του $\{k_{i_1}, k_{i_2}, \ldots, k_{i_m}\}$ αντιστοιχεί ένα μοναδικό στοιχείο ω της $\mathcal{G}(E/F)$.

Στην αρχή της απόδειξης δείξαμε ότι σε κάθε στοιχείο τ της $\mathcal{G}(E/F)$ αντιστοιχεί στοιχείο $\tau(k)$ του $\{k_{i_1}, k_{i_2}, \ldots, k_{i_m}\}$. Και επίσης δείξαμε ότι σε διαφορετικά στοιχεία τ της $\mathcal{G}(E/F)$ αντιστοιχούν διαφορετικά στοιχεία $\tau(k)$ του $\{k_{i_1}, k_{i_2}, \ldots, k_{i_m}\}$. Δηλαδή, σε κάθε στοιχείο τ της $\mathcal{G}(E/F)$ αντιστοιχεί μοναδικό στοιχείο του $\{k_{i_1}, k_{i_2}, \ldots, k_{i_m}\}$.

Έχουμε δείξει ότι, σε κάθε διαφορετικό στοιχείο της $\mathcal{G}(E/F)$ αντιστοιχεί διαφορετικό στοιχείο του $\{k_{i_1}, k_{i_2}, \ldots, k_{i_m}\}$ και αντιστρόφως. Άρα, υπάρχει μία ένα προς ένα και επί αντιστοίχιση των στοιχείων της $\mathcal{G}(E/F)$ με τα στοιχεία του $\{k_{i_1}, k_{i_2}, \ldots, k_{i_m}\}$ που επάγει το ζητούμενο αποτέλεσμα.

§127. Έστω $\mathbf{E}, \mathbf{F}$ σώματα, $\mathbf{E} \supseteq \mathbf{F}$, $\mathbf{E/F}$ πεπερασμένη επέκταση του $\mathbf{F}$. Τότε, $|\mathcal{G}(\mathbf{E/F})| \leq (\mathbf{E} : \mathbf{F})$.

Από την §75, η E/F ως πεπερασμένη επέκταση του F είναι και απλή επέκταση του F δηλαδή, υπάρχει $k \in E$ αλγεβρικό επί του F ώστε $E = F(k)$. Από την §66, προκύπτει ότι η διάσταση $(E : F)$ ισούται με τον βαθμό ενός ελαχίστου πολυωνύμου του k στο $F[x]$ δηλαδή, με το πλήθος των ριζών του πολυωνύμου αυτού, που από τις §65, §71 είναι διακεκριμένες. Όλες οι διαδικασίες είναι ανεξάρτητες από το πιο ελάχιστο πολυώνυμο του k στο $F[x]$ θα επιλέξουμε αφού, αν $g(x)$ είναι ένα ελάχιστο πολυώνυμο του k στο $F[x]$ από την §65, όλα τα ελάχιστα πολυώνυμα του k στο $F[x]$ είναι $a\,g(x)$ με $a \in F - \{0\}$. Δηλαδή, δεν αλλάζουν ούτε ο βαθμός ούτε οι ρίζες τους. Όλα τα ελάχιστα πολυώνυμα του k στο $F[x]$ έχουν τον ίδιο βαθμό και τις ίδιες ρίζες.

Από την §126, η $|\mathcal{G}(E/F)|$ ισούται με το πλήθος εκείνων των ριζών ενός ελαχίστου πολυωνύμου του k στο $F[x]$, που ανήκουν στο E. Το πλήθος αυτό είναι πάντα μικρότερο ή ίσο από το πλήθος όλων των ριζών του ελαχίστου πολυωνύμου του k στο $F[x]$ γιατί, δεν είναι υποχρεωτικό όλες οι ρίζες του να ανήκουν στο E. Το συμπέρασμα προκύπτει.

§128. Έστω $\mathbf{E}, \mathbf{K}, \mathbf{F}$ σώματα με $\mathbf{E} \supseteq \mathbf{F}$. Το $\mathbf{K}$ θα λέγεται ενδιάμεσο σώμα των $\mathbf{E}, \mathbf{F}$ αν ισχύει $\mathbf{E} \supseteq \mathbf{K} \supseteq \mathbf{F}$.

§129. Έστω $\mathbf{E}, \mathbf{F}$ σώματα με $\mathbf{E} \supseteq \mathbf{F}$. Το σύνολο,

$$\mathbf{F}_{\mathcal{G}} = \{\mathbf{a} \in \mathbf{E} \,:\, \tau(\mathbf{a}) = \mathbf{a}\,, \forall\, \tau \in \mathcal{G}(\mathbf{E/F})\},$$

είναι ενδιάμεσο σώμα των $\mathbf{E}, \mathbf{F}$.

Από τον ορισμό της $\mathcal{G}(E/F)$ προκύπτει ότι, $F \subseteq F_{\mathcal{G}}$. Από τον ορισμό του $F_{\mathcal{G}}$ προκύπτει ότι, $F_{\mathcal{G}} \subseteq E$. Αρκεί να αποδείξουμε ότι το $F_{\mathcal{G}}$ είναι σώμα. Από την §2 αρκεί τα στοιχεία του $F_{\mathcal{G}}$ να ικανοποιούν τις ιδιότητες (I1–I9) ως προς την «πρόσθεση» και τον «πολλαπλασιασμό» του E.
(I1). Για κάθε $a, b \in F_{\mathcal{G}}$ και κάθε $\tau \in \mathcal{G}(E/F)$ έχουμε, $\tau(a+b) = \tau(a)+\tau(b) = a + b$, $\tau(b + a) = \tau(b) + \tau(a) = b + a$. Επιπλέον, $a + b = b + a$ γιατί τα a, b ανήκουν και στο E που είναι σώμα. Άρα, $a + b = b + a \in F_{\mathcal{G}}$.
(I2). Από την §123, $\tau(0) = 0$ για κάθε $\tau \in \mathcal{G}(E/F)$ οπότε, $0 \in F_{\mathcal{G}}$ δηλαδή, το ουδέτερο στοιχείο της «πρόσθεσης» του E ανήκει στο $F_{\mathcal{G}}$.
(I3). Για κάθε $a \in F_{\mathcal{G}} - \{0\}$, και κάθε $\tau \in \mathcal{G}(E/F)$ από την §123 έχουμε, $\tau(-a) = -\tau(a) = -a$. Άρα, για κάθε $a \in F_{\mathcal{G}} - \{0\}$ το μοναδικό του αντίθετο ως προς την «πρόσθεση» του E ανήκει στο $F_{\mathcal{G}}$.
(I4). Επειδή τα στοιχεία του $F_{\mathcal{G}}$ είναι και στοιχεία του σώματος E, ισχύει για αυτά η προσετεριστική ιδιότητα ως προς την «πρόσθεση» του E.
(I5). Για κάθε $a, b \in F_{\mathcal{G}}$ και κάθε $\tau \in \mathcal{G}(E/F)$ έχουμε, $\tau(a\,b) = \tau(a)\,\tau(b) = a\,b$, $\tau(b\,a) = \tau(b)\,\tau(a) = b\,a$. Επιπλέον, $a\,b = b\,a$ γιατί τα a, b ανήκουν και στο E που είναι σώμα. Άρα, $a\,b = b\,a \in F_{\mathcal{G}}$.
(I6). Από την §123, $\tau(1) = 1$ για κάθε $\tau \in \mathcal{G}(E/F)$ οπότε, $1 \in F_{\mathcal{G}}$ δηλαδή, το ουδέτερο στοιχείο του «πολλαπλασιασμού» του E ανήκει στο $F_{\mathcal{G}}$.
(I7). Για κάθε $a \in F_{\mathcal{G}} - \{0\}$, και κάθε $\tau \in \mathcal{G}(E/F)$ από την §123 έχουμε, $\tau(a^{-1}) = (\tau(a))^{-1} = a^{-1}$. Άρα, για κάθε $a \in F_{\mathcal{G}} - \{0\}$ το μοναδικό του αντίστροφο ως προς τον «πολλαπλασιασμό» του E ανήκει στο $F_{\mathcal{G}}$.
(I8). Επειδή τα στοιχεία του $F_{\mathcal{G}}$ είναι και στοιχεία του σώματος E, ισχύει για αυτά η προσετεριστική ιδιότητα ως προς τον «πολλαπλασιασμό» του E.
(I9). Επειδή τα στοιχεία του $F_{\mathcal{G}}$ είναι και στοιχεία του σώματος E, ισχύει για αυτά η επιμεριστική του «πολλαπλασιασμού» του E επί της «πρόσθεσης» του E.
Το συμπέρασμα προκύπτει.

§130. Έστω $\mathbf{E, F}$ σώματα με $\mathbf{E \supseteq F}$, $\mathbf{E/F}$ επέκταση του $\mathbf{F}$. Το σύνολο, $\mathbf{F_{\mathcal{G}}}$ λέγεται σταθερό σώμα της $\mathbf{\mathcal{G}(E/F)}$.

§131. Έστω $\mathbf{E, F}$ σώματα με $\mathbf{E \supseteq F}$, $\mathbf{E/F}$ πεπερασμένη επέκταση του $\mathbf{F}$. Η $\mathbf{E/F}$ λέγεται κανονική επέκταση του $\mathbf{F}$ αν, κάθε ανάγωγο πολυώνυμο στο $\mathbf{F[x]}$ που έχει μία ρίζα του στο $\mathbf{E}$ έχει όλες τις ρίζες του στο $\mathbf{E}$.

§132. Έστω $\mathbf{E, F}$ σώματα με $\mathbf{E \supseteq F}$, $\mathbf{E/F}$ κανονική επέκταση του $\mathbf{F}$. Το $\mathbf{E}$ είναι σώμα διαχωρισμού για κάποιο $\mathbf{f(x) \in F[x]}$.

Από την §131, η E/F είναι πεπερασμένη επέκταση του F. Από την §75, η E/F είναι και απλή επέκταση του F δηλαδή, υπάρχει $k \in E$ αλγεβρικό επί του F ώστε $E = F(k)$. Έστω $f(x)$ ένα ελάχιστο πολυώνυμο του k στο $F[x]$ με $deg[f(x)] = n$. Από τις §65, §71, το $f(x)$ είναι ανάγωγο στο $F[x]$ και οι ρίζες του $k = k_1, k_2, \ldots, k_n$ είναι διακεκριμένες. Από την κανονικότητα της επέκτασης E/F προκύπτει ότι οι $k = k_1, k_2, \ldots, k_n$ ανήκουν στο E. Το E περιέχει τα $k = k_1, k_2, \ldots, k_n$ και F άρα $F(k_1, k_2, \ldots, k_n) \subseteq E$. Όμως, $E = F(k) = F(k_1) \subseteq F(k_1, k_2, \ldots, k_n) \subseteq E$ οπότε, $E = F(k_1, k_2, \ldots, k_n)$ που είναι το σώμα διαχωρισμού του $f(x)$ στην επέκταση E/F.

§133. Έστω $\mathbf{F}$ σώμα, $\mathbf{f(x) = \sum_{k=0}^{n} a_k\, x^k \in F[x]}$ με ρίζες $\mathbf{b_1, b_2, \ldots, b_n}$

λαμβάνοντας υπ' όψιν και την πολλαπλότητά τους. Έστω $\mathbf{h(x_1, x_2, \ldots, x_n)}$ συμμετρικό πολυώνυμο του $\mathbf{F[x_1, x_2, \ldots, x_n]}$. Τότε, το $\mathbf{h(b_1, b_2, \ldots, b_n)}$ είναι στοιχείο του F.

Από την §42, μπορούμε να γράψουμε,

$$\begin{aligned}\sum_{k=0}^{n} a_k\, x^k &= a_n\,(x-b_1)\,(x-b_2)\,\cdots\,(x-b_n) = \\ &= a_n\, x^n + \sum_{k=1}^{n} (-1)^k\, a_n\, e_k(b_1, b_2, \ldots, b_n)\, x^{n-k},\end{aligned}$$

με $e_k(b_1, b_2, \ldots, b_n)$ την τιμή του στοιχειώδους συμμετρικού πολυωνύμου $e_k(x_1, x_2, \ldots, x_n)$ στην n–άδα $(b_1, b_2, \ldots, b_n)$. Λαμβάνουμε λοιπόν,

$$\begin{aligned}-\frac{a_{n-1}}{a_n} &= \sum_{i=1}^{n} b_i = e_1(b_1, b_2, \ldots, b_n), \\ \frac{a_{n-2}}{a_n} &= \sum_{1\le i_1<i_2\le n} b_{i_1}\, b_{i_2} = e_2(b_1, b_2, \ldots, b_n), \\ &\vdots \\ (-1)^k\,\frac{a_{n-k}}{a_n} &= \sum_{1\le i_1<i_2<\cdots<i_{k\le n}} b_{i_1}\, b_{i_2}\,\cdots\, b_{i_k} = e_k(b_1, b_2, \ldots, b_n), \\ &\vdots \\ (-1)^n\,\frac{a_0}{a_n} &= b_1\, b_2\,\cdots\, b_n = e_n(b_1, b_2, \ldots, b_n).\end{aligned}$$

Από την §86, το $h(x_1, x_2, \ldots, x_n)$ γράφεται,

$$h(x_1, x_2, \ldots, x_n) = g(e_1(x_1, \ldots, x_n), e_2(x_1, \ldots, x_n), \ldots, e_n(x_1, \ldots, x_n)),$$

με $g(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$. Οπότε το,

$$\begin{aligned}h(b_1, b_2, \ldots, b_n) &= g(e_1(b_1, \ldots, b_n), e_2(b_1, \ldots, b_n), \ldots, e_n(b_1, \ldots, b_n)) = \\ &= g\left(-\frac{a_{n-1}}{a_n}, \frac{a_{n-2}}{a_n}, \ldots, (-1)^n\,\frac{a_0}{a_n}\right),\end{aligned}$$

είναι στοιχείο του F ως αποτέλεσμα πράξεων μεταξύ στοιχείων του F.

§134. Έστω $\mathbf{E, F}$ σώματα με $\mathbf{E \supseteq F}$, $\mathbf{E/F}$ πεπερασμένη επέκταση του F. Αν το E είναι σώμα διαχωρισμού για κάποιο $\mathbf{f(x) \in F[x]}$, η $\mathbf{E/K}$ είναι κανονική επέκταση για κάθε ενδιάμεσο σώμα K των $\mathbf{E, F}$.

Έστω $k_1, k_2, \ldots, k_n$ οι ρίζες του $f(x)$. Από την §60, το E ως σώμα διαχωρισμού του $f(x)$ γράφεται $E = F(k_1, k_2, \ldots, k_n)$. Από την §51,

$$F(k_1, k_2, \ldots, k_n) = (((F(k_1))(k_2))\cdots)(k_n).$$

Θέτουμε $F_0 = F$ και $F_j = (((F(k_1))(k_2))\cdots)(k_j)$, $j = 1, 2, \ldots, n$. Το $f(x) \in F[x] \subseteq F_{j-1}[x]$. Άρα, τα $k_1, k_2, \ldots, k_j$ ως ρίζες του $f(x) \in F[x]$ είναι και ρίζες

του $f(x) \in F_{j-1}[x]$. Άρα, τα $k_1, k_2, \ldots, k_j$ είναι αλγεβρικά και επί των F_{j-1}. Από την §66, η F_j/F_{j-1} είναι πεπερασμένη επέκταση του F_{j-1}, $j = 1, 2, \ldots, n$ με βάση $\mathcal{K}_j = \{1, k_j, k_j^2, \ldots, k_j^{m_j-1}\}$ όπου m_j είναι ο βαθμός ενός ελαχίστου πολυωνύμου του k_j στο $F_{j-1}[x]$. Από τις §48, §49 επαγωγικά προκύπτει ότι, μία βάση επί του F της επέκτασης E/F είναι το σύνολο $\mathfrak{K} = \mathcal{K}_1\,\mathcal{K}_2 \cdots \mathcal{K}_n$ που αποτελείται από γινόμενα n το πλήθος παραγόντων, έκαστος των οποίων προέρχεται από ακριβώς ένα εκ' των $\mathcal{K}_j$. Κάθε στοιχείο του E είναι γραμμικός συνδυασμός επί του F των στοιχείων της βάσης $\mathfrak{K}$ δηλαδή, υπάρχουν πολυώνυμα $p(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$ ώστε τα στοιχεία του E να έχουν τη μορφή $p(k_1, k_2, \ldots, k_n)$.

Έστω K ένα ενδιάμεσο σώμα των E, F. Θεωρούμε το $g(x) \in K[x]$ ανάγωγο στο $K[x]$ ώστε μία ρίζα του, η a, να ανήκει στο E. Θα δείξουμε ότι όλες οι ρίζες του $g(x)$ ανήκουν στο E. Το a ως στοιχείο του E έχει τη μορφή $a = p(k_1, k_2, \ldots, k_n)$ για κάποιο $p(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$. Έστω $\tau_\nu \in S_n$, $\nu = 1, 2, \ldots, n!$ οι μεταθέσεις των n στοιχείων $\{1, 2, \ldots, n\}$, (άρα και των $\{k_1, k_2, \ldots, k_n\}$). Θέτουμε,

$$a_\nu = p(k_{\tau_\nu(1)}, k_{\tau_\nu(2)}, \ldots, k_{\tau_\nu(n)}),$$

τις τιμές του $p(k_1, k_2, \ldots, k_n)$ που προκύπτουν μεταθέτοντας τα $\{k_1, k_2, \ldots, k_n\}$ σύμφωνα με τις μεταθέσεις $\tau_\nu \in S_n$, $\nu = 1, 2, \ldots, n!$, με $\tau_1 = id$. Τα $a_2, \ldots, a_{n!}$ είναι στοιχεία του E γιατί είναι αποτελέσματα πράξεων του σώματος E μεταξύ στοιχείων του E. Θέτουμε και $a_1 = a \in E$.

Θα δείξουμε ότι, το πολυώνυμο $g(x) \in K[x] \subseteq E[x]$ διαιρεί στο $E[x]$, το πολυώνυμο $h(x) = \prod_{\nu=1}^{n!}(x - a_\nu) \in E[x]$ οπότε, οι ρίζες του $g(x)$ είναι μεταξύ των ριζών του $h(x)$ άρα, οι ρίζες του $g(x)$ ανήκουν στο E.

$$h(x) = x^{n!} + \sum_{\nu=1}^{n!} (-1)^\nu\, e_\nu(a_1, a_2, \ldots, a_{n!})\, x^{n!-\nu},$$

με $e_\nu(a_1, a_2, \ldots, a_{n!})$ την τιμή του στοιχειώδους συμμετρικού πολυωνύμου $e_\nu(x_1, x_2, \ldots, x_{n!})$ στην $n!$–άδα $(a_1, a_2, \ldots, a_{n!})$. Όμως,

$$\begin{aligned} e_\nu(a_1, a_2, \ldots, a_{n!}) &= e_\nu(p(k_1, k_2, \ldots, k_n), p(k_{\tau_2(1)}, k_{\tau_2(2)}, \ldots, k_{\tau_2(n)}), \ldots, \\ &\quad p(k_{\tau_{n!}(1)}, k_{\tau_{n!}(2)}, \ldots, k_{\tau_{n!}(n)})), \text{ και θέτουμε,} \\ d_\nu(x_1, x_2, \ldots, x_n) &= e_\nu(p(x_1, x_2, \ldots, x_n), p(x_{\tau_2(1)}, x_{\tau_2(2)}, \ldots, x_{\tau_2(n)}), \ldots, \\ &\quad p(x_{\tau_{n!}(1)}, x_{\tau_{n!}(2)}, \ldots, x_{\tau_{n!}(n)})), \text{ οπότε,} \end{aligned}$$

Κάθε μετάθεση των n στοιχείων $\{1, 2, \ldots, n\}$, (άρα και των $\{x_1, x_2, \ldots, x_n\}$), έχει ως αποτέλεσμα μετάθεση των στοιχείων,

$$\{p(x_1, x_2, \ldots, x_n), p(x_{\tau_2(1)}, x_{\tau_2(2)}, \ldots, x_{\tau_2(n)}), \ldots, p(x_{\tau_{n!}(1)}, x_{\tau_{n!}(2)}, \ldots, x_{\tau_{n!}(n)})\},$$

που αφήνει τα $d_\nu(x_1, x_2, \ldots, x_n)$ αμετάβλητα αφού τα e_ν είναι συμμετρικά πολυώνυμα στις μεταβλητές $x_1, x_2, \ldots, x_{n!}$. Άρα, τα $d_\nu(x_1, x_2, \ldots, x_n)$ είναι συμμετρικά πολυώνυμα του $F[x_1, x_2, \ldots, x_n]$ και από την §133, η τιμή του $d_\nu(k_1, k_2, \ldots, k_n)$

στις ρίζες του $f(x) \in F[x]$ είναι στοιχείο του F. Οπότε, τα $e_\nu(a_1, a_2, \ldots, a_{n!})$ είναι στοιχεία του F και το $h(x) \in F[x] \subseteq K[x]$.

Τα $h(x) \in K[x]$, $g(x) \in K[x]$ έχουν κοινή ρίζα την $a_1 = a$. Έστω $q(x) \in K[x]$ ένας μέγιστος κοινός διαιρέτης των $h(x)$, $g(x)$. Από την §70, η $a_1 = a$ είναι ρίζα και του $q(x)$ οπότε, $deg[q(x)] \geq 1$. Επειδή, το $g(x)$ είναι ανάγωγο στο $K[x]$ δεν μπορεί να διαιρείται από πολυώνυμο του $K[x]$ βαθμού μικρότερου του βαθμού του $g(x)$. Άρα, υπάρχει $c \in K - \{0\}$ ώστε $q(x) = c\,g(x)$. Το $c\,g(x)$ διαιρεί το $h(x)$ δηλαδή, $h(x) = (c\,g(x))\,m(x)$ με $m(x) \in K[x]$ οπότε, $h(x) = g(x)\,(c\,m(x))$ με $c\,m(x) \in K[x]$ και το $g(x)$ διαιρεί το $h(x)$ στο $K[x]$ άρα, και στο $E[x] \supseteq K[x]$ όπως θέλαμε να δείξουμε και το συμπέρασμα προκύπτει.

§135. Έστω $\mathbf{E, F}$ σώματα με $\mathbf{E \supseteq F}$, $\mathbf{E/F}$ πεπερασμένη επέκταση του $\mathbf{F}$, $\mathbf{E/K}$ κανονική επέκταση του $\mathbf{K}$ για κάθε ενδιάμεσο σώμα $\mathbf{K}$ των $\mathbf{E, F}$. Τότε, η $\mathbf{E/F}$ είναι κανονική επέκταση του $\mathbf{F}$.

Το F είναι ενδιάμεσο σώμα των E, F. Το συμπέρασμα προκύπτει από την υπόθεση της §135 για $K = F$.

§136. Έστω $\mathbf{E, F}$ σώματα με $\mathbf{E \supseteq F}$, $\mathbf{E/F}$ κανονική επέκταση του $\mathbf{F}$. Τότε, $|\mathcal{G}(\mathbf{E/F})| = (\mathbf{E : F})$.

Η E/F ως κανονική επέκταση του F είναι πεπερασμένη. Από την §75, η E/F είναι απλή αλγεβρική επέκταση του F και άρα, $E = F(k)$ για κάποιο $k \in E$ αλγεβρικό επί του F. Έστω $k_1 = k, k_2, \ldots, k_n$ οι ρίζες ενός ελαχίστου πολυωνύμου του k στο $F[x]$. Έστω $p(x)$ το πολυώνυμο αυτό. Από τις §65, §71, το $p(x)$ είναι ανάγωγο στο $F[x]$ και οι ρίζες του είναι διακεκριμένες. Οπότε, ο βαθμός του $p(x)$ είναι n και από την §66, $(E : F) = n$. Μία ρίζα του $p(x)$, η $k_1 = k$, ανήκει στο E. Από την κανονικότητα της E/F, όλες οι ρίζες του $p(x)$ ανήκουν στο $E = F(k)$. Από την §126, $|\mathcal{G}(E/F)|$ ισούται με το πλήθος των ριζών του $p(x)$ που ανήκουν στο E δηλαδή, $|\mathcal{G}(E/F)| = n = (E : F)$.

§137. Έστω $\mathbf{E, F}$ σώματα με $\mathbf{E \supseteq F}$, $\mathbf{E/F}$ πεπερασμένη επέκταση του $\mathbf{F}$, $|\mathcal{G}(\mathbf{E/F})| = (\mathbf{E : F})$. Τότε, το $\mathbf{E}$ είναι σώμα διαχωρισμού για κάποιο $\mathbf{f(x) \in F[x]}$ στην επέκταση $\mathbf{K/F}$ που περιέχει τις ρίζες του $\mathbf{f(x)}$.

Από την §75, η E/F ως πεπερασμένη επέκταση του F είναι απλή αλγεβρική επέκταση του F και άρα, $E = F(k)$ για κάποιο $k \in E$ αλγεβρικό επί του F. Έστω $k_1 = k, k_2, \ldots, k_n$ οι ρίζες ενός ελαχίστου πολυωνύμου του k στο $F[x]$, και K/F μία επέκταση του F που περιέχει τις ρίζες αυτές, §42. Από την απόδειξη της §126 προκύπτει ότι, υπάρχει μία ένα προς ένα και επί αντιστοίχιση μεταξύ των στοιχείων της $\mathcal{G}(E/F)$ και εκείνων από τα $k_1 = k, k_2, \ldots, k_n$ που ανήκουν στο $E = F(k)$.

Έστω $p(x)$ το ελάχιστο πολυώνυμο του k με το οποίο δουλεύουμε. Από τις §65, §71, το $p(x)$ είναι ανάγωγο στο $F[x]$ και οι ρίζες του είναι διακεκριμένες. Οπότε, ο βαθμός του $p(x)$ είναι n και από την §66, $(E : F) = n$. Από την υπόθεση, $|\mathcal{G}(E/F)| = (E : F) = n$. Άρα, υπάρχει μία ένα προς ένα και επί αντιστοίχιση μεταξύ των n στοιχείων της $\mathcal{G}(E/F)$ και εκείνων από τα $k_1 = k, k_2, \ldots, k_n$ που ανήκουν στο $E = F(k)$. Το τελευταίο συμπέρασμα επάγει ότι

όλα τα $k_1 = k, k_2, \ldots, k_n$ ανήκουν στο E και,

$$E = F(k) \subseteq F(k_1, k_2, \ldots, k_n) \subseteq E,$$

$E = F(k_1, k_2, \ldots, k_n)$ είναι σώμα διαχωρισμού για το $p(x) \in F[x]$ στην επέκταση K/F που περιέχει τις ρίζες του $p(x)$.

§138. Έστω $\mathbf{E}, \mathbf{F}$ σώματα με $\mathbf{E} \supseteq \mathbf{F}$, $\mathbf{E/F}$ πεπερασμένη επέκταση του $\mathbf{F}$, $|\mathcal{G}(\mathbf{E/F})| = (\mathbf{E} : \mathbf{F})$. Τότε, $\mathbf{F}_{\mathcal{G}} = \mathbf{F}$.

Από την §129, το $F_{\mathcal{G}}$ είναι ενδιάμεσο σώμα των E, F. Από τις §134, §137, η $E/F_{\mathcal{G}}$ είναι κανονική επέκταση του $F_{\mathcal{G}}$. Από την §136, $|\mathcal{G}(E/F_{\mathcal{G}})| = (E : F_{\mathcal{G}})$. Κάθε στοιχείο της $\mathcal{G}(E/F_{\mathcal{G}})$ είναι αυτομορφισμός του E ταυτοτικός στο $F_{\mathcal{G}}$. Επειδή $F \subseteq F_{\mathcal{G}} \subseteq E$, κάθε στοιχείο της $\mathcal{G}(E/F_{\mathcal{G}})$ είναι αυτομορφισμός του E ταυτοτικός και στο F. Άρα, κάθε στοιχείο της της $\mathcal{G}(E/F_{\mathcal{G}})$ είναι και στοιχείο της $\mathcal{G}(E/F)$ και $\mathcal{G}(E/F_{\mathcal{G}}) \subseteq \mathcal{G}(E/F)$.

Από τον ορισμό του $F_{\mathcal{G}}$, κάθε στοιχείο της $\mathcal{G}(E/F)$ είναι ταυτοτικό στο $F_{\mathcal{G}}$. Άρα, κάθε στοιχείο της $\mathcal{G}(E/F)$ είναι και στοιχείο της $\mathcal{G}(E/F_{\mathcal{G}})$ και $\mathcal{G}(E/F) \subseteq \mathcal{G}(E/F_{\mathcal{G}})$. Οπότε, $\mathcal{G}(E/F_{\mathcal{G}}) = \mathcal{G}(E/F)$. Από τα προηγούμενα συμπεράσματα και την υπόθεση έχουμε,

$$(E : F_{\mathcal{G}}) = |\mathcal{G}(E/F_{\mathcal{G}})| = |\mathcal{G}(E/F)| = (E : F).$$

Επειδή $F \subseteq F_{\mathcal{G}} \subseteq E$, από την §49 προκύπτει,

$$(E : F) = (E : F_{\mathcal{G}})\,(F_{\mathcal{G}} : F) = (E : F)\,(F_{\mathcal{G}} : F).$$

Δηλαδή, $(F_{\mathcal{G}} : F) = 1$. Το τελευταίο συμπέρασμα επάγει ότι, κάθε βάση του $F_{\mathcal{G}}$ επί του F περιέχει ένα μόνο στοιχείο. Έστω $\{u\}$ μία βάση του $F_{\mathcal{G}}$ επί του F. Τότε, $F_{\mathcal{G}} \ni 1 = f\,u$ για κάποιο $f \in F - \{0\}$. Οπότε, $u = f^{-1} \in F$. Κάθε στοιχείο $a \in F_{\mathcal{G}}$ είναι γινόμενο κάποιου $g \in F$ με το u άρα, $a = g\,f^{-1} \in F$ και $F_{\mathcal{G}} \subseteq F$. Επειδή και $F \subseteq F_{\mathcal{G}}$ προκύπτει το τελικό συμπέρασμα.

§139. Έστω $\mathbf{E}, \mathbf{F}$ σώματα με $\mathbf{E} \supseteq \mathbf{F}$, $\mathbf{E/F}$ πεπερασμένη επέκταση του $\mathbf{F}$, $\mathbf{F}_{\mathcal{G}} = \mathbf{F}$. Τότε, $|\mathcal{G}(\mathbf{E/F})| = (\mathbf{E} : \mathbf{F})$.

Από την §75, η E/F ως πεπερασμένη επέκταση του F είναι απλή αλγεβρική επέκταση του F και άρα, $E = F(k)$ για κάποιο $k \in E$ αλγεβρικό επί του F. Έστω $k_1 = k, k_2, \ldots, k_n$ οι ρίζες ενός ελαχίστου πολυωνύμου του k στο $F[x]$. Έστω $p(x)$ το πολυώνυμο αυτό. Από τις §65, §71, το $p(x)$ είναι ανάγωγο στο $F[x]$ και οι ρίζες του είναι διακεκριμένες. Οπότε, ο βαθμός του $p(x)$ είναι n και από την §66, $(E : F) = n$. Έστω $|\mathcal{G}(E/F)| = m$. Θεωρούμε το πολυώνυμο $h(x) = \prod_{i=1}^{m} (x - \tau_i(k_1))$ με $\tau_i \in \mathcal{G}(E/F)$. Θα δείξουμε ότι $h(x) \in F[x]$.

$$h(x) = x^m + \sum_{\nu=1}^{m} (-1)^{\nu}\, e_{\nu}(\tau_1(k_1), \tau_2(k_1), \ldots, \tau_m(k_1))\, x^{m-\nu},$$

με $e_{\nu}(\tau_1(k_1), \tau_2(k_1), \ldots, \tau_m(k_1))$ την τιμή του στοιχειώδους συμμετρικού πολυωνύμου $e_{\nu}(x_1, x_2, \ldots, x_m)$ στη m–άδα $(\tau_1(k_1), \tau_2(k_1), \ldots, \tau_m(k_1))$. Από την μορφή τους, κάθε $e_{\nu}(\tau_1(k_1), \tau_2(k_1), \ldots, \tau_m(k_1))$ είναι αποτέλεσμα πολλαπλασιασμών και προσθέσεων μεταξύ των $\tau_1(k_1), \tau_2(k_1), \ldots, \tau_m(k_1)$. Τα $\tau_1(k_1), \tau_2(k_1), \ldots, \tau_m(k_1)$ ως εικόνες του $k_1 \in E$ μέσω αυτομορφισμών του E, είναι στοιχεία του

E. Άρα, κάθε $e_\nu(\tau_1(k_1), \tau_2(k_1), \ldots, \tau_m(k_1))$ είναι αποτέλεσμα πολλαπλασιασμών και προσθέσεων μεταξύ στοιχείων του E και ανήκει στο E.

Έστω τώρα τυχαίο $\psi \in \mathcal{G}(E/F)$.

$$\begin{aligned} \psi(e_\nu(\tau_1(k_1), \tau_2(k_1), \ldots, \tau_m(k_1))) &= \\ = \psi\left(\sum_{1\le i_1<i_2<\cdots<i_\nu\le m} \tau_{i_1}(k_1)\,\tau_{i_2}(k_1)\ldots\tau_{i_\nu}(k_1)\right) &= \\ = \sum_{1\le i_1<i_2<\cdots<i_\nu\le m} \psi(\tau_{i_1}(k_1))\,\psi(\tau_{i_2}(k_1))\ldots\psi(\tau_{i_\nu}(k_1)) &= \\ = \sum_{1\le i_1<i_2<\cdots<i_\nu\le m} (\psi\,\tau_{i_1})(k_1)\,(\psi\,\tau_{i_2})(k_1)\ldots(\psi\,\tau_{i_\nu})(k_1) &= \\ = \sum_{1\le j_1<j_2<\cdots<j_\nu\le m} \tau_{j_1}(k_1)\,\tau_{j_2}(k_1)\ldots\tau_{j_\nu}(k_1), & \end{aligned}$$

γιατί, οι $\psi\,\tau_{i_t} = \tau_{j_t}$, $t = 1, 2, \ldots, \nu$, είναι διακεκριμένα στοιχεία της $\mathcal{G}(E/F)$. Πράγματι, αν $\psi(\tau_{i_\alpha}) = \psi(\tau_{i_\beta})$ με $\tau_{i_\alpha} \neq \tau_{i_\beta}$, τότε για κάθε $b \in E$ έπεται $(\psi\,\tau_{i_\alpha})(b) = (\psi\,\tau_{i_\beta})(b)$ ή $\psi(\tau_{i_\alpha}(b)) = \psi(\tau_{i_\beta}(b))$ ή, επειδή ο ψ είναι ένα προς ένα $\tau_{i_\alpha}(b) = \tau_{i_\beta}(b)$ που επάγει ότι $\tau_{i_\alpha} = \tau_{i_\beta}$ ως συναρτήσεις με ίδιο πεδίο ορισμού, το E, ίδιο σύνολο τιμών, το E, και ίδιες τιμές στα στοιχεία του E.

Το τελευταίο συμπέρασμα αντιβαίνει την υπόθεση $\tau_{i_\alpha} \neq \tau_{i_\beta}$ και άρα, οι $\psi\,\tau_{i_t} = \tau_{j_t}$, $t = 1, 2, \ldots, \nu$, είναι διακεκριμένα στοιχεία της $\mathcal{G}(E/F)$. Από τα πιο πάνω προκύπτει,

$$\begin{aligned} \psi(e_\nu(\tau_1(k_1), \tau_2(k_1), \ldots, \tau_m(k_1))) &= \\ = \sum_{1\le j_1<j_2<\cdots<j_\nu\le m} \tau_{j_1}(k_1)\,\tau_{j_2}(k_1)\ldots\tau_{j_\nu}(k_1) &= \\ = e_\nu(\tau_1(k_1), \tau_2(k_1), \ldots, \tau_m(k_1)), & \end{aligned}$$

για κάθε $\psi \in \mathcal{G}(E/F)$ εφ' όσον η ψ επελέγη τυχαία. Άρα, κάθε $e_\nu(\tau_1(k_1), \tau_2(k_1), \ldots, \tau_m(k_1))$ ανήκει στο $F_\mathcal{G}$ και από την υπόθεση $F_\mathcal{G} = F$. Τα $e_\nu(\tau_1(k_1), \tau_2(k_1), \ldots, \tau_m(k_1))$ που είναι $\mp$ οι συντελεστές του $h(x)$ είναι στοιχεία του F και το $h(x) \in F[x]$.

Οι ρίζες του $h(x)$ είναι $\tau_i(k_1)$, $i = 1, 2, \ldots, m$ δηλαδή, οι εικόνες του $k_1 = k$ μέσω κάθε στοιχείου της $\mathcal{G}(E/F)$. Άρα, και η εικόνα του $k_1 = k$ μέσω του $id \in \mathcal{G}(E/F)$. Το $id(k_1) = k_1 = k$ είναι ρίζα του $h(x)$ και τα $h(x) \in F[x]$, $p(x) \in F[x]$ έχουν κοινή ρίζα το k. Στο τελευταίο μέρος της απόδειξης της §134 δείξαμε ότι,

Αν δύο πολυώνυμα $\mathbf{a(x)}$, $\mathbf{b(x)}$ του ιδίου δακτυλίου πολυωνύμων $\mathbf{R[x]}$ έχουν κοινή ρίζα και το $\mathbf{a(x)}$ είναι ανάγωγο στον $\mathbf{R[x]}$, τότε το $\mathbf{a(x)}$ διαιρεί το $\mathbf{b(x)}$ στον $\mathbf{R[x]}$.

Στην περίπτωσή μας, το $p(x)$ διαιρεί το $h(x)$ και άρα, όλες οι ρίζες $k_1 = k, k_2, \ldots, k_n$ του $p(x)$ είναι μεταξύ των ριζών του $h(x)$. Αυτό σημαίνει ότι $m = deg[h(x)] \geq deg[p(x)] = n$. Από την §127, $m = |\mathcal{G}(E/F)| \leq (E : F) = n$. Τελικά, $m = n$ και το συμπέρασμα προκύπτει.

§140. Έστω $\mathbf{E}, \mathbf{F}$ σώματα με $\mathbf{E} \supseteq \mathbf{F}$, $\mathbf{E/F}$ πεπερασμένη επέκταση του $\mathbf{F}$. Στις §132, §134, §135, §136, §137, §138, §139 απεδείχθη η ισοδυναμία των κάτωθι προτάσεων,

- **Η $\mathbf{E/F}$ είναι κανονική επέκταση του $\mathbf{F}$.**

$$\Updownarrow$$

- **Το $\mathbf{E}$ είναι σώμα διαχωρισμού για κάποιο $\mathbf{f(x) \in F[x]}$.**

$$\Updownarrow$$

- $|\mathcal{G}(\mathbf{E/F})| = (\mathbf{E : F})$.

$$\Updownarrow$$

- **Το $\mathbf{F}_{\mathcal{G}} = \mathbf{F}$.**

$$\Updownarrow$$

- **Η $\mathbf{E/K}$ είναι κανονική επέκταση για κάθε ενδιάμεσο σώμα $\mathbf{K}$ των $\mathbf{E}, \mathbf{F}$.**

§141. Έστω $\mathbf{E}, \mathbf{F}$ σώματα με $\mathbf{E} \supseteq \mathbf{F}$, $\mathbf{E/F}$ κανονική επέκταση του $\mathbf{F}$. Σε κάθε ενδιάμεσο σώμα $\mathbf{K}$ των $\mathbf{E}, \mathbf{F}$ αντιστοιχεί μοναδική υποομάδα $\mathcal{G}(\mathbf{E/K})$ της $\mathcal{G}(\mathbf{E/F})$ που έχει το $\mathbf{K}$ ως σταθερό σώμα και αντιστρόφως. Επίσης, $\mathbf{F \subseteq K_1 \subseteq K_2 \subseteq E}$ αν και μόνο αν $\mathcal{G}(\mathbf{E/K_2}) \subseteq \mathcal{G}(\mathbf{E/K_1}) \subseteq \mathcal{G}(\mathbf{E/F})$.

Για το ευθύ. Έστω $F \subseteq K \subseteq E$. Θέτουμε,

$$\mathcal{K} = \{\tau \in \mathcal{G}(E/F) \,:\, \tau(k) = k \,, \forall\, k \in K\}.$$

Το $\mathcal{K}$ δεν είναι κενό αφού περιέχει τον $id \in \mathcal{G}(E/F)$. Το $\mathcal{K} \subseteq \mathcal{G}(E/F)$ από τον ορισμό του. Θα δείξουμε ότι το $\mathcal{K}$ είναι ομάδα ως προς την πράξη της $\mathcal{G}(E/F)$.

- Αν $\tau_1, \tau_2 \in \mathcal{K}$, τότε οι $\tau_1\,\tau_2$ και $\tau_2\,\tau_1$ είναι στοιχεία της $\mathcal{G}(E/F)$ ως «γινόμενα» στοιχείων της $\mathcal{G}(E/F)$. Επιπλέον, $(\tau_1\,\tau_2)(k) = \tau_1(\tau_2(k)) = \tau_1(k) = k$ και $(\tau_2\,\tau_1)(k) = \tau_2(\tau_1(k)) = \tau_2(k) = k$ για κάθε $k \in K$. Άρα, $\tau_1\,\tau_2$ και $\tau_2\,\tau_1 \in \mathcal{K}$ και το $\mathcal{K}$ είναι κλειστό ως προς την πράξη.

- Ουδέτερο στοιχείο της πράξης στο $\mathcal{K}$ είναι ο id που όπως προείπαμε ανήκει σε αυτό.

- Αν $\tau \in \mathcal{K}$, τότε και $\tau^{-1} \in \mathcal{K}$ αφού, ο τ^{-1} είναι στοιχείο της $\mathcal{G}(E/F)$ και $\tau^{-1}(k) = \tau^{-1}(\tau(k)) = k$ για κάθε $k \in K$. Κάθε στοιχείο του $\mathcal{K}$ έχει αντίστροφο.

- Επειδή τα στοιχεία του $\mathcal{K}$ είναι και στοιχεία της $\mathcal{G}(E/F)$, για αυτά ισχύει η προσετεριστικότητα του «γινομένου», (σύνθεσης), συναρτήσεων.

Το $\mathcal{K}$ είναι η υποομάδα $\mathcal{G}(E/K)$ της $\mathcal{G}(E/F)$ γιατί περιέχει τους αυτομορφισμούς του E που είναι ταυτοτικοί στο K. Επειδή η E/F είναι κανονική επέκταση του F, από την §140, η E/K είναι κανονική επέκταση του ενδιαμέσου σώματος K και από την §140 εκ΄ νέου, το σταθερό σώμα της $\mathcal{G}(E/K)$ είναι $K_{\mathcal{G}} = K$. Άρα, στο ενδιάμεσο σώμα K των E, F αντιστοιχεί η υποομάδα $\mathcal{G}(E/K)$ της $\mathcal{G}(E/F)$ με σταθερό σώμα K.

Για τη μοναδικότητα του ευθέως. Έστω $H \neq \mathcal{G}(E/K)$ υποομάδα της $\mathcal{G}(E/F)$ η οποία έχει σταθερό σώμα $K_H = K$. Επειδή η E/K είναι κανονική επέκταση του K, είναι και πεπερασμένη επέκταση του K και από την §75, E/K είναι απλή αλγεβρική επέκταση του K και άρα, $E = K(c)$ για κάποιο $c \in E$ αλγεβρικό επί του K. Έστω $c_1 = c, c_2, \ldots, c_n$ οι ρίζες ενός ελαχίστου πολυωνύμου του c στο $K[x]$. Έστω $p(x)$ το πολυώνυμο αυτό. Από τις §65, §71, το $p(x)$ είναι ανάγωγο στο $K[x]$ και οι ρίζες του είναι διακεκριμένες. Οπότε, ο βαθμός του $p(x)$ είναι n και από την §66, $(E : K) = n$.

Έστω $|H| = m$. Θεωρούμε το πολυώνυμο $h(x) = \prod_{i=1}^{m} (x - \tau_i(c_1))$ με $\tau_i \in H$. Θα δείξουμε ότι $h(x) \in K[x]$.

$$h(x) = x^m + \sum_{\nu=1}^{m} (-1)^\nu \, e_\nu(\tau_1(c_1), \tau_2(c_1), \ldots, \tau_m(c_1)) \, x^{m-\nu},$$

με $e_\nu(\tau_1(c_1), \tau_2(c_1), \ldots, \tau_m(c_1))$ η τιμή του στοιχειώδους συμμετρικού πολυωνύμου $e_\nu(x_1, x_2, \ldots, x_m)$ στη m–άδα $(\tau_1(c_1), \tau_2(c_1), \ldots, \tau_m(c_1))$. Από την μορφή τους, κάθε $e_\nu(\tau_1(c_1), \tau_2(c_1), \ldots, \tau_m(c_1))$ είναι αποτέλεσμα πολλαπλασιασμών και προσθέσεων μεταξύ των $\tau_1(c_1), \tau_2(c_1), \ldots, \tau_m(c_1)$. Τα $\tau_1(c_1), \tau_2(c_1), \ldots, \tau_m(c_1)$ ως εικόνες του $c_1 \in E$ μέσω αυτομορφισμών του E, είναι στοιχεία του E. Άρα, κάθε $e_\nu(\tau_1(c_1), \tau_2(c_1), \ldots, \tau_m(c_1))$ είναι αποτέλεσμα πολλαπλασιασμών και προσθέσεων μεταξύ στοιχείων του E και ανήκει στο E.

Έστω τώρα τυχαίο $\psi \in H$.

$$\begin{aligned}
\psi(e_\nu(\tau_1(c_1), \tau_2(c_1), \ldots, \tau_m(c_1))) &= \\
= \psi \left(\sum_{1 \leq i_1 < i_2 < \cdots < i_\nu \leq m} \tau_{i_1}(c_1) \, \tau_{i_2}(c_1) \ldots \tau_{i_\nu}(c_1) \right) &= \\
= \sum_{1 \leq i_1 < i_2 < \cdots < i_\nu \leq m} \psi(\tau_{i_1}(c_1)) \, \psi(\tau_{i_2}(c_1)) \ldots \psi(\tau_{i_\nu}(c_1)) &= \\
= \sum_{1 \leq i_1 < i_2 < \cdots < i_\nu \leq m} (\psi \, \tau_{i_1})(c_1) \, (\psi \, \tau_{i_2})(c_1) \ldots (\psi \, \tau_{i_\nu})(c_1) &= \\
= \sum_{1 \leq j_1 < j_2 < \cdots < j_\nu \leq m} \tau_{j_1}(c_1) \, \tau_{j_2}(c_1) \ldots \tau_{j_\nu}(c_1), &
\end{aligned}$$

γιατί, οι $\psi \, \tau_{i_t} = \tau_{j_t}$, $t = 1, 2, \ldots, \nu$, είναι διακεκριμένα στοιχεία της H. Πράγματι, αν $\psi(\tau_{i_\alpha}) = \psi(\tau_{i_\beta})$ με $\tau_{i_\alpha} \neq \tau_{i_\beta}$, τότε για κάθε $b \in E$ έπεται $(\psi \, \tau_{i_\alpha})(b) = (\psi \, \tau_{i_\beta})(b)$ ή $\psi(\tau_{i_\alpha}(b)) = \psi(\tau_{i_\beta}(b))$ ή, επειδή ο ψ είναι ένα προς ένα $\tau_{i_\alpha}(b) = \tau_{i_\beta}(b)$ που επάγει ότι $\tau_{i_\alpha} = \tau_{i_\beta}$ ως συναρτήσεις με ίδιο πεδίο ορισμού, το E, ίδιο σύνολο τιμών, το E, και ίδιες τιμές στα στοιχεία του E.

Το τελευταίο συμπέρασμα αντιβαίνει την υπόθεση $\tau_{i_\alpha} \neq \tau_{i_\beta}$ και άρα, οι $\psi \, \tau_{i_t} = \tau_{j_t}$, $t = 1, 2, \ldots, \nu$, είναι διακεκριμένα στοιχεία της H. Από τα πιο πάνω προκύπτει,

$$\begin{aligned}
\psi(e_\nu(\tau_1(c_1), \tau_2(c_1), \ldots, \tau_m(c_1))) &= \\
= \sum_{1 \leq j_1 < j_2 < \cdots < j_\nu \leq m} \tau_{j_1}(c_1) \, \tau_{j_2}(c_1) \ldots \tau_{j_\nu}(c_1) &= \\
= e_\nu(\tau_1(c_1), \tau_2(c_1), \ldots, \tau_m(c_1)), &
\end{aligned}$$

για κάθε $\psi \in H$ εφ' όσον η ψ επελέγη τυχαία. Άρα, κάθε $e_\nu(\tau_1(c_1), \tau_2(c_1), \ldots, \tau_m(c_1))$ ανήκει στο K_H και από την υπόθεση $K_H = K$. Τα $e_\nu(\tau_1(c_1), \tau_2(c_1), \ldots, \tau_m(c_1))$ που είναι $\mp$ οι συντελεστές του $h(x)$ είναι στοιχεία του K και το $h(x) \in K[x]$.

Οι ρίζες του $h(x)$ είναι $\tau_i(c_1)$, $i = 1, 2, \ldots, m$ δηλαδή, οι εικόνες του $c_1 = c$ μέσω κάθε στοιχείου της H. Άρα, και η εικόνα του $c_1 = c$ μέσω του $id \in H$. Το $id(c_1) = c_1 = c$ είναι ρίζα του $h(x)$ και τα $h(x) \in K[x]$, $p(x) \in K[x]$ έχουν κοινή ρίζα το c. Κατ' αναλογία με την απόδειξη της §139, το $p(x)$ διαιρεί το $h(x)$ και άρα, όλες οι ρίζες $c_1 = c, c_2, \ldots, c_n$ του $p(x)$ είναι μεταξύ των ριζών του $h(x)$. Αυτό σημαίνει ότι $m = deg[h(x)] \geq deg[p(x)] = n$. Από την §127, $|\mathcal{G}(E/K)| \leq (E : K) = n \leq m = |H|$. Τελικά, $m = n$.

Επειδή η H έχει υποτεθεί υποομάδα της $\mathcal{G}(E/F)$ με σταθερό σώμα το K, κάθε στοιχείο της H είναι στοιχείο της $\mathcal{G}(E/F)$ που είναι ταυτοτικό στο K. Όμως εξ' ορισμού, τα στοιχεία της $\mathcal{G}(E/F)$ που είναι ταυτοτικά στο K ανήκουν στην $\mathcal{G}(E/K)$. Άρα, τα στοιχεία της H ανήκουν στην $\mathcal{G}(E/K)$ και η H είναι γνήσια υποομάδα της $\mathcal{G}(E/K)$ αφού υποθέσαμε ότι $H \neq \mathcal{G}(E/K)$. Οπότε, $|\mathcal{G}(E/K)| > |H|$. Όμως, επειδή η E/K είναι κανονική επέκταση του K από την §140, $|\mathcal{G}(E/K)| = (E : K) = n = m = |H|$. Άρα, κακώς υποθέσαμε ότι $H \neq \mathcal{G}(E/K)$ και $H = \mathcal{G}(E/K)$.

Για το αντίστροφο. Έστω H υποομάδα της $\mathcal{G}(E/F)$. Θα δείξουμε ότι, υπάρχει μοναδικό ενδιάμεσο σώμα K των E, F, που να είναι το σταθερό σώμα της H. Θεωρούμε το σύνολο,

$$K = \{a \in E \,:\, \tau(a) = a\,, \forall\, \tau \in H\}.$$

Θα δείξουμε ότι το K είναι ενδιάμεσο σώμα των E, F.

Κάθε στοιχείο της H είναι και στοιχείο της $\mathcal{G}(E/F)$. Άρα, για κάθε $a \in F$ και κάθε $\tau \in H$, $\tau(a) = a$ και $F \subseteq K$. Από τον ορισμό του, το $K \subseteq E$. Αρκεί να αποδείξουμε ότι το K είναι σώμα. Από την §2, αρκεί τα στοιχεία του K να ικανοποιούν τις ιδιότητες (I1–I9) ως προς την «πρόσθεση» και τον «πολλαπλασιασμό» του E.

(I1). Για κάθε $a, b \in K$ και κάθε $\tau \in H$ έχουμε, $\tau(a+b) = \tau(a)+\tau(b) = a+b$, $\tau(b+a) = \tau(b)+\tau(a) = b+a$. Επιπλέον, $a+b = b+a$ γιατί τα a, b ανήκουν και στο E που είναι σώμα. Άρα, $a+b = b+a \in K$.

(I2). Από την §123, $\tau(0) = 0$ για κάθε $\tau \in H$ οπότε, $0 \in K$ δηλαδή, το ουδέτερο στοιχείο της «πρόσθεσης» του E ανήκει στο K.

(I3). Για κάθε $a \in K - \{0\}$, και κάθε $\tau \in H$ από την §123 έχουμε, $\tau(-a) = -\tau(a) = -a$. Άρα, για κάθε $a \in K - \{0\}$ το μοναδικό του αντίθετο ως προς την «πρόσθεση» του E ανήκει στο K.

(I4). Επειδή τα στοιχεία του K είναι και στοιχεία του σώματος E, ισχύει για αυτά η προσεταιριστική ιδιότητα ως προς την «πρόσθεση» του E.

(I5). Για κάθε $a, b \in K$ και κάθε $\tau \in H$ έχουμε, $\tau(a\,b) = \tau(a)\,\tau(b) = a\,b$, $\tau(b\,a) = \tau(b)\,\tau(a) = b\,a$. Επιπλέον, $a\,b = b\,a$ γιατί τα a, b ανήκουν και στο E που είναι σώμα. Άρα, $a\,b = b\,a \in K$.

(I6). Από την §123, $\tau(1) = 1$ για κάθε $\tau \in H$ οπότε, $1 \in K$ δηλαδή, το ουδέτερο στοιχείο του «πολλαπλασιασμού» του E ανήκει στο K.

(I7). Για κάθε $a \in K - \{0\}$, και κάθε $\tau \in H$ από την §123 έχουμε, $\tau(a^{-1}) = (\tau(a))^{-1} = a^{-1}$. Άρα, για κάθε $a \in K - \{0\}$ το μοναδικό του αντίστροφο ως

προς τον «πολλαπλασιασμό» του E ανήκει στο K.
(I8). Επειδή τα στοιχεία του K είναι και στοιχεία του σώματος E, ισχύει για αυτά η προσετεριστική ιδιότητα ως προς τον «πολλαπλασιασμό» του E.
(I9). Επειδή τα στοιχεία του K είναι και στοιχεία του σώματος E, ισχύει για αυτά η επιμεριστική του «πολλαπλασιασμού» του E επί της «πρόσθεσης» του E. Το K είναι μοναδικό γιατί είναι το μεγαλύτερο ενδιάμεσο σώμα των E, F που είναι σταθερό σώμα για την H. Και η $H = \mathcal{G}(E/K)$. Το συμπέρασμα προκύπτει.

Για την απόδειξη της ισοδυναμίας σχετικά με την σχέση του περιέχεσθε έχουμε,

Έστω $F \subseteq K_1 \subseteq K_2 \subseteq E$. Κάθε αυτομορφισμός του E που είναι ταυτοτικός στο K_2 είναι ταυτοτικός στο υποσύνολό του K_2, το K_1. Άρα, κάθε στοιχείο της $\mathcal{G}(E/K_2)$ είναι και στοιχείο της $\mathcal{G}(E/K_1)$ ή, $\mathcal{G}(E/K_2) \subseteq \mathcal{G}(E/K_1)$.

Αντιστρόφως, αν $\mathcal{G}(E/K_2) \subseteq \mathcal{G}(E/K_1)$, για κάθε $a \in K_1$ και κάθε $\tau \in \mathcal{G}(E/K_2)$ έπεται, $\tau(a) = a$ γιατί ο τ είναι και στοιχείο της $\mathcal{G}(E/K_1)$ δηλαδή, ταυτοτικός και στο K_1. Άρα, τα στοιχεία του K_1 μένοντας αμετάβλητα από κάθε στοιχείο της $\mathcal{G}(E/K_2)$ ανήκουν στο σταθερό σώμα της $\mathcal{G}(E/K_2)$ που από το προηγούμενο μέρος της απόδειξης ξέρουμε ότι είναι το K_2. Άρα, $K_1 \subseteq K_2$.

Από τα πιο πάνω είναι άμεσο ότι, $\mathbf{F \subseteq K_1 \subseteq K_2 \subseteq E}$ αν και μόνο αν $\mathcal{G}(\mathbf{E/K_2}) \subseteq \mathcal{G}(\mathbf{E/K_1}) \subseteq \mathcal{G}(\mathbf{E/F})$.

§142. Έστω $\mathbf{E, F}$ σώματα με $\mathbf{E \supseteq F}$, $\mathbf{E/F}$ πεπερασμένη επέκταση του $\mathbf{F}$, $\mathbf{K}$ ενδιάμεσο σώμα των $\mathbf{E, F}$, $\tau \in \mathcal{G}(\mathbf{E/F})$,

$$\tau(\mathbf{K}) = \{\tau(\mathbf{k}) \,:\, \mathbf{k} \in \mathbf{K}\}.$$

Τότε, το $\tau(\mathbf{K})$ είναι επίσης ενδιάμεσο σώμα των $\mathbf{E, F}$ και $(\mathbf{K} : \mathbf{F}) = (\tau(\mathbf{K}) : \mathbf{F})$.

Επειδή, $F \subseteq K \subseteq E$ κάθε στοιχείο $a \in F$ ανήκει στο K και $a = \tau(a) \in \tau(K)$ δηλαδή, $F \subseteq \tau(K)$. Κάθε $k \in K$ ανήκει και στο E. $\tau(k) \in E$ και $\tau(K) \subseteq E$. Δείξαμε ότι, $F \subseteq \tau(K) \subseteq E$. Απομένει να δείξουμε ότι το $\tau(K)$ είναι σώμα ως προς την «πρόσθεση» και τον «πολλαπλασιασμό» του E.
(I1). Για κάθε $\tau(a), \tau(b) \in \tau(K)$ έχουμε, $\tau(a) + \tau(b) = \tau(a + b) \in \tau(K)$, $\tau(b) + \tau(a) = \tau(b + a) \in \tau(K)$. Επιπλέον, $a + b = b + a$ γιατί τα a, b ανήκουν στο K που είναι σώμα. Άρα, $\tau(a) + \tau(b) = \tau(b) + \tau(a) \in \tau(K)$.
(I2). Από την §123, $0 = \tau(0) \in \tau(K)$ δηλαδή, το ουδέτερο στοιχείο της «πρόσθεσης» του E ανήκει στο $\tau(K)$.
(I3). Για κάθε $\tau(a) \in \tau(K) - \{0\}$ από την §123 έχουμε, $-\tau(a) = \tau(-a) \in \tau(K)$. Άρα, για κάθε $\tau(a) \in \tau(K) - \{0\}$ το μοναδικό του αντίθετο ως προς την «πρόσθεση» του E ανήκει στο $\tau(K)$.
(I4). Επειδή τα στοιχεία του $\tau(K)$ είναι και στοιχεία του σώματος E, ισχύει για αυτά η προσετεριστική ιδιότητα ως προς την «πρόσθεση» του E.
(I5). Για κάθε $\tau(a), \tau(b) \in \tau(K)$ έχουμε, $\tau(a)\,\tau(b) = \tau(a\,b) \in \tau(K)$, $\tau(b)\,\tau(a) = \tau(b\,a) \in \tau(K)$. Επιπλέον, $a\,b = b\,a$ γιατί τα a, b ανήκουν στο K που είναι σώμα. Άρα, $\tau(a)\,\tau(b) = \tau(b)\,\tau(a) \in \tau(K)$.
(I6). Από την §123, $1 = \tau(1) \in \tau(K)$ οπότε, $1 \in \tau(K)$ δηλαδή, το ουδέτερο στοιχείο του «πολλαπλασιασμού» του E ανήκει στο $\tau(K)$.
(I7). Για κάθε $\tau(a) \in \tau(K) - \{0\}$, από την §123 έχουμε, $(\tau(a))^{-1} = \tau(a^{-1}) \in \tau(K)$. Άρα, για κάθε $\tau(a) \in \tau(K) - \{0\}$ το μοναδικό του αντίστροφο ως προς τον «πολλαπλασιασμό» του E ανήκει στο $\tau(K)$.

(I8). Επειδή τα στοιχεία του $\tau(K)$ είναι και στοιχεία του σώματος E, ισχύει για αυτά η προσετεριστική ιδιότητα ως προς τον «πολλαπλασιασμό» του E.
(I9). Επειδή τα στοιχεία του $\tau(K)$ είναι και στοιχεία του σώματος E, ισχύει για αυτά η επιμεριστική του «πολλαπλασιασμού» του E επί της «πρόσθεσης» του E.

Το $\tau(K)$ είναι ενδιάμεσο σώμα των E, F. Έστω τώρα $(K : F) = n$ και $\{k_1, k_2, \ldots, k_n\}$ μία βάση της επέκτασης K/F του F. Επειδή τα $k_i \in K$, τα $\tau(k_i) \in \tau(K)$. Θα δείξουμε ότι η $\{\tau(k_1), \tau(k_2), \ldots, \tau(k_n)\}$ είναι μία βάση της επέκτασης $\tau(K)/F$ του F.

Έστω $\sum_{i=1}^{n} f_i\, \tau(k_i) = 0$ με $f_i \in F$. Τότε,

$$0 = \sum_{i=1}^{n} \tau(f_i)\, \tau(k_i) = \sum_{i=1}^{n} \tau(f_i\, k_i) = \tau\left(\sum_{i=1}^{n} f_i\, k_i\right) \overset{\S 123}{\Rightarrow} 0 = \sum_{i=1}^{n} f_i\, k_i,$$

που συνεπάγεται $f_i = 0$, $i = 1, 2, \ldots, n$ γιατί τα k_i, ως στοιχεία μίας βάσης της επέκτασης K/F επί του F, είναι γραμμικώς ανεξάρτητα επί του F.
Έστω $\tau(k) \in \tau(K)$. Το k ως στοιχείο του K γράφεται ως γραμμικός συνδυασμός των στοιχείων της βάσης $\{k_1, k_2, \ldots, k_n\}$ της επέκτασης K/F του F. Έτσι, υπάρχουν $f_i \in F$ ώστε $k = \sum_{i=1}^{n} f_i\, k_i$ και,

$$\tau(k) = \tau\left(\sum_{i=1}^{n} f_i\, k_i\right) = \sum_{i=1}^{n} \tau(f_i\, k_i) = \sum_{i=1}^{n} \tau(f_i)\, \tau(k_i) = \sum_{i=1}^{n} f_i\, \tau(k_i).$$

Κάθε στοιχείο του $\tau(K)$ γράφεται ως γραμμικός συνδυασμός επί του F των στοιχείων του συνόλου $\{\tau(k_1), \tau(k_2), \ldots, \tau(k_n)\}$. Αποδείξαμε ότι το σύνολο $\{\tau(k_1), \tau(k_2), \ldots, \tau(k_n)\}$ είναι μία βάση της επέκτασης $\tau(K)/F$ του F και $n = (K : F) = (\tau(K) : F)$.

§143. Έστω $\mathbf{E}, \mathbf{F}$ σώματα με $\mathbf{E} \supseteq \mathbf{F}$, $\mathbf{E}/\mathbf{F}$ επέκταση του $\mathbf{F}$, $\mathbf{k} \in \mathbf{E}$ αλγεβρικό επί του $\mathbf{F}$, $\tau \in \mathcal{G}(\mathbf{E}/\mathbf{F})$ ώστε $\tau(\mathbf{k}) = \mathbf{k}$. Τότε, ο τ είναι ταυτοτικός στο $\mathbf{F}(\mathbf{k})$.

Από την §66 προκύπτει ότι, η επέκταση $F(k)/F$ είναι πεπερασμένη και αν d είναι η διάστασή της, κάθε στοιχείο του $F(k)$ γράφεται ως $\sum_{i=0}^{d-1} f_i\, k^i$ με $f_i \in F$. Τότε,

$$\tau\left(\sum_{i=0}^{d-1} f_i\, k^i\right) = \sum_{i=0}^{d-1} \tau(f_i)\, \tau(k^i) = \sum_{i=0}^{d-1} f_i\, \tau(k)^i = \sum_{i=0}^{d-1} f_i\, k^i,$$

και κάθε στοιχείο του $F(k)$ απεικονίζεται μέσω του τ στον εαυτό του. Το συμπέρασμα προκύπτει.

§144. Έστω $\mathbf{E}, \mathbf{F}$ σώματα με $\mathbf{E} \supseteq \mathbf{F}$, $\mathbf{E}/\mathbf{F}$ επέκταση του $\mathbf{F}$, $\mathbf{K_1}, \mathbf{K_2}$ ενδιάμεσα σώματα των $\mathbf{E}, \mathbf{F}$. Τα $\mathbf{K_1}, \mathbf{K_2}$ λέγονται συζυγή αν υπάρχουν $\mathbf{k_1}, \mathbf{k_2} \in \mathbf{E}$ αλγεβρικά επί του $\mathbf{F}$ ώστε τα $\mathbf{k_1}, \mathbf{k_2}$ να έχουν ένα ίδιο ελάχιστο πολυώνυμο στο $\mathbf{F}[\mathbf{x}]$ και $\mathbf{K_1} = \mathbf{F}(\mathbf{k_1})$, $\mathbf{K_2} = \mathbf{F}(\mathbf{k_2})$.

§145. Έστω $\mathbf{G}$ ομάδα με πεπερασμένου πλήθους στοιχεία, $\mathbf{H}$ υποομάδα της $\mathbf{G}$, $\mathbf{g} \in \mathbf{G}$. Τα σύνολα $\mathbf{gH}$, $\mathbf{Hg}$ λέγονται αριστερό, δεξί σύμπλοκο της $\mathbf{H}$ στην $\mathbf{G}$ αντιστοίχως.

Στην §90, αποδείξαμε ότι η ομάδα G μπορεί να γραφεί ως $G = H \cup (g_1\, H) \cup \cdots \cup (g_n\, H)$ με $g_i \in G - (H \cup (g_1\, H) \cup \cdots \cup (g_{i-1}\, H))$, $i = 1, 2, \ldots, n$, $g_0 = 1$ και

ανά δύο τα $H, g_1 H, \cdots, g_n H$ δεν έχουν κοινά στοιχεία. Δηλαδή, η G μπορεί να γραφεί ως πεπερασμένη ένωση ξένων ανά δύο αριστερών συμπλόκων της H στην G. Κατ΄ αναλογία, η G μπορεί να γραφεί ως πεπερασμένη ένωση ξένων ανά δύο δεξιών συμπλόκων της H στην G. Οι δύο τρόποι γραφής εμπεριέχουν το ίδιο πλήθος συμπλόκων. Το πλήθος τους, είναι ο δείκτης της H στην G.

§146. Έστω $\mathbf{E}, \mathbf{F}$ σώματα με $\mathbf{E} \supseteq \mathbf{F}$, $\mathbf{E}/\mathbf{F}$ κανονική επέκταση του $\mathbf{F}$, $\mathbf{k} \in \mathbf{E}$ αλγεβρικό επί του $\mathbf{F}$, $\mathbf{p(x)} \in \mathbf{F[x]}$ ένα ελάχιστο πολυώνυμο του $\mathbf{k}$ στο $\mathbf{F[x]}$ βαθμού $\mathbf{n}$, $\{\mathbf{k_1} = \mathbf{k}, \mathbf{k_2}, \ldots, \mathbf{k_n}\}$ οι ρίζες του $\mathbf{p(x)}$. Τότε, υπάρχουν $(\mathbf{E} : \mathbf{F(k_1)})$ το πλήθος στοιχεία τ της $\mathcal{G}(\mathbf{E}/\mathbf{F})$ ώστε $\tau(\mathbf{k_1}) = \mathbf{k_i}$, $\mathbf{i} = \mathbf{1}, \mathbf{2}, \ldots, \mathbf{n}$.

Επειδή, το $F(k_1)$ είναι ενδιάμεσο σώμα των E, F από την §141, η $\mathcal{G}(E/F(k_1))$ είναι η μοναδική υποομάδα της $\mathcal{G}(E/F)$ που έχει το $F(k_1)$ ως σταθερό σώμα είναι δηλαδή, η ομάδα Galois της επέκτασης $E/F(k_1)$. Έστω m ο δείκτης της $\mathcal{G}(E/F(k_1))$ στην $\mathcal{G}(E/F)$. Επειδή,

$$|\mathcal{G}(E/F)| = [\mathcal{G}(E/F) : \mathcal{G}(E/F(k_1))]\, |\mathcal{G}(E/F(k_1))| = m\, |\mathcal{G}(E/F(k_1))|,$$

και $|\mathcal{G}(E/F)| \geq 1$ εφ΄ όσον $id \in \mathcal{G}(E/F)$, προκύπτει ότι $m \in \mathbb{N} - \{0\}$. Από την §66, $(F(k_1) : F) = n$ και από την §49,

$$(E : F) = (E : F(K_1))\, (F(k_1) : F) = (E : F(K_1))\, n.$$

Επειδή η E/F είναι κανονική επέκταση του F, από την §140, $|\mathcal{G}(E/F)| = (E : F)$. Επίσης, από την §140, η $E/F(k_1)$ είναι κανονική επέκταση του $F(k_1)$ και $|\mathcal{G}(E/F(k_1))| = (E : F(k_1))$. Επίσης, $|\mathcal{G}(E/F(k_1))| \geq 1$ εφ΄ όσον $id \in \mathcal{G}(E/F(k_1))$. Άρα,

$$m\, |\mathcal{G}(E/F(k_1))| = |\mathcal{G}(E/F)| = (E : F) = (E : F(K_1))\, n = |\mathcal{G}(E/F(k_1))|\, n,$$

που από την §145, επάγει ότι η $\mathcal{G}(E/F(k_1))$ έχει n το πλήθος ξένα μεταξύ τους σύμπλοκα στην $\mathcal{G}(E/F)$. Έστω,

$$\psi_1\, \mathcal{G}(E/F(k_1)),\ \psi_2\, \mathcal{G}(E/F(k_1)),\ \ldots,\ \psi_n\, \mathcal{G}(E/F(k_1)),$$

με $\psi_t \in \mathcal{G}(E/F)$, $t = 1, 2, \ldots, n$ τα σύμπλοκα αυτά. Από την §65, το $p(x)$ είναι ανάγωγο στο $F[x]$ και μία ρίζα του, η $k_1 = k$, ανήκει στην κανονική επέκταση E/F του F. Τότε, και όλες οι ρίζες $k_1, k_2, \ldots, k_n$ του $p(x)$ ανήκουν στην επέκταση E/F του F. Από την απόδειξη της §124, η εικόνα μίας ρίζας του $p(x)$ μέσω ενός στοιχείου της $\mathcal{G}(E/F)$ είναι εκ΄ νέου ρίζα του $p(x)$. Άρα, $\psi_t(k_1) = k_i$, για $t = 1, 2, \ldots, n$, είναι ρίζες του $p(x)$.

Θα δείξουμε ότι, οι $\psi_t(k_1)$, για $t = 1, 2, \ldots, n$, είναι διακεκριμένες μεταξύ τους. Έστω, $\psi_j(k_1) = \psi_t(k_1)$ για κάποια j, t διακεκριμένα στοιχεία του $\{1, 2, \ldots, n\}$. Τότε,

$$\psi_j(k_1) = \psi_t(k_1) \Rightarrow (\psi_t^{-1}\, \psi_j)(k_1) = k_1 \Rightarrow \psi_t^{-1}\, \psi_j \in \mathcal{G}(E/F(k_1)),$$

γιατί, ο $\psi_t^{-1}\, \psi_j$ είναι αυτομορφισμός του E, (ως «γινόμενο» αυτομορφισμών του E), και από την §143, ταυτοτικός στο $F(k_1)$. Υπάρχει $\omega \in \mathcal{G}(E/F(k_1))$ ώστε,

$$(\psi_t^{-1}\, \psi_j) = \omega \Rightarrow \psi_j = \psi_t\, \omega \in \psi_t\, \mathcal{G}(E/F(k_1)) \Rightarrow$$
$$\psi_j\, \mathcal{G}(E/F(k_1)) \subseteq \psi_t\, \mathcal{G}(E/F(k_1)),$$

άτοπο γιατί τα σύμπλοκα είναι ξένα μεταξύ τους. Δείξαμε λοιπόν ότι, οι $\psi_t(k_1)$, για $t = 1, 2, \ldots, n$, είναι n το πλήθος διακεκριμένες μεταξύ τους ρίζες του $p(x)$ άρα,

$$\{\psi_1(k_1), \psi_2(k_1), \ldots, \psi_n(k_1)\} = \{k_1, k_2, \ldots, k_n\}. \tag{39}$$

Έστω μία ρίζα k_i του $p(x)$. Θεωρούμε το σύνολο,

$$A_i = \{\tau \in \mathcal{G}(E/F) : \tau(k_1) = k_i\}.$$

Το $A_i \neq \emptyset$ γιατί, από την ισότητα των συνόλων στην (39), κάποιο $\psi_t(k_1) = k_i$. Έστω $\psi \in A_i$. Για κάθε $\tau \in A_i$, ο $\psi^{-1}\tau \in \mathcal{G}(E/F)$ ως «γινόμενο» στοιχείων της $\mathcal{G}(E/F)$. Επιπλέον, $(\psi^{-1}\tau)(k_1) = \psi^{-1}(\tau(k_1)) = \psi^{-1}(k_i) = k_1$. Από την §143, ο $\psi^{-1}\tau$ είναι ταυτοτικός στο $F(k_1)$. Άρα, ο $\psi^{-1}\tau$ είναι στοιχείο της $\mathcal{G}(E/F(k_1))$. Υπάρχει $\omega \in \mathcal{G}(E/F(k_1))$ ώστε,

$$(\psi^{-1}\tau) = \omega \Rightarrow \tau = \psi\,\omega \in \psi\,\mathcal{G}(E/F(k_1)) \Rightarrow$$
$$A_i \subseteq \psi\,\mathcal{G}(E/F(k_1)),$$

Για κάθε $\omega \in \mathcal{G}(E/F(k_1))$, ο $\psi\,\omega \in \mathcal{G}(E/F)$ ως «γινόμενο» στοιχείων της $\mathcal{G}(E/F)$. Επιπλέον, $(\psi\,\omega)(k_1) = \psi\,(\omega(k_1)) = \psi(k_1) = k_i$. Άρα, ο $\psi\,\omega \in A_i$ και $\psi\,\mathcal{G}(E/F(k_1)) \subseteq A_i$. Τελικά, $A_i = \psi\,\mathcal{G}(E/F(k_1))$ και $|A_i| = |\psi\,\mathcal{G}(E/F(k_1))| = |\mathcal{G}(E/F(k_1))| = (E : F(k_1))$ και το συμπέρασμα προκύπτει.

§147. Έστω $\mathbf{E}, \mathbf{F}$ σώματα με $\mathbf{E} \supseteq \mathbf{F}$, $\mathbf{E}/\mathbf{F}$ κανονική επέκταση του $\mathbf{F}$. Τα ενδιάμεσα σώματα $\mathbf{K_1}$, $\mathbf{K_2}$ των $\mathbf{E}, \mathbf{F}$ είναι συζυγή αν και μόνο αν υπάρχει $\tau \in \mathcal{G}(\mathbf{E}/\mathbf{F})$ ώστε $\tau(\mathbf{K_1}) = \mathbf{K_2}$.

Έστω ότι υπάρχει $\tau \in \mathcal{G}(E/F)$ ώστε $\tau(K_1) = K_2$. Από την §131, η E/F είναι πεπερασμένη επέκταση του F. Επειδή, το K_1 είναι ενδιάμεσο σώμα των E, F, από την §49, $(E : F) = (E : K_1)\,(K_1 : F)$ και η διάσταση $(K_1 : F)$ είναι πεπερασμένη. Από την §75, $K_1 = F(k_1)$ για κάποιο $k_1 \in E$ αλγεβρικό επί του F, με ένα ελάχιστο πολυώνυμο $p(x)$ στο $F[x]$ βαθμού n.

Από την απόδειξη της §124, η εικόνα μίας ρίζας του $p(x)$ μέσω ενός στοιχείου της $\mathcal{G}(E/F)$ είναι εκ' νέου ρίζα του $p(x)$. Άρα, $\tau(k_1) = k_2 \in E$ είναι μία ρίζα του $p(x)$. Από την §66, κάθε στοιχείο του $F(k_1)$ γράφεται ως $\sum_{i=0}^{n-1} f_i\,k_1^i$ με $f_i \in F$. Οπότε,

$$\tau\left(\sum_{i=0}^{n-1} f_i\,k_1^i\right) = \sum_{i=0}^{n-1} \tau(f_i)\,\tau(k_1^i) = \sum_{i=0}^{n-1} f_i\,\tau(k_1)^i = \sum_{i=0}^{n-1} f_i\,k_2^i,$$

Οπότε,

$$K_2 = \tau(K_1) = \left\{\tau\left(\sum_{i=0}^{n-1} f_i\,k_1^i\right) : f_i \in F\right\} = \left\{\sum_{i=0}^{n-1} f_i\,k_2^i : f_i \in F\right\}.$$

Από την §142, το ενδιάμεσο σώμα των E, F, το K_2, έχει διάσταση $(K_2 : F) = (\tau(K_1) : F) = (K_1 : F) = n$. Η K_2/F είναι πεπερασμένη επέκταση του F με διάσταση n. Θα δείξουμε ότι $K_2 = F(k_2)$ δείχνοντας ότι το σύνολο $\mathcal{K} = \{1, k_2, k_2^2, \ldots, k_2^{n-1}\}$ είναι μία βάση του K_2 επί του F.

Από τον ορισμό του K_2, κάθε στοιχείο του K_2 είναι γραμμικός συνδυασμός επί του F των στοιχείων του $\mathcal{K}$. Αρκεί να δείξουμε ότι τα στοιχεία του $\mathcal{K}$ είναι

γραμμικώς ανεξάρτητα επί του F. Αν ήταν γραμμικώς εξαρτημένα επί του F, τότε το k_2 θα ήταν ρίζα πολυωνύμου του $F[x]$ βαθμού μικρότερου ή ίσου του $n-1$. Έτσι, ένα ελάχιστο πολυώνυμο του k_2 στο $F[x]$ θα είχε βαθμό μικρότερο του n.

Από την §125 όμως, ένα ελάχιστο πολυώνυμο του k_2 στο $F[x]$ είναι το $p(x)$ που έχει βαθμό n. Από την §65 όλα τα ελάχιστα πολυώνυμα του k_2 στο $F[x]$ είναι της μορφής $a\,p(x)$ με $a \in F - \{0\}$. Ο βαθμός τους είναι n. Το k_2 δεν μπορεί να έχει ελάχιστο πολυώνυμο στο $F[x]$ βαθμού μικρότερου του n. Άρα, τα στοιχεία του $\mathcal{K}$ είναι γραμμικώς ανεξάρτητα επί του F και το $\mathcal{K}$ είναι μία βάση του K_2 επί του F. Τα K_2, $F(k_2)$ έχουν ίδια βάση επί του F οπότε, είναι ίσα. Τα $K_1 = F(k_1)$, $K_2 = F(k_2)$ είναι συζυγή γιατί είναι ενδιάμεσα σώματα των E, F και από την §125, τα k_1, k_2 είναι στοιχεία του E αλγεβρικά επί του F και έχουν ένα ίδιο ελάχιστο πολυώνυμο στο $F[x]$.

Έστω τώρα ότι τα K_1, K_2 είναι συζυγή. Τότε, $K_1 = F(k_1)$, $K_2 = F(k_2)$, με k_1, k_2 στοιχεία του E αλγεβρικά επί του F τα οποία έχουν ένα ίδιο ελάχιστο πολυώνυμο στο $F[x]$ έστω βαθμού n. Από την §146, υπάρχει $\tau \in \mathcal{G}(E/F)$ ώστε $\tau(k_1) = k_2$. Οπότε,

$$\tau(K_1) = \left\{ \tau\left(\sum_{i=0}^{n-1} f_i\, k_1^i \right) :\ f_i \in F \right\} = \left\{ \sum_{i=0}^{n-1} f_i\, k_2^i :\ f_i \in F \right\} = F(k_2) = K_2.$$

Το συμπέρασμα απεδείχθη.

§148. Έστω G ομάδα. Η H είναι κανονική υποομάδα της G αν και μόνο αν η H ισούται με όλες τις συζυγής ομάδες της.

Έστω ότι η H είναι κανονική υποομάδα της G. Όλες οι συζυγής ομάδες της H είναι οι $g^{-1}\,H\,g$ για κάθε $g \in G$. Για κάθε $h \in H$ και κάθε $g \in G$, το $g^{-1}\,h\,g \in H$ γιατί η H είναι κανονική. Άρα, $g^{-1}\,H\,g \subseteq H$ για κάθε $g \in G$. Η H περιέχει όλες τις συζυγής ομάδες της.

Από την άλλη, για κάθε $h \in H$ και κάθε $g \in G$, $h = g\,(g^{-1}\,h\,g)\,g^{-1} = g\,h_g\,g^{-1}$ με $h_g \in H$ γιατί η H είναι κανονική. Άρα, για κάθε $g \in G$, η H περιέχεται στην $g\,H\,g^{-1}$. Όμως, για κάθε $g \in G$, $g\,H\,g^{-1} = (g^{-1})^{-1}\,H\,g^{-1} = b^{-1}\,H\,b$ για κάθε $b \in G$. Η H περιέχεται σε όλες τις συζυγής ομάδες της. Από τα προηγούμενα προκύπτει ότι η H ισούται με όλες τις συζυγής ομάδες της.

Έστω ότι η H ισούται με όλες τις συζυγής ομάδες της. Τότε $H = g^{-1}\,H\,g$ για κάθε $g \in G$. Άρα, για κάθε $h \in H$ και κάθε $g \in G$, το $g^{-1}\,h\,g \in g^{-1}\,H\,g = H$ και η H είναι κανονική.

§149. Έστω E, F σώματα με E ⊇ F, E/F κανονική επέκταση του F. Τα ενδιάμεσα σώματα K₁, K₂ των E, F είναι συζυγή αν και μόνο αν οι $\mathcal{G}(E/K_1)$, $\mathcal{G}(E/K_2)$ είναι συζυγής ομάδες. Ένα ενδιάμεσο σώμα K των E, F επάγει μία κανονική επέκταση K/F του F αν και μόνο αν η $\mathcal{G}(E/K)$ είναι κανονική υποομάδα της $\mathcal{G}(E/F)$.

Έστω ότι τα K_1, K_2 είναι συζυγή. Από την §147, υπάρχει $\tau \in \mathcal{G}(E/F)$ ώστε $\tau(K_1) = K_2$. Έστω $\psi \in \mathcal{G}(E/K_1)$. Για κάθε $k \in K_2$, $\tau^{-1}(k) \in K_1$ και $\psi(\tau^{-1}(k)) = \tau^{-1}(k)$ γιατί ο ψ είναι ταυτοτικός στο K_1. Οπότε,

$$(\tau\,\psi\,\tau^{-1})(k) = \tau(\psi(\tau^{-1}(k))) = \tau(\tau^{-1}(k)) = (\tau\,\tau^{-1})(k) = k.$$

Το «γινόμενο» $\tau\,\psi\,\tau^{-1}$ αυτομορφισμών του E είναι αυτομορφισμός του E και ταυτοτικός στο K_2. Άρα, $\tau\,\psi\,\tau^{-1} \in \mathcal{G}(E/K_2)$ και $\psi = \tau^{-1}\,(\tau\,\psi\,\tau^{-1})\,\tau$ που σημαίνει ότι, κάθε στοιχείο της $\mathcal{G}(E/K_1)$ είναι και στοιχείο της $\tau^{-1}\,\mathcal{G}(E/K_2)\,\tau$ δηλαδή, $\mathcal{G}(E/K_1) \subseteq \tau^{-1}\,\mathcal{G}(E/K_2)\,\tau$.

Έστω $\chi \in \mathcal{G}(E/K_2)$. Για κάθε $b \in K_1$, $\tau(b) \in K_2$ και $\chi(\tau(b)) = \tau(b)$ γιατί ο χ είναι ταυτοτικός στο K_2. Οπότε,

$$(\tau^{-1}\,\chi\,\tau)(b) = \tau^{-1}(\chi(\tau(b))) = \tau^{-1}(\tau(b)) = (\tau^{-1}\,\tau)(b) = b.$$

Το «γινόμενο» $\tau^{-1}\,\chi\,\tau$ αυτομορφισμών του E είναι αυτομορφισμός του E και ταυτοτικός στο K_1. Άρα, $\tau^{-1}\,\chi\,\tau \in \mathcal{G}(E/K_1)$ και $\chi = \tau\,(\tau^{-1}\,\chi\,\tau)\,\tau^{-1}$ που σημαίνει ότι, κάθε στοιχείο της $\mathcal{G}(E/K_2)$ είναι και στοιχείο της $\tau\,\mathcal{G}(E/K_1)\,\tau^{-1}$ δηλαδή, $\mathcal{G}(E/K_2) \subseteq \tau\,\mathcal{G}(E/K_1)\,\tau^{-1}$ ή $\tau^{-1}\,\mathcal{G}(E/K_2)\,\tau \subseteq \mathcal{G}(E/K_1)$. Τελικά, $\mathcal{G}(E/K_1) = \tau^{-1}\,\mathcal{G}(E/K_2)\,\tau$ και οι $\mathcal{G}(E/K_1)$, $\mathcal{G}(E/K_2)$ είναι συζυγής.

Έστω τώρα ότι οι $\mathcal{G}(E/K_1)$, $\mathcal{G}(E/K_2)$ είναι συζυγής. Τότε υπάρχει $\tau \in \mathcal{G}(E/F)$ ώστε $\mathcal{G}(E/K_1) = \tau^{-1}\,\mathcal{G}(E/K_2)\,\tau$. Επειδή η επέκταση E/F του F είναι κανονική, από την §140, η επέκταση E/K_2 του K_2 είναι επίσης κανονική και το σταθερό σώμα της $\mathcal{G}(E/K_2)$ είναι το K_2. Έστω $b \in K_1$ ώστε το $\tau(b) \notin K_2$. Αυτό σημαίνει ότι, το $\tau(b)$ δεν είναι στοιχείο του σταθερού σώματος K_2 της $\mathcal{G}(E/K_2)$.

Επειδή, το K_2 ως σταθερό σώμα της $\mathcal{G}(E/K_2)$ ισούται με,

$$\{k \in E :\, \chi(k) = k,\, \forall\, \chi \in \mathcal{G}(E/K_2)\},$$

υπάρχει $\chi \in \mathcal{G}(E/K_2)$ ώστε,

$$\tau(b) \neq \chi(\tau(b)) \Rightarrow b \neq \tau^{-1}(\chi(\tau(b))) = (\tau^{-1}\,\chi\,\tau)(b).$$

Όμως, από την υπόθεση $\mathcal{G}(E/K_1) = \tau^{-1}\,\mathcal{G}(E/K_2)\,\tau$, το $\tau^{-1}\,\chi\,\tau \in \mathcal{G}(E/K_1)$ που σημαίνει ότι, το «γινόμενο» $\tau^{-1}\,\chi\,\tau$ είναι ταυτοτικός αυτομορφισμός στο K_1 και άρα, $b = (\tau^{-1}\,\chi\,\tau)(b)$ αντιβαίνοντας το προηγούμενο συμπέρασμα $b \neq (\tau^{-1}\,\chi\,\tau)(b)$. Κακώς λοιπόν υποθέσαμε ότι υπάρχει $b \in K_1$ ώστε το $\tau(b) \notin K_2$. Τελικά, $\tau(b) \in K_2$ για κάθε $b \in K_1$ και $\tau(K_1) \subseteq K_2$.

Επειδή η επέκταση E/F του F είναι κανονική, από την §140, η επέκταση E/K_1 του K_1 είναι επίσης κανονική και το σταθερό σώμα της $\mathcal{G}(E/K_1)$ είναι το K_1. Έστω $k \in K_2$ ώστε το $\tau^{-1}(k) \notin K_1$. Αυτό σημαίνει ότι, το $\tau^{-1}(k)$ δεν είναι στοιχείο του σταθερού σώματος K_1 της $\mathcal{G}(E/K_1)$.

Επειδή, το K_1 ως σταθερό σώμα της $\mathcal{G}(E/K_1)$ ισούται με,

$$\{b \in E :\, \psi(b) = b,\, \forall\, \psi \in \mathcal{G}(E/K_1)\},$$

υπάρχει $\psi \in \mathcal{G}(E/K_1)$ ώστε,

$$\tau^{-1}(k) \neq \psi(\tau^{-1}(k)) \Rightarrow k \neq \tau(\psi(\tau^{-1}(k))) = (\tau\,\psi\,\tau^{-1})(k).$$

Όμως, από την υπόθεση $\mathcal{G}(E/K_1) = \tau^{-1}\,\mathcal{G}(E/K_2)\,\tau$, το $\tau\,\psi\,\tau^{-1} \in \mathcal{G}(E/K_2)$ που σημαίνει ότι, το «γινόμενο» $\tau\,\psi\,\tau^{-1}$ είναι ταυτοτικός αυτομορφισμός στο K_2 και άρα, $k = (\tau\,\psi\,\tau^{-1})(k)$ αντιβαίνοντας το προηγούμενο συμπέρασμα $k \neq (\tau\,\psi\,\tau^{-1})(k)$. Κακώς λοιπόν υποθέσαμε ότι υπάρχει $k \in K_2$ ώστε το $\tau^{-1}(k) \notin K_1$. Τελικά, $\tau^{-1}(k) \in K_1$ για κάθε $k \in K_2$ και $\tau^{-1}(K_2) \subseteq K_1$ δηλαδή, $K_2 \subseteq$

$\tau(K_1)$. Έχουμε ήδη αποδείξει και ότι $\tau(K_1) \subseteq K_2$ και άρα, $\tau(K_1) = K_2$.

Έστω τώρα K/F μία κανονική επέκταση του F. Κάθε ανάγωγο πολυώνυμο στο $F[x]$ που έχει μία ρίζα στο K έχει όλες τις ρίζες του στο K. Αν υπάρχει ενδιάμεσο σώμα T των E, F που να είναι συζυγές με το K, τότε υπάρχουν k_1, k_2 στοιχεία του E αλγεβρικά επί του F ώστε $K = F(k_1)$, $T = F(k_2)$ και τα k_1, k_2 έχουν ένα ίδιο ελάχιστο πολυώνυμο $p(x)$ στο $F[x]$.

Από την §65, το $p(x)$ είναι ανάγωγο στο $F[x]$ και μία ρίζα του η k_1 περιέχεται στο K. Από την κανονικότητα της επέκτασης K/F του F, όλες οι ρίζες του $p(x)$, (άρα και η k_2), περιέχονται στο K. Το $K = F(k_1)$ περιέχει το F και το k_2 άρα, περιέχει και το $F(k_2) = T$. Συμπεραίνουμε ότι κάθε ενδιάμεσο σώμα των E, F που είναι συζυγές του K περιέχεται στο K.
Από την §141, στο K αντιστοιχεί η $\mathcal{G}(E/K)$. Όλες οι συζυγής ομάδες της $\mathcal{G}(E/K)$ είναι οι $\omega^{-1}\,\mathcal{G}(E/K)\,\omega$ για κάθε $\omega \in \mathcal{G}(E/F)$ που από την §106 προκύπτει ότι είναι υποομάδες της $\mathcal{G}(E/F)$. Από την §141, σε κάθε $\omega^{-1}\,\mathcal{G}(E/K)\,\omega$ αντιστοιχεί ένα ενδιάμεσο σώμα T_ω των E, F που από το πρώτο μέρος της §149 είναι συζυγές του K. Από το προηγούμενο συμπέρασμα, $T_\omega \subseteq K$. Από την §141 προκύπτει ότι, $\mathcal{G}(E/K) \subseteq \omega^{-1}\,\mathcal{G}(E/K)\,\omega$ για κάθε $\omega \in \mathcal{G}(E/F)$. Δηλαδή, η $\mathcal{G}(E/K)$ περιέχεται σε όλες τις συζυγής της ομάδες.

Έστω ένα στοιχείο $\omega^{-1}\,\psi\,\omega$ κάποιας $\omega^{-1}\,\mathcal{G}(E/K)\,\omega$. Το $\omega^{-1}\,\psi\,\omega$ ανήκει στην $\mathcal{G}(E/F)$ ως «γινόμενο» στοιχείων της $\mathcal{G}(E/F)$. Η K/F ως κανονική είναι και πεπερασμένη επέκταση του F. Από την §75, υπάρχει $k \in K$ αλγεβρικό επί του F, με ένα ελάχιστο πολυώνυμο $g(x)$ στο $F[x]$, ώστε $K = F(k)$. Από την §65, το $g(x)$ είναι ανάγωγο στο $F[x]$ και μία ρίζα του η k ανήκει στο K.

Από την κανονικότητα της επέκτασης K/F του F, όλες οι ρίζες του $g(x)$ ανήκουν στο K. Από την απόδειξη της §124, το $\omega(k)$ είναι κάποια ρίζα k_i του $g(x)$. Η k_i όπως προαναφέραμε ανήκει στο K. Άρα, $\psi(k_i) = k_i$ γιατί ο ψ είναι ταυτοτικός στο K ως στοιχείο της $\mathcal{G}(E/K)$. Το,

$$(\omega^{-1}\,\psi\,\omega)(k) = \omega^{-1}(\psi(\omega(k))) = \omega^{-1}(\psi(k_i)) = \omega^{-1}(k_i) = k.$$

Από την §143, $(\omega^{-1}\,\psi\,\omega)(K) = (\omega^{-1}\,\psi\,\omega)(F(k)) = F(k) = K$. Άρα, ο $\omega^{-1}\,\psi\,\omega$ είναι αυτομορφισμός του E ταυτοτικός στο K και $\omega^{-1}\,\psi\,\omega \in \mathcal{G}(E/K)$. Αποδείξαμε ότι η $\omega^{-1}\,\mathcal{G}(E/K)\,\omega \subseteq \mathcal{G}(E/K)$ για κάθε $\omega \in \mathcal{G}(E/F)$. Δηλαδή, η $\mathcal{G}(E/K)$ περιέχει όλες τις συζυγής της ομάδες. Τελικά, από τα προηγούμενα, η $\mathcal{G}(E/K)$ ισούται με όλες τις συζυγής της ομάδες και από την §148 είναι κανονική.

Για το αντίστροφο του συμπεράσματος, θεωρούμε K ενδιάμεσο σώμα των E, F με $\mathcal{G}(E/K)$ κανονική υποομάδα της $\mathcal{G}(E/F)$. Από την §148, η $\mathcal{G}(E/K)$ ισούται με τις συζυγής της υποομάδες. Από την §141 και το πρώτο μέρος της §149, κάθε ενδιάμεσο σώμα T των E, F που είναι συζυγές με το K αντιστοιχεί σε υποομάδα της $\mathcal{G}(E/F)$ που είναι συζυγής με την $\mathcal{G}(E/K)$.

Έστω T ένα τέτοιο σώμα και H_T η αντίστοιχη ομάδα του από την §141. Η H_T είναι συζυγής με την $\mathcal{G}(E/K)$ και ίση με αυτή. Αν $T \subset K$, τότε από την §141, $\mathcal{G}(E/K) \subset H_T$ άτοπο γιατί από την υπόθεση $\mathcal{G}(E/K) = H_T$. Αν $T \supset K$, τότε από την §141, $\mathcal{G}(E/K) \supset H_T$ άτοπο γιατί από την υπόθεση $\mathcal{G}(E/K) = H_T$. Άρα, $T = K$ και το K ισούται με όλα τα συζυγή σώματά του.

Από την §131, η E/F είναι πεπερασμένη επέκταση του F. Επειδή, το K είναι ενδιάμεσο σώμα των E, F, από την §49, $(E : F) = (E : K)\,(K : F)$ και η διάσταση $(K : F)$ είναι πεπερασμένη. Από την §75, $K = F(k)$ για κάποιο $k \in K$

αλγεβρικό επί του F, με ένα ελάχιστο πολυώνυμο $p(x)$ στο $F[x]$ βαθμού n. Έστω $k_1 = k, k_2, \ldots, k_n$ οι ρίζες του $p(x)$. Τα $F(k_i)$, $i = 1, 2, \ldots, n$ είναι ενδιάμεσα σώματα των E, F και συζυγή γιατί, από την §125, τα k_i, $i = 1, 2, \ldots, n$ έχουν ένα ίδιο ελάχιστο στο $F[x]$ πολυώνυμο, το $p(x)$. Από το προηγούμενο αποτέλεσμα,

$$K = F(k) = F(k_1) = F(k_2) = \cdots = F(k_n),$$

που σημαίνει ότι το $F(k_1)$ περιέχει όλες τις ρίζες του $p(x)$ οπότε,

$$F(k_1) \subseteq F(k_1, k_2, \ldots, k_n) \subseteq F(k_1) \Rightarrow K = F(k_1) = F(k_1, k_2, \ldots, k_n),$$

και το K είναι σώμα διαχωρισμού ενός πολυωνύμου του $F[x]$. Από την §140, η K/F είναι κανονική επέκταση του F.

§150. Έστω $\mathbf{E}, \mathbf{F}$ σώματα με $\mathbf{E} \supseteq \mathbf{F}$, $\mathbf{E}/\mathbf{F}$ κανονική επέκταση του $\mathbf{F}$ με διάσταση $(\mathbf{E} : \mathbf{F}) = \mathbf{p}$ πρώτο αριθμό, ζ μια πρωταρχική p–οστή ρίζα της μονάδας. Τότε, η $\mathbf{E}(\zeta)/\mathbf{F}(\zeta)$ είναι κανονική επέκταση του $\mathbf{F}(\zeta)$, διάστασης $(\mathbf{E}(\zeta) : \mathbf{F}(\zeta)) = \mathbf{p}$.

Επειδή $F \subseteq E \subseteq E(\zeta)$, από την §49 προκύπτει,

$$(E(\zeta) : F) = (E(\zeta) : E)\,(E : F). \tag{40}$$

Επειδή $F \subseteq F(\zeta) \subseteq E(\zeta)$, από την §49 προκύπτει,

$$(E(\zeta) : F) = (E(\zeta) : F(\zeta))\,(F(\zeta) : F). \tag{41}$$

Οπότε, από την υπόθεση και τις (40), (41) παίρνουμε,

$$(E(\zeta) : E)\,p = (E(\zeta) : F(\zeta))\,(F(\zeta) : F). \tag{42}$$

Η ζ είναι αλγεβρική επί του F ως ρίζα του $f(x) = x^p - 1 \in F[x]$. Από την §66, η $F(\zeta)/F$ είναι πεπερασμένη επέκταση του F. Επίσης, η ζ είναι αλγεβρική επί του E αφού $f(x) \in F[x] \subseteq E[x]$. Από την §66, η $E(\zeta)/E$ είναι πεπερασμένη επέκταση του E. Από την (42) η διάσταση της $E(\zeta)/F(\zeta)$ είναι πεπερασμένη γιατί αν ήταν άπειρη τότε και η διάσταση της $E(\zeta)/E$ θα ήταν άπειρη, άτοπο.

Από την §104, η ζ ως πρωταρχική p–οστή ρίζα της μονάδας είναι διάφορη της μονάδας αφού παράγει μία κυκλική ομάδα, την $\mathcal{Z}$, τάξης p. Οπότε, $0 = f(\zeta) = \zeta^p - 1 = (\zeta - 1)\sum_{i=0}^{p-1} \zeta^i$ επάγει ότι η ζ είναι ρίζα του $\sum_{i=0}^{p-1} x^i \in F[x]$ και άρα, ο βαθμός κάθε ελαχίστου πολυωνύμου της ζ στο $F[x]$ είναι μικρότερος ή ίσος με $p - 1$. Δηλαδή, $(F(\zeta) : F) \leq p - 1$. Από την (42), ο p διαιρεί το γινόμενο $(E(\zeta) : F(\zeta))\,(F(\zeta) : F)$. Δεν μπορεί να διαιρεί την διάσταση $(F(\zeta) : F) \leq p-1$. Άρα ο p διαιρεί την διάσταση $(E(\zeta) : F(\zeta))$ και $(E(\zeta) : F(\zeta)) \geq p$.

Έστω $e(x) \in E[x]$, $g(x) \in F[x]$ ελαχίστου βαθμού πολυώνυμα της ζ στα $E[x]$, $F[x]$ αντιστοίχως. Επειδή, $F[x] \subseteq E[x]$ το $g(x)$ είναι και πολυώνυμο του $E[x]$ με ρίζα την ζ. Όμως, $deg[e(x)]$ είναι ο μικρότερος βαθμός ανάμεσα στους βαθμούς των πολυωνύμων του $E[x]$ που έχουν την ζ ως ρίζα. Οπότε, $deg[e(x)] \leq deg[g(x)]$. Από την §66, $(E(\zeta) : E) = deg[e(x)] \leq deg[g(x)] = (F(\zeta) : F)$.

Από την (42) παίρνουμε,

$$\begin{aligned} (E(\zeta) : E)\,p &= (E(\zeta) : F(\zeta))\,(F(\zeta) : F) \Rightarrow \\ (F(\zeta) : F)\,p &\geq (E(\zeta) : F(\zeta))\,(F(\zeta) : F) \Rightarrow \\ p &\geq (E(\zeta) : F(\zeta)). \end{aligned}$$

Από τα προηγούμενα, $(E(\zeta) : F(\zeta)) = p$.

Η E/F ως κανονική επέκταση του F είναι και πεπερασμένη επέκταση του F. Από την §75, υπάρχει $e \in E$ αλγεβρικό επί του F ώστε $E = F(e)$. Έστω $a(x) \in F[x]$ ένα ελάχιστο πολυώνυμο του e στο $F[x]$ με ρίζες $e_1 = e, e_2, \ldots, e_n$. Από την §65, το $a(x)$ είναι ανάγωγο στο $F[x]$ και μία ρίζα του η $e_1 = e$ ανήκει στο E. Από την κανονικότητα της επέκτασης E/F, όλες οι ρίζες e_i, $i = 1, 2, \ldots, n$ ανήκουν στο E.

Το $E(\zeta)$ περιέχει μία πρωταρχική p–οστή ρίζα της μονάδας. Και επειδή από την §104 όλες οι p–οστές ρίζες της μονάδας είναι της μορφής ζ^j, $j = 0, 1, \ldots, p-1$, όλες οι p–οστές ρίζες της μονάδας ανήκουν στο $E(\zeta)$. Οπότε,

$$E(\zeta) = (F(e_1))(\zeta) = F(e_1, \zeta) \supseteq F(e_1, e_2, \ldots, e_n, \zeta).$$

Από την άλλη, $F(e_1, \zeta) \subseteq F(e_1, e_2, \ldots, e_n, \zeta)$. Άρα, $E(\zeta) = F(e_1, e_2, \ldots, e_n, \zeta)$ είναι το σώμα διαχωρισμού στην επέκταση $E(\zeta)/F(\zeta)$ του πολυωνύμου $h(x) = (x^p - 1)\, a(x) \in (F(\zeta))[x]$. Από την §140, η $E(\zeta)/F(\zeta)$ είναι κανονική επέκταση του του $F(\zeta)$.

§151. Έστω F σώμα, $\mathbf{x_1, x_2, \ldots, x_n} \in \mathbf{F}$. Η ορίζουσα Vandermonde είναι η,

$$\mathbf{V_n} = \begin{vmatrix} \mathbf{1} & \mathbf{x_1} & \mathbf{x_1^2} & \cdots & \mathbf{x_1^{n-1}} \\ \mathbf{1} & \mathbf{x_2} & \mathbf{x_2^2} & \cdots & \mathbf{x_2^{n-1}} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \mathbf{1} & \mathbf{x_n} & \mathbf{x_n^2} & \cdots & \mathbf{x_n^{n-1}} \end{vmatrix} = \prod_{\mathbf{1 \le i < j \le n}} (\mathbf{x_j - x_i}).$$

Από τις ιδιότητες των οριζουσών,

$$V_n = \begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix} =$$

$$= \begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix} \begin{vmatrix} 1 & -x_1 & 0 & \cdots & 0 \\ 0 & 1 & -x_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & -x_1 \\ 0 & 0 & 0 & \cdots & 1 \end{vmatrix} =$$

$$= \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & (x_2 - x_1) & x_2\,(x_2 - x_1) & \cdots & x_2^{n-2}\,(x_2 - x_1) \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & (x_n - x_1) & x_n\,(x_n - x_1) & \cdots & x_n^{n-2}\,(x_n - x_1) \end{vmatrix} =$$

$$= (x_2 - x_1)\,(x_3 - x_1) \cdots (x_n - x_1) \begin{vmatrix} 1 & x_2 & x_2^2 & \cdots & x_2^{n-2} \\ 1 & x_3 & x_3^2 & \cdots & x_3^{n-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-2} \end{vmatrix} =$$

$$= \prod_{2\le j\le n}(x_j - x_1)\begin{vmatrix} 1 & y_1 & y_1^2 & \cdots & y_1^{n-2} \\ 1 & y_2 & y_2^2 & \cdots & y_2^{n-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & y_{n-1} & y_{n-1}^2 & \cdots & y_{n-1}^{n-2} \end{vmatrix} = \quad (\text{επαγωγικώς})$$

$$= \prod_{2\le j\le n}(x_j - x_1)\prod_{1\le i<j\le n-1}(y_j - y_i) =$$

$$= \prod_{2\le j\le n}(x_j - x_1)\prod_{2\le i<j\le n}(x_j - x_i) = \prod_{1\le i<j\le n}(x_j - x_i).$$

§152. Έστω $\mathbf{E}, \mathbf{F}$ σώματα, $\mathbf{E} \supseteq \mathbf{F}$, $\mathbf{E/F}$ κανονική επέκταση του $\mathbf{F}$ με διάσταση $(\mathbf{E} : \mathbf{F}) = \mathbf{p}$ πρώτο αριθμό, το $\mathbf{F}$ περιέχει τις $\mathbf{p}$–οστές ρίζες της μονάδας. Τότε, υπάρχουν στοιχεία $\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_{p-1}} \in \mathbf{E}$ ώστε $\mathbf{a_i^p} \in \mathbf{F}$ και $\mathbf{E} = \mathbf{F}(\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_{p-1}})$.

Η E/F ως κανονική επέκταση του F είναι και πεπερασμένη. Από την §75 υπάρχει $e \in E$ αλγεβρικό επί του F ώστε $E = F(e)$. Από την υπόθεση, η διάσταση $(E : F) = (F(e) : F) = p$ πρώτος αριθμός. Από τις §65, §66, ο βαθμός κάθε ελαχίστου πολυωνύμου του e στο $F[x]$ είναι p. Έστω $e_1 = e, e_2, \ldots, e_p$ οι ρίζες ενός ελαχίστου πολυωνύμου $q(x)$ του e στο $F[x]$. Από την §65 το $q(x)$ είναι ανάγωγο στο $F[x]$. Από την κανονικότητα της E/F όλες οι ρίζες του $q(x)$ ανήκουν στο E. Από την κανονικότητα της E/F επίσης, $|\mathcal{G}(E/F)| = (E : F) = p$. Από την §105, η $\mathcal{G}(E/F)$ είναι κυκλική ομάδα και επειδή ο p ως πρώτος είναι μεγαλύτερος ή ίσος του 2, υπάρχει $\tau \in \mathcal{G}(E/F) - \{id\}$ ώστε $\mathcal{G}(E/F) = \langle\tau\rangle$.

Από την απόδειξη της §124 οι εικόνες των ριζών του $q(x)$ μέσω των στοιχείων της $\mathcal{G}(E/F)$ είναι εκ΄ νέου ρίζες του $q(x)$. Οπότε, οι $\tau^i(e_1)$, $i = 1, 2, \ldots, p$ είναι ρίζες του $q(x)$ γιατί,

$$\tau^i(e_1) = \underbrace{\tau(\tau(\cdots\tau(\tau}_{i-\text{το πλήθος}}(e_1)))).$$

Θέτουμε $k_i = \tau^i(e_1)$, $i = 1, 2, \ldots, p$. Οι τ^i, $i = 1, 2, \ldots, p$ είναι τα p το πλήθος διακεκριμένα στοιχεία της $\mathcal{G}(E/F)$. Αν $k_i = k_j$ για $1 \le i < j \le p$, τότε $\tau^i(e_1) = \tau^j(e_1)$ ή $(\tau^j\,\tau^{-i})(e_1) = e_1$. Ο $\tau^j\,\tau^{-i} \in \mathcal{G}(E/F)$ ως «γινόμενο» στοιχείων της $\mathcal{G}(E/F)$. Από την §143 ο $\tau^j\,\tau^{-i} = id$ ή $\tau^j = \tau^i$, άτοπο γιατί τα τ^ℓ για $\ell = 1, 2, \ldots, p$ είναι διακεκριμένα.

Οι k_i είναι οι p το πλήθος διακεκριμένες ρίζες του $q(x)$ δηλαδή, $\{k_1, k_2, \ldots, k_p\} = \{e_1, e_2, \ldots, e_p\} \subseteq E$. Έστω ζ μία πρωταρχική p–οστή ρίζα της μονάδας. Από την §104, οι p–οστές ρίζες της μονάδας είναι οι $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$ και από την υπόθεση όλες ανήκουν στο F. Θέτουμε,

$$a_j = \sum_{i=1}^{p} \zeta^{(i-1)\,j}\,k_i,\ j = 0, 1, \ldots, p-1. \tag{43}$$

Το $h(x_1, \ldots, x_p) = \sum_{i=1}^p x_i \in F[x_1, \ldots, x_p]$ είναι συμμετρικό. Από την §133, το $a_0 = \sum_{i=1}^p k_i = h(k_1, \ldots, k_p) \in F$. Για τον γεννήτορα $\tau \in \mathcal{G}(E/F)$,

$$\tau(a_j^p) = [\tau(a_j)]^p = \left[\tau\left(\sum_{i=1}^{p}\zeta^{(i-1)\,j}\,k_i\right)\right]^p = \left[\sum_{i=1}^{p}[\tau(\zeta)]^{(i-1)\,j}\,\tau(k_i)\right]^p =$$

$$= \left[\sum_{i=1}^{p}\zeta^{(i-1)\,j}\,\tau(\tau^i(e_1))\right]^p = \left[\sum_{i=1}^{p}\zeta^{(i-1)\,j}\,\tau^{i+1}(e_1)\right]^p =$$

$$= \left[\sum_{i=1}^{p} \zeta^{(i-1)\,j}\, k_{i+1}\right]^p = \left[\zeta^{(p-1)\,j}\, k_{p+1} + \sum_{i=1}^{p-1} \zeta^{(i-1)\,j}\, k_{i+1}\right]^p =$$

$$= \left[\zeta^{(p-1)\,j}\, k_1 + \sum_{i=1}^{p-1} \zeta^{(i-1)\,j}\, k_{i+1}\right]^p,$$

γιατί, $k_{p+1} = \tau^{p+1}(e_1) = \tau(\tau^p(e_1)) = \tau(e_1) = k_1$ εφ' όσον, $\tau^p = id$ από την δομή της $\mathcal{G}(E/F) = \langle\tau\rangle$. Άρα,

$$\tau(a_j^p) = \left[\zeta^{-j}\left(\zeta^{p\,j}\, k_1 + \sum_{i=1}^{p-1} \zeta^{i\,j}\, k_{i+1}\right)\right]^p \overset{\zeta^p=1}{=}$$

$$= \left[\zeta^{-j}\left(k_1 + \sum_{\ell=2}^{p} \zeta^{(\ell-1)\,j}\, k_\ell\right)\right]^p =$$

$$= \left[\zeta^{-j}\left(\sum_{i=1}^{p} \zeta^{(i-1)\,j}\, k_i\right)\right]^p = \left[\zeta^{-j}\, a_j\right]^p \overset{\zeta^p=1}{=} a_j^p.$$

$$\tau^i(a_j^p) = \underbrace{\tau(\tau(\cdots\tau(\tau}_{i-\text{το πλήθος}}(a_j^p)))) = a_j^p,\ i = 1, 2, \ldots, p.$$

Οπότε, η εικόνα των a_j^p, $j = 1, 2, \ldots, p-1$ μέσω των στοιχείων της $\mathcal{G}(E/F)$ μένει αμετάβλητη επάγοντας ότι τα a_j^p, $j = 1, 2, \ldots, p-1$ ανήκουν στο σταθερό σώμα της $\mathcal{G}(E/F)$ που από την κανονικότητα της E/F και την §140 είναι το F. Επίσης, έχοντας δείξει πιο πάνω ότι $a_0 \in F$ έπεται ότι και $a_0^p \in F$. Η (43) ξαναγράφεται ως,

$$\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_j \\ \vdots \\ a_{p-1} \end{bmatrix} = \begin{bmatrix} 1 & (\zeta^0)^1 & (\zeta^0)^2 & \cdots & (\zeta^0)^{p-1} \\ 1 & (\zeta^1)^1 & (\zeta^1)^2 & \cdots & (\zeta^1)^{p-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & (\zeta^j)^1 & (\zeta^j)^2 & \cdots & (\zeta^j)^{p-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & (\zeta^{p-1})^1 & (\zeta^{p-1})^2 & \cdots & (\zeta^{p-1})^{p-1} \end{bmatrix} \begin{bmatrix} k_1 \\ k_2 \\ \vdots \\ k_j \\ \vdots \\ k_p \end{bmatrix} \Rightarrow A = J\,K.$$

Όμως η ορίζουσα του J είναι τύπου Vandermonde και από την §151, $|J| = \prod_{0\le i<j\le p-1}(\zeta^j - \zeta^i) \neq 0$. Άρα, $K = J^{-1}\,A$.

Θεωρούμε το σώμα $F(a_0, a_1, \ldots, a_{p-1})$. Από τα προηγούμενα, κάθε k_i, $i = 1, 2, \ldots, p$ είναι έκφραση στοιχείων του $F(a_0, a_1, \ldots, a_{p-1})$ μέσω των πράξεών του. Άρα, το $k_p = \tau^p(e_1) = e_1$ ανήκει στο $F(a_0, a_1, \ldots, a_{p-1})$ και $E = F(e_1) \subseteq F(a_0, a_1, \ldots, a_{p-1})$. Από την άλλη, πιο πάνω έχουμε δείξει ότι τα ζ και k_i, $i = 1, 2, \ldots, p$ ανήκουν στο E. Από την (43) και τα a_i, $i = 1, 2, \ldots, p$ ανήκουν στο E και $F(a_0, a_1, \ldots, a_{p-1}) \subseteq F(e_1) = E$. Το συμπέρασμα προκύπτει επειδή $F(a_1, \ldots, a_{p-1}) = F(a_0, a_1, \ldots, a_{p-1})$ εφ' όσον $a_0 \in F$.

§153. Έστω $\mathbf{L, E, F}$ σώματα, $\mathbf{L \supseteq F}$, $\mathbf{f(x) \in F[x]}$, $\mathbf{E}$ το σώμα διαχωρισμού του $\mathbf{f(x)}$ στην $\mathbf{L/F}$, η $\mathcal{G}(\mathbf{E/F})$ είναι επιλύσιμη. Τότε, υπάρχει σειρά σωμάτων $\mathbf{F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n = E}$ ώστε

για $\mathbf{j = 0, 1, \ldots, n-1}$ η $\mathbf{K_{j+1}/K_j}$ είναι κανονική επέκταση του $\mathbf{K_j}$ με διάσταση $\mathbf{(K_{j+1} : K_j) = p_j}$ πρώτο αριθμό.

Από την επιλυσιμότητα της $\mathcal{G}(E/F)$ και την §107, υπάρχει κανονική σειρά υποομάδων της $\mathcal{G}(E/F)$,

$$\{id\} = G_n \subseteq G_{n-1} \subseteq \cdots \subseteq G_1 \subseteq G_0 = \mathcal{G}(E/F),$$

ώστε για $j = 0, 1, \ldots, n-1$ η G_{j+1} είναι κανονική υποομάδα της G_j με δείκτη $[G_j : G_{j+1}] = p_j$ πρώτο αριθμό. Από την §140, η E/F είναι κανονική επέκταση του F εφ' όσον από την υπόθεση, το E είναι σώμα διαχωρισμού κάποιου πολυωνύμου του $F[x]$. Από την §141, σε κάθε G_j, $j = 0, 1, \ldots, n$ αντιστοιχεί ενδιάμεσο σώμα K_j των E, F ώστε το K_j να είναι το σταθερό σώμα της G_j και $G_j = \mathcal{G}(E/K_j)$. Επίσης, από την §141 προκύπτει ότι για $G_{j+1} \subseteq G_j$ έπεται $K_j \subseteq K_{j+1}$. Οπότε, υπάρχει σειρά σωμάτων,

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n = E.$$

Από την §140, η E/K_j είναι κανονική επέκταση του K_j και $(E : K_j) = |\mathcal{G}(E/K_j)|$. Επειδή η G_{j+1} είναι κανονική υποομάδα της G_j από την §149, η K_{j+1}/K_j είναι κανονική επέκταση του K_j. Επίσης,

$$\begin{aligned}(E : K_j) &= (E : K_{j+1})\,(K_{j+1} : K_j) \Rightarrow (K_{j+1} : K_j) = \frac{(E : K_j)}{(E : K_{j+1})} = \\ &= \frac{|\mathcal{G}(E/K_j)|}{|\mathcal{G}(E/K_{j+1})|} = \frac{|G_j|}{|G_{j+1}|} = [G_j : G_{j+1}] = p_j,\end{aligned}$$

και το συμπέρασμα προκύπτει.

§154. Έστω $\mathbf{L, E, F}$ σώματα, $\mathbf{L \supseteq F}$, $\mathbf{f(x) \in F[x]}$, $\mathbf{E}$ το σώμα διαχωρισμού του $\mathbf{f(x)}$ στην $\mathbf{L/F}$. Αν η $\mathcal{G}(\mathbf{E/F})$ είναι επιλύσιμη, τότε η πολυωνυμική εξίσωση $\mathbf{f(x) = 0}$ είναι επιλύσιμη δια ριζικών.

Έστω ότι η $\mathcal{G}(E/F)$ είναι επιλύσιμη. Από την §153, υπάρχει σειρά σωμάτων,

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n = E \tag{44}$$

ώστε για $j = 0, 1, \ldots, n-1$ η K_{j+1}/K_j είναι κανονική επέκταση του K_j με διάσταση $(K_{j+1} : K_j) = p_j$ πρώτο αριθμό. Έστω ζ_j μία πρωταρχική p_j–οστή ρίζα της μονάδας. Από την §150, η $K_{j+1}(\zeta_j)/K_j(\zeta_j)$ είναι κανονική επέκταση του $K_j(\zeta_j)$ με διάσταση $(K_{j+1}(\zeta_j) : K_j(\zeta_j)) = p_j$ πρώτο αριθμό. Επειδή η ζ_j είναι πρωταρχική p_j–οστή ρίζα της μονάδας από την §104, το $K_j(\zeta_j)$ περιέχει όλες τις p_j–οστές ρίζες της μονάδας. Από την §152, υπάρχουν $a_{j\ell} \in K_{j+1}(\zeta_j)$, $\ell = 1, 2, \ldots, p_j - 1$ ώστε $a_{j\ell}^{p_j} \in K_j(\zeta_j)$ και,

$$K_{j+1}(\zeta_j) = (K_j(\zeta_j))(a_{j1}, a_{j2}, \ldots, a_{j(p_j-1)}) \overset{\S51}{=} K_j(\zeta_j, a_{j1}, a_{j2}, \ldots, a_{j(p_j-1)}).$$

Οπότε,

$$\begin{aligned}K_j(\zeta_j) &\subseteq K_j(\zeta_j, a_{j1}) \subseteq K_j(\zeta_j, a_{j1}, a_{j2}) \subseteq \cdots \subseteq K_j(\zeta_j, a_{j1}, \ldots, a_{j(p_j-1)}) = \\ &= K_{j+1}(\zeta_j),\end{aligned} \tag{45}$$

με $\zeta_j^{p_j} = 1 \in K_j(\zeta_j)$ και $a_{j\ell}^{p_j} \in K_j(\zeta_j, a_{j1}, \dots a_{j(\ell-1)})$, $\ell = 1, 2, \dots, p_j - 1$ υιοθετώντας τον συμβολισμό $K_j(\zeta_j, a_{j0}) \equiv K_j(\zeta_j)$. Από την (45) η $K_{j+1}(\zeta_j)/K_j(\zeta_j)$ είναι ριζική επέκταση του $K_j(\zeta_j)$ ύψους $p_j - 1$. Συνεχίζοντας με την ίδια λογική,

$$\begin{aligned} K_{j+1}(\zeta_j) &\subseteq K_{j+1}(\zeta_j, \zeta_{j+1}) \subseteq K_{j+1}(\zeta_j, \zeta_{j+1}, a_{(j+1)1}) \subseteq \\ &\subseteq K_{j+1}(\zeta_j, \zeta_{j+1}, a_{(j+1)1}, a_{(j+1)2}) \subseteq \cdots \subseteq \\ &\subseteq K_{j+1}(\zeta_j, \zeta_{j+1}, a_{(j+1)1}, \dots, a_{(j+1)(p_{(j+1)}-1)}) = \\ &= (K_{j+1}(\zeta_{j+1}, a_{(j+1)1}, \dots, a_{(j+1)(p_{(j+1)}-1)}))(\zeta_j) = \\ &= (K_{j+2}(\zeta_{j+1}))(\zeta_j) = K_{j+2}(\zeta_j, \zeta_{j+1}), \end{aligned} \tag{46}$$

με $\zeta_{j+1}^{p_{j+1}} = 1 \in K_{j+1}(\zeta_j)$, και $a_{(j+1)\ell}^{p_{j+1}} \in K_{j+1}(\zeta_j, \zeta_{j+1}, a_{(j+1)1}, \dots a_{(j+1)(\ell-1)})$, $\ell = 1, 2, \dots, p_{j+1} - 1$ υιοθετώντας τον συμβολισμό $K_{j+1}(\zeta_j, \zeta_{j+1}, a_{(j+1)0}) \equiv K_{j+1}(\zeta_j, \zeta_{j+1})$. Από την (46) η $K_{j+2}(\zeta_j, \zeta_{j+1})/K_{j+1}(\zeta_j)$ είναι ριζική επέκταση του $K_{j+1}(\zeta_j)$ ύψους p_{j+1}.

Επιπλέον, η $K_0(\zeta_0)/K_0$ είναι ριζική επέκταση του K_0 ύψους 1 εφ' όσον $\zeta_0^{p_0} = 1 \in K_0$. Από την (44) και τα προηγούμενα επαγωγικά προκύπτει ότι,

- Η $K_0(\zeta_0)/K_0$ είναι ριζική επέκταση του K_0 πεπερασμένου ύψους.
- Η $K_1(\zeta_0)/K_0(\zeta_0)$ είναι ριζική επέκταση του $K_0(\zeta_0)$ πεπερασμένου ύψους.
- Η $K_2(\zeta_0, \zeta_1)/K_1(\zeta_0)$ είναι ριζική επέκταση του $K_1(\zeta_0)$ πεπερασμένου ύψους.

$$\vdots$$

- Η $K_n(\zeta_0, \zeta_1, \dots, \zeta_{n-1})/K_{n-1}(\zeta_0, \zeta_1, \dots, \zeta_{n-2}))$ είναι ριζική επέκταση του $K_{n-1}(\zeta_0, \zeta_1, \dots, \zeta_{n-2})$ πεπερασμένου ύψους.

Άρα, η $K_n(\zeta_0, \zeta_1, \dots, \zeta_{n-1})/K_0$ είναι ριζική επέκταση πεπερασμένου ύψους του $K_0 = F$. Επιπλέον, $E = K_n \subseteq K_n(\zeta_0, \zeta_1, \dots, \zeta_{n-1})$ και το συμπέρασμα προκύπτει.

§155. Έστω $\mathbf{F}$ σώμα, $\mathbf{f} : \mathbb{Q} \mapsto \mathbf{F}_{\mathbb{Q}}$ ο ισομορφισμός της §5. Ορίζουμε την συνάρτηση $\mathbf{g} : \mathbb{Q}[\mathbf{x}] \mapsto \mathbf{F}_{\mathbb{Q}}[\mathbf{x}]$ με $\mathbf{g}\left(\sum_{\mathbf{i=0}}^{\mathbf{n}} \mathbf{q_i}\,\mathbf{x^i}\right) = \sum_{\mathbf{i=0}}^{\mathbf{n}} \mathbf{f(q_i)}\,\mathbf{x^i}$. Τότε, η $\mathbf{g}$ είναι ισομορφισμός δακτυλίων.

Έστω $b(x) = \sum_{i=0}^{n} b_i\, x^i \in F_{\mathbb{Q}}[x]$. Επειδή ο f είναι ισομορφισμός, είναι επί του $F_{\mathbb{Q}}$ και άρα υπάρχουν $q_i \in \mathbb{Q}$ ώστε $f(q_i) = b_i$. Θέτουμε $a(x) = \sum_{i=0}^{n} q_i\, x^i$. Τότε, $g(a(x)) = b(x)$ και η g είναι επί του $F_{\mathbb{Q}}[x]$.

Έστω $a_1(x) = \sum_{i=0}^{n_1} q_{1i}\, x^i \in \mathbb{Q}[x]$, $a_2(x) = \sum_{i=0}^{n_2} q_{2i}\, x^i \in \mathbb{Q}[x]$ ώστε $g(a_1(x)) = g(a_2(x))$. Τότε,

$$\begin{aligned} g(a_1(x)) = g(a_2(x)) &\Rightarrow \sum_{i=0}^{n_1} f(q_{1i})\, x^i = \sum_{i=0}^{n_2} f(q_{2i})\, x^i \Rightarrow \\ &\Rightarrow n_1 = n_2 = n \text{ και } f(q_{1i}) = f(q_{2i}) \Rightarrow \\ &\Rightarrow n_1 = n_2 = n \text{ και } q_{1i} = q_{2i},\ i = 1, 2, \dots, n. \end{aligned}$$

γιατί ο ισομορφισμός f είναι ένα προς ένα. Άρα, $a_1(x) = a_2(x)$ και η g είναι ένα προς ένα. Επίσης,

$$\begin{aligned}
g(a_1(x)+a_2(x)) &= g\left(\sum_{i=0}^{\max\{n_1,n_2\}}(q_{1i}+q_{2i})\,x^i\right)= \\
&= \sum_{i=0}^{\max\{n_1,n_2\}} f(q_{1i}+q_{2i})\,x^i= \\
&= \sum_{i=0}^{\max\{n_1,n_2\}} [f(q_{1i})+f(q_{2i})]\,x^i= \\
&= \sum_{i=0}^{n_1} f(q_{1i})\,x^i+\sum_{i=0}^{n_2} f(q_{2i})\,x^i= \\
&= g(a_1(x))+g(a_2(x)).\\
g(a_1(x)\,a_2(x)) &= g\left(\sum_{i=0}^{n_1+n_2}\left[\sum_{j=0}^{i} q_{1(i-j)}\,q_{2j}\right]x^i\right)= \\
&= \sum_{i=0}^{n_1+n_2} f\left(\sum_{j=0}^{i} q_{1(i-j)}\,q_{2j}\right)x^i= \\
&= \sum_{i=0}^{n_1+n_2}\left(\sum_{j=0}^{i} f(q_{1(i-j)})\,f(q_{2j})\right)x^i= \\
&= \sum_{i=0}^{n_1} f(q_{1i})\,x^i\sum_{i=0}^{n_2} f(q_{2i})\,x^i= \\
&= g(a_1(x))\,g(a_2(x)).
\end{aligned}$$

Η g διατηρεί τις πράξεις του $\mathbb{Q}[x]$. Το συμπέρασμα προκύπτει.

§156. Έστω F σώμα, p πρώτος αριθμός, $\mathbf{F_{\mathbb{Q}}}$ το σώμα της §5. Το $\mathbf{q(x)=\sum_{i=0}^{p-1} x^i}$ είναι ανάγωγο στο $\mathbf{F_{\mathbb{Q}}[x]}$.

Έστω ότι το $q(x)$ δεν είναι ανάγωγο στο $F_{\mathbb{Q}}[x]$. Τότε υπάρχουν $a_1(x)=\sum_{i=0}^{n_1} a_i\,x^i\in F_{\mathbb{Q}}[x]$, $a_2(x)=\sum_{i=0}^{n_2} b_i\,x^i\in F_{\mathbb{Q}}[x]$ με $n_1\geq 1$, $n_2\geq 1$ ώστε $q(x)=a(x)\,b(x)$. Έστω g ο ισομορφισμός της §155. Τότε,

$$\begin{aligned}
g^{-1}(q(x)) &= g^{-1}(a_1(x)\,a_2(x))=g^{-1}(a_1(x))\,g^{-1}(a_2(x))= \\
&= \sum_{i=0}^{n_1} f^{-1}(a_i)\,x^i\sum_{i=0}^{n_2} f^{-1}(b_i)\,x^i\Rightarrow \\
g^{-1}\left(\sum_{i=0}^{p-1} x^i\right) &= \sum_{i=0}^{n_1} f^{-1}(a_i)\,x^i\sum_{i=0}^{n_2} f^{-1}(b_i)\,x^i\Rightarrow \\
\sum_{i=0}^{p-1} f^{-1}(1)\,x^i &= \sum_{i=0}^{n_1} f^{-1}(a_i)\,x^i\sum_{i=0}^{n_2} f^{-1}(b_i)\,x^i\Rightarrow
\end{aligned}$$

$$\sum_{i=0}^{p-1} x^i = \sum_{i=0}^{n_1} f^{-1}(a_i)\, x^i \sum_{i=0}^{n_2} f^{-1}(b_i)\, x^i,$$

που σημαίνει ότι το $\sum_{i=0}^{p-1} x^i$ ως πολυώνυμο του $\mathbb{Q}[x]$ δεν είναι ανάγωγο στο $\mathbb{Q}[x]$, άτοπο από το [**9**] της βιβλιογραφίας. Το συμπέρασμα προκύπτει.

§157. Έστω F σώμα, p πρώτος αριθμός, $\mathbf{F}_{\mathbb{Q}}$ το σώμα της §5, ζ μία πρωταρχική p–οστή ρίζα της μονάδας. Η $\mathcal{G}(\mathbf{F}_{\mathbb{Q}}(\zeta)/\mathbf{F}_{\mathbb{Q}})$ είναι κυκλική ομάδα.

Από την §104, η ζ ως πρωταρχική p–οστή ρίζα της μονάδας παράγει τις υπόλοιπες p–οστές ρίζες της μονάδας άρα, $\zeta \neq 1$. Η ζ ως ρίζα του $x^p - 1 = (x-1)\sum_{i=0}^{p-1} x^i \in F_{\mathbb{Q}}[x]$ είναι τελικά ρίζα του $q(x) = \sum_{i=0}^{p-1} x^i \in F_{\mathbb{Q}}[x]$ που από την §156 είναι ανάγωγο στο $F_{\mathbb{Q}}[x]$.

Έστω $f(x) \in F_{\mathbb{Q}}[x]$ ένα ελάχιστο πολυώνυμο της ζ στο $F_{\mathbb{Q}}[x]$. Από την §65, το $f(x)$ είναι ανάγωγο στο $F_{\mathbb{Q}}[x]$. Από το τελευταίο μέρος της απόδειξης της §139, τα $f(x)$, $q(x)$ διαιρούν το ένα το άλλο στο $F_{\mathbb{Q}}[x]$. Όμως και τα δύο είναι ανάγωγα στο $F_{\mathbb{Q}}[x]$. Οπότε, μπορούν να διαιρούν το ένα το άλλο στο $F_{\mathbb{Q}}[x]$ μόνο αν υπάρχουν $a, b \in F_{\mathbb{Q}} - \{0\}$ ώστε $f(x) = a\, q(x)$ και $q(x) = b\, f(x)$. Από την τελευταία ισότητα και την §65, το $q(x)$ είναι ένα ελάχιστο πολυώνυμο της ζ στο $F_{\mathbb{Q}}[x]$.

Εφ' όσον η ζ παράγει όλες τις p–οστές ρίζες της μονάδας, αυτές είναι της μορφής ζ^k, $k = 0, 1, \ldots, p-1$. Το $F_{\mathbb{Q}}(\zeta)$ περιέχει τις δυνάμεις της ζ άρα περιέχει τις p–οστές ρίζες της μονάδας. Οι p–οστές ρίζες της μονάδας ζ^k, $k = 1, \ldots, p-1$ είναι οι ρίζες του $q(x)$. Το $F_{\mathbb{Q}}(\zeta)$ περιέχει όλες τις ρίζες ενός ελαχίστου πολυωνύμου της ζ. Από την §126, $|\mathcal{G}(F_{\mathbb{Q}}(\zeta)/F_{\mathbb{Q}})| = p - 1$.

Είναι γνωστό αποτέλεσμα της Θεωρίας Αριθμών, ([**4**], Θεώρημα 27, σελίδα 102), ότι για κάθε πρώτο p υπάρχει στοιχείο $g \in \{1, 2, \ldots, p-1\}$ ώστε, $g^{p-1} \equiv 1 \pmod p$ και ο $p-1$ είναι ο μικρότερος θετικός ακέραιος με την ιδιότητα αυτή. Τότε, $\Gamma = \{g \pmod p, g^2 \pmod p, \ldots, g^{p-1} \pmod p\} = \{1, 2, \ldots, p-1\}$ γιατί τα στοιχεία του Γ είναι τα $p-1$ το πλήθος διαφορετικά υπόλοιπα της Ευκλείδειας διαίρεσης με τον p. Πράγματι, αν δύο στοιχεία του Γ, π.χ. τα $g^i \pmod p$ και $g^j \pmod p$ με $1 \leq i < j \leq p-1$ ήταν ίσα, τότε $g^j \equiv g^i \pmod p$ και $g^{j-i} \equiv 1 \pmod p$ με $1 < j - i < p-1$, άτοπο από την ιδιότητα του $p-1$. Δείξαμε λοιπόν ότι τα στοιχεία του Γ είναι διακεκριμένα και $p-1$ το πλήθος. Από τον ορισμό τους είναι υπόλοιπα της Ευκλείδειας διαίρεσης με τον p. Άρα, $\Gamma = \{1, 2, \ldots, p-1\}$.

Από την απόδειξη της §126, κάθε διαφορετικό στοιχείο της $\mathcal{G}(F_{\mathbb{Q}}(\zeta)/F_{\mathbb{Q}})$ απεικονίζει την ζ σε μία διαφορετική ρίζα του $q(x)$ που ανήκει στο $F_{\mathbb{Q}}(\zeta)$. Δηλαδή, στην περίπτωσή μας επειδή όλες οι ρίζες του $q(x)$ ανήκουν στο $F_{\mathbb{Q}}(\zeta)$, κάθε διαφορετικό στοιχείο της $\mathcal{G}(F_{\mathbb{Q}}(\zeta)/F_{\mathbb{Q}})$ απεικονίζει την ζ σε μία διαφορετική ζ^k, $k = 1, 2, \ldots, p-1$. Θέτουμε τ_g το στοιχείο της $\mathcal{G}(F_{\mathbb{Q}}(\zeta)/F_{\mathbb{Q}})$ για το οποίο ισχύει $\tau_g(\zeta) = \zeta^g$. Τότε, για $k = 1, 2, \ldots, p-1$ οι $g^k = p\, h_k + u_k$ με $0 < u_k < p$. Οπότε, $\zeta^{g^k} = (\zeta^p)^{h_k}\, \zeta^{u_k} = \zeta^{u_k} = \zeta^{g^k (\mathrm{mod}\ p)}$ και $\tau_g^k(\zeta) = \zeta^{g^k} = \zeta^{g^k (\mathrm{mod}\ p)}$. Άρα, για $k = 1, 2, \ldots, p-1$ οι τ_g^k είναι στοιχεία της $\mathcal{G}(F_{\mathbb{Q}}(\zeta)/F_{\mathbb{Q}})$ ως «γινόμενα» στοιχείων της $\mathcal{G}(F_{\mathbb{Q}}(\zeta)/F_{\mathbb{Q}})$ που απεικονίζουν την ζ στις διαφορετικές ρίζες του $q(x)$.

Από τα πιο πάνω οι τ_g^k είναι $p-1$ το πλήθος διακεκριμένα στοιχεία της $\mathcal{G}(F_{\mathbb{Q}}(\zeta)/F_{\mathbb{Q}})$. Όπως έχουμε ήδη δείξει η $\mathcal{G}(F_{\mathbb{Q}}(\zeta)/F_{\mathbb{Q}})$ έχει $p-1$ το πλήθος στοιχεία. Τελικά, $\mathcal{G}(F_{\mathbb{Q}}(\zeta)/F_{\mathbb{Q}}) = \{\tau_g, \tau_g^2, \ldots, \tau_g^{p-1}\}$ και το συμπέρασμα προ-

κύπτει.

§158. Έστω F σώμα, G ένα σύνολο αυτομορφισμών του F, (το G δεν περιέχει υποχρεωτικά όλους τους αυτομορφισμούς του F). Αν το G είναι πεπερασμένο και κλειστό ως προς το «γινόμενο», (σύνθεση), των αυτομορφισμών, τότε το G είναι ομάδα.

Έστω ότι το G περιέχει n το πλήθος στοιχεία. Έστω τ ένα στοιχείο του G. Εφ' όσον το G είναι κλειστό ως προς το «γινόμενο» των αυτομορφισμών τα $\tau, \tau^2, \ldots, \tau^n, \tau^{n+1}$ είναι στοιχεία του G. Επειδή το G περιέχει μόνο n στοιχεία θα πρέπει τουλάχιστον δύο εκ' των $\tau, \tau^2, \ldots, \tau^n, \tau^{n+1}$ να είναι ίσα. Έστω ότι $\tau^i = \tau^j$ με $1 \leq i < j \leq n+1$. Οπότε, $\tau^{j-i} = id$. Το τελευταίο συμπέρασμα επάγει ότι ο id ανήκει στο G.

Επιπλέον, αν $j - i = 1$ ο $\tau = id$ και ο αντίστροφός του ανήκει στο G. Αν $j - i > 1$, τότε $\tau^{j-i-1}\,\tau = \tau\,\tau^{j-i-1} = id$ και ο αντίστροφος του τ είναι ο τ^{j-i-1} που ανήκει στο G ως γινόμενο στοιχείων του G.

§159. Έστω $\mathbf{L, E, F}$ σώματα, $\mathbf{L \supseteq E \supseteq F}$, $\mathbf{k \in L}$ αλγεβρικό επί των $\mathbf{E, F}$, $\mathcal{K} = \{\mathbf{k_1 = k, k_2, \ldots, k_n}\}$ το σύνολο των ριζών ενός ελαχίστου πολυωνύμου $\mathbf{q_E(x)}$ του k στο $\mathbf{E[x]}$. Έστω ότι τα στοιχεία του $\mathcal{K}$ ανήκουν στα $\mathbf{E(k), F(k)}$. Συμβολίζουμε με $\tau_\mathbf{r}$ τον περιορισμό του $\tau \in \mathcal{G}(\mathbf{E(k)/E})$ στο $\mathbf{F(k)}$, $\mathbf{P} = \{\tau_\mathbf{r} : \tau \in \mathcal{G}(\mathbf{E(k)/E})\}$. Τότε, το P είναι υποομάδα της $\mathcal{G}(\mathbf{F(k)/F})$.

Από την §126, η $\mathcal{G}(E(k)/E)$ περιέχει n το πλήθος στοιχεία έκαστο των οποίων απεικονίζει την $k_1 = k$ σε διαφορετική ρίζα k_j, $j = 1, 2, \ldots, n$ του $q_E(x)$. Έστω $q_F(x)$ ένα ελάχιστο πολυώνυμο του k στο $F[x]$. Επειδή $F[x] \subseteq E[x]$, το $q_F(x)$ είναι και πολυώνυμο του $E[x]$. Τα $q_F(x)$, $q_E(x)$ είναι πολυώνυμα του $E[x]$ και έχουν κοινή ρίζα την $k_1 = k$. Επιπλέον, από την §65 το $q_E(x)$ είναι ανάγωγο στο $E[x]$. Από το τελευταίο μέρος της απόδειξης της §139, το $q_E(x)$ διαιρεί το $q_F(x)$ στο $E[x]$ και οι ρίζες του $q_E(x)$ είναι και ρίζες του $q_F(x)$. Άρα, οι k_j, $j = 1, 2, \ldots, n$ είναι ρίζες και του $q_F(x)$. Ενδεχομένως, το $q_F(x)$ έχει περισσότερες ρίζες των k_j, $j = 1, 2, \ldots, n$ γιατί διαιρούμενο από το $q_E(x)$ προκύπτει $deg[q_F(x)] \geq deg[q_E(x)]$. Και ενδεχομένως, $m \geq n$ από αυτές τις ρίζες ανήκουν στο $F(k)$. Από την υπόθεση πάντως ξέρουμε ότι τουλάχιστον οι n το πλήθος ρίζες k_j, $j = 1, 2, \ldots, n$, του $q_F(x)$, (δηλαδή, οι ρίζες του $q_E(x)$), ανήκουν στο $F(k)$.

Από την §126, η $\mathcal{G}(F(k)/F)$ περιέχει m το πλήθος στοιχεία έκαστο των οποίων απεικονίζει την $k_1 = k$ σε διαφορετική ρίζα του $q_F(x)$ από αυτές που ανήκουν στο $F(k)$. Από τα προηγούμενα προκύπτει ότι, n το πλήθος στοιχεία της $\mathcal{G}(F(k)/F)$ απεικονίζουν την $k_1 = k$ στις διαφορετικές ρίζες k_j, $j = 1, 2, \ldots, n$ του $q_E(x)$. Έστω $n = d_E = deg[q_E(x)]$, $d_F = deg[q_F(x)]$. Από την §66,

$$F(k) = \left\{ \sum_{t=0}^{d_F - 1} f_t\, k^t \,:\, f_t \in F \right\},$$

$$E(k) = \left\{ \sum_{t=0}^{d_E - 1} e_t\, k^t \,:\, e_t \in E \right\}.$$

Συμβολίζουμε με τ_j το στοιχείο της $\mathcal{G}(E(k)/E)$ ώστε $\tau_j(k_1) = \tau_j(k) = k_j$. Από

τον ορισμό του τ_j,

$$\tau_j\left(\sum_{t=0}^{d_E-1} e_t\,k^t\right)=\sum_{t=0}^{d_E-1} e_t\,k_j^t.$$

Ο περιορισμός $(\tau_j)_r$ του τ_j στο $F(k)$ αναφέρεται στην δράση του τ_j σε εκείνα τα στοιχεία του $E(k)$ που ανήκουν στο $F(k)\subseteq E(k)$. Για τα στοιχεία του $E(k)$ που ανήκουν και στο $F(k)$ ισχύει,

$$\sum_{t=0}^{d_E-1} e_t\,k^t=\sum_{t=0}^{d_F-1} f_t\,k^t.$$

Οπότε, για κάθε στοιχείο $\sum_{t=0}^{d_E-1} e_t\,k^t$ του $E(k)$ που ανήκει στο $F(k)$ έχουμε,

$$\begin{aligned}(\tau_j)_r\left(\sum_{t=0}^{d_E-1} e_t\,k^t\right)&=(\tau_j)_r\left(\sum_{t=0}^{d_F-1} f_t\,k^t\right)\quad=\\ =\sum_{t=0}^{d_F-1} f_t\,[(\tau_j)_r(k)]^t&=\sum_{t=0}^{d_F-1} f_t\,[\tau_j(k)]^t\quad=\\ &=\sum_{t=0}^{d_F-1} f_t\,k_j^t. \qquad (47)\end{aligned}$$

Επειδή όμως $F(k)\subseteq E(k)$, τα στοιχεία του $E(k)$ που ανήκουν και στο $F(k)$ συγκροτούν όλο το $F(k)$. Η (47) επάγει τον κανόνα ορισμού του $(\tau_j)_r$ στα στοιχεία του $F(k)$.

Όπως αναφέραμε πιο πάνω, n το πλήθος στοιχεία της $\mathcal{G}(F(k)/F)$ απεικονίζουν την $k_1=k$ στις διαφορετικές ρίζες k_j, $j=1,2,\ldots,n$ του $q_E(x)$. Έστω $\psi_j\in\mathcal{G}(F(k)/F)$ ώστε $\psi_j(k)=k_j$. Από τον ορισμό του ψ_j,

$$\psi_j\left(\sum_{t=0}^{d_F-1} f_t\,k^t\right)=\sum_{t=0}^{d_F-1} f_t\,k_j^t. \qquad (48)$$

Από τις (47), (48) προκύπτει ότι οι $(\tau_j)_r$, ψ_j είναι ίσες συναρτήσεις στο $F(k)$. Άρα, $(\tau_j)_r=\psi_j\in\mathcal{G}(F(k)/F)$ και ως συνέπεια $P\subseteq\mathcal{G}(F(k)/F)$. Ισχύει και το αντίστροφο δηλαδή, αν $\psi_j\in\mathcal{G}(F(k)/F)$ με $\psi_j(k)=k_j$, $j=1,2,\ldots,n$, τότε ο ψ_j επεκτείνεται σε στοιχείο $\tau_j\in\mathcal{G}(E(k)/E)$ με $\tau_j(k)=k_j$ και $(\tau_j)_r=\psi_j$. Πράγματι, αν ορίσουμε,

$$\tau_j\left(\sum_{t=0}^{d_E-1} e_t\,k^t\right)=\sum_{t=0}^{d_E-1} e_t\,k_j^t.$$

ο $\tau_j\in\mathcal{G}(E(k)/E)$ και ο $(\tau_j)_r=\psi_j$. Η απόδειξη ότι ο $\tau_j\in\mathcal{G}(E(k)/E)$ είναι ακριβώς ίδια με αυτήν που παρουσιάζεται στην §126 σε σχέση με το εκεί αποδεικνυόμενο αποτέλεσμα $\omega\in\mathcal{G}(E/F)=\mathcal{G}(F(k)/F)$ με E στη θέση του F και L στη θέση του E. Μέχρις στιγμής έχουμε δείξει ότι το P περιέχει ακριβώς εκείνα τα στοιχεία ψ_j της $\mathcal{G}(F(k)/F)$ για τα οποία ισχύει $\psi_j(k)=k_j$, $j=1,2,\ldots,n$.

Θα δείξουμε τώρα ότι το P είναι ομάδα ως προς την πράξη της $\mathcal{G}(F(k)/F)$. Έστω $(\tau_j)_r, (\tau_\ell)_r \in P$. Πρέπει πρώτα να δείξουμε ότι και το «γινόμενο» $(\tau_j)_r\,(\tau_\ell)_r \in P$. Από τα προηγούμενα, κάθε στοιχείο του P ισούται με ένα στοιχείο της $\mathcal{G}(F(k)/F)$ που απεικονίζει την $k_1 = k$ στις διαφορετικές ρίζες k_j, $j = 1, 2, \ldots, n$ του $q_E(x)$ και αντιστρόφως. Άρα, $(\tau_j)_r = \psi_j \in \mathcal{G}(F(k)/F)$ με $\psi_j(k) = k_j$ και $(\tau_\ell)_r = \psi_\ell \in \mathcal{G}(F(k)/F)$ με $\psi_\ell(k) = k_\ell$, $j, \ell \in \{1, 2, \ldots, n\}$. Για να ανήκει το «γινόμενο» $(\tau_j)_r\,(\tau_\ell)_r$ στο P αρκεί να υπάρχει στοιχείο $\psi_s \in \mathcal{G}(F(k)/F)$ με $\psi_s(k) = k_s$, $s \in \{1, 2, \ldots, n\}$ ώστε $(\tau_j)_r\,(\tau_\ell)_r = \psi_s$ ή ισοδυνάμως $\psi_j\,\psi_\ell = \psi_s$.

Το $\psi_j\,\psi_\ell$ είναι στοιχείο της $\mathcal{G}(F(k)/F)$ ως «γινόμενο» στοιχείων της ομάδας $\mathcal{G}(F(k)/F)$. Επιπλέον, $(\psi_j\,\psi_\ell)(k) = \psi_j(\psi_\ell(k)) = \psi_j(k_\ell)$. Όμως το k_ℓ είναι ρίζα του $q_E(x)$ και από τα προαναφερθέντα, $\psi_j(k_\ell) = (\tau_j)_r(k_\ell) = \tau_j(k_\ell) = k_s$ με $s \in \{1, 2, \ldots, n\}$ γιατί από την §126, τα στοιχεία της $\mathcal{G}(E(k)/E)$ απεικονίζουν τις ρίζες του $q_E(x)$ σε ρίζες του $q_E(x)$. Άρα, $(\psi_j\,\psi_\ell)(k) = k_s$ με $s \in \{1, 2, \ldots, n\}$ και το «γινόμενο» $(\tau_j)_r\,(\tau_\ell)_r \in P$.

Το P είναι ένα κλειστό ως προς την πράξη της $\mathcal{G}(F(k)/F)$ και πεπερασμένο ως προς το πλήθος των στοιχείων που περιέχει σύνολο αυτομορφισμών του $F(k)$. Από την §158, το P είναι ομάδα ως προς το «γινόμενο» αυτομορφισμών, και σαν υποσύνολο της $\mathcal{G}(F(k)/F)$ είναι υποομάδα της.

§160. Έστω F σώμα, p πρώτος αριθμός, ζ μία p–οστή πρωταρχική ρίζα της μονάδας. Η $\mathcal{G}(\mathbf{F}(\zeta)/\mathbf{F})$ είναι κυκλική ομάδα.

Θεωρούμε το σύνολο P των περιορισμών των στοιχείων της $\mathcal{G}(F(\zeta)/F)$ στο $F_{\mathbb{Q}}(\zeta)$. Από την §5, $F_{\mathbb{Q}} \subseteq F$. Έστω $q_F(x)$ ένα ελάχιστο πολυώνυμο της ζ στο $F[x]$ και $q_{F_{\mathbb{Q}}}(x)$ ένα ελάχιστο πολυώνυμο της ζ στο $F_{\mathbb{Q}}[x]$. Από την §65, τα $q_F(x)$, $q_{F_{\mathbb{Q}}}(x)$ είναι ανάγωγα στα $F[x]$, $F_{\mathbb{Q}}[x]$ αντιστοίχως. Από την §156, και το $q(x) = \sum_{i=0}^{p-1} x^i$ είναι ανάγωγο στο $F_{\mathbb{Q}}[x]$. Επιπλέον, οι ρίζες του $q(x)$ είναι οι $\zeta, \zeta^2, \ldots, \zeta^{p-1}$.

Τα $q_{F_{\mathbb{Q}}}(x)$, $q(x)$ είναι ανάγωγα στο $F_{\mathbb{Q}}[x]$ και έχουν κοινή ρίζα την ζ. Από το τελευταίο μέρος της απόδειξης της §139, το $q_{F_{\mathbb{Q}}}(x)$ διαιρεί το $q(x)$ στο $F_{\mathbb{Q}}[x]$ και αντιστρόφως. Άρα, $q(x) = a\,q_{F_{\mathbb{Q}}}(x)$ με $a \in F_{\mathbb{Q}} - \{0\}$. Από την §65, το $q(x)$ είναι ένα ελάχιστο πολυώνυμο της ζ στο $F_{\mathbb{Q}}[x]$ και στην συνέχεια αντί του $q_{F_{\mathbb{Q}}}(x)$ θα χρησιμοποιούμε το $q(x)$. Το $q(x)$ ανήκει και στο $F[x]$ αφού, $F_{\mathbb{Q}}[x] \subseteq F[x]$. Τα $q(x)$, $q_F(x)$ έχουν κοινή ρίζα την ζ και το $q_F(x)$ είναι ανάγωγο στο $F[x]$. Από το τελευταίο μέρος της απόδειξης της §139, το $q_F(x)$ διαιρεί το $q(x)$ στο $F[x]$ και οι ρίζες του $q_F(x)$ περιέχονται στις ρίζες του $q(x)$.

Άρα, όλες οι ρίζες ενός ελαχίστου πολυωνύμου της ζ στο $F[x]$ περιέχονται στο σύνολο $\{\zeta, \zeta^2, \ldots, \zeta^{p-1}\}$ των ριζών του $q(x)$. Οι ρίζες του $q(x)$ ανήκουν στο $F_{\mathbb{Q}}(\zeta)$ και στο $F(\zeta)$. Άρα, οι ρίζες ενός ελαχίστου πολυωνύμου της ζ στο $F[x]$ ανήκουν στα $F_{\mathbb{Q}}(\zeta)$ και $F(\zeta)$. Από την §159, το P είναι υποομάδα της $\mathcal{G}(F_{\mathbb{Q}}(\zeta)/F_{\mathbb{Q}})$ η οποία $\mathcal{G}(F_{\mathbb{Q}}(\zeta)/F_{\mathbb{Q}})$ με τη σειρά της, από την §157, είναι κυκλική ομάδα. Από τις §90, §98, §126, προκύπτει ότι, η $\mathcal{G}(F_{\mathbb{Q}}(\zeta)/F_{\mathbb{Q}})$ έχει πεπερασμένη τάξη, η τάξη της P διαιρεί την τάξη της $\mathcal{G}(F_{\mathbb{Q}}(\zeta)/F_{\mathbb{Q}})$ και άρα η P είναι κυκλική ομάδα.

Εφαρμόζοντας την απόδειξη της §159 για $E = F$, $F = F_{\mathbb{Q}}$, $q_E(x) = q_F(x)$, $k = \zeta$, $\mathcal{K}$ το σύνολο των ριζών του $q_F(x)$ προκύπτει ότι κάθε στοιχείο της P επεκτείνεται σε στοιχείο της $\mathcal{G}(F(\zeta)/F)$. Επίσης, τα στοιχεία της P είναι τα στοιχεία της $\mathcal{G}(F(\zeta)/F)$ περιορισμένα στο $F_{\mathbb{Q}}(\zeta)$. Τα στοιχεία των $\mathcal{G}(F(\zeta)/F)$ και P βρίσκονται σε ένα προς ένα και επί αντιστοιχία. Επιπλέον, από την §126

κάθε στοιχείο της $\mathcal{G}(F(\zeta)/F)$ απεικονίζει την ζ σε ρίζα του $q_F(x)$ δηλαδή, σε κάποια δύναμη ζ^k με $k \in \{1, 2, \ldots, p-1\}$. Οπότε, αν $\tau \in \mathcal{G}(F(\zeta)/F)$, $\tau(\zeta) = \zeta^k$ για κάποιο $k \in \{1, 2, \ldots, p-1\}$.

Συμβολίζουμε με τ_r τον περιορισμό του τ στο $F_{\mathbb{Q}}(\zeta)$. Από τον ορισμό του τ_r, η δράση του τ_r πάνω στην ζ είναι η δράση του τ πάνω στην ζ όταν την ζ την βλέπουμε ως στοιχείο του $F_{\mathbb{Q}}(\zeta)$. Όμως η ζ, είναι ταυτόχρονα στοιχείο και του $F(\zeta)$ και του $F_{\mathbb{Q}}(\zeta)$. Άρα, όταν ο τ δρα πάνω στην ζ ως στοιχείο του $F_{\mathbb{Q}}(\zeta)$ ταυτόχρονα δρα πάνω σε αυτήν και ως στοιχείο του $F(\zeta)$. Τελικά, $\zeta^k = \tau(\zeta) = \tau_r(\zeta)$. Δηλαδή, ο περιορισμός κάθε στοιχείου της $\mathcal{G}(F(\zeta)/F)$ στο $F_{\mathbb{Q}}(\zeta)$, επίσης απεικονίζει την ζ στην ίδια δύναμη ζ^k με $k \in \{1, 2, \ldots, p-1\}$ στην οποία το ζ απεικονίζεται από το αντίστοιχο στοιχείο της $\mathcal{G}(F(\zeta)/F)$ που έδωσε τον περιορισμό αυτό.

Συμβολίζουμε με $[\tau_r]_g$ έναν γεννήτορα της κυκλικής ως προς την πράξη «γινόμενο» ομάδας P. Θεωρούμε το στοιχείο $\tau_g \in \mathcal{G}(F(\zeta)/F)$ του οποίου περιορισμός στο $F_{\mathbb{Q}}(\zeta)$ είναι ο $[\tau_r]_g$. Θα δείξουμε ότι κάθε στοιχείο της $\mathcal{G}(F(\zeta)/F)$ γράφεται ως δύναμη του τ_g. Έστω $\psi \in \mathcal{G}(F(\zeta)/F)$, ψ_r ο περιορισμός του ψ στο $F_{\mathbb{Q}}(\zeta)$. Από την §66 και τον ορισμό των ψ, ψ_r,

$$\psi\left(\sum_{t=0}^{d_F-1} f_t\,\zeta^t\right) = \sum_{t=0}^{d_F-1} f_t\,\psi(\zeta)^t = \sum_{t=0}^{d_F-1} f_t\,\psi_r(\zeta)^t, \tag{49}$$

με $d_F = deg[q_F(x)]$, $f_t \in F$. Όμως, $\psi_r \in P$ και άρα, $\psi_r = [\tau_r]_g^{\ell}$ για κάποιο $\ell \in \mathbb{N}$. Σύμφωνα με τα όσα αναφέραμε πιο πάνω, $\tau_g(\zeta) = [\tau_r]_g(\zeta) = \zeta^k$ για κάποιο $k \in \{1, 2, \ldots, p-1\}$. Οπότε,

$$\begin{aligned}\psi_r(\zeta) &= [\tau_r]_g^{\ell}(\zeta) = \underbrace{[\tau_r]_g([\tau_r]_g(\cdots[\tau_r]_g([\tau_r]_g}_{\ell-\text{το πλήθος}}(\zeta)))) = \\ &= \underbrace{\tau_g(\tau_g(\cdots\tau_g(\tau_g}_{\ell-\text{το πλήθος}}(\zeta)))) = \tau_g^{\ell}(\zeta).\end{aligned}$$

Από την (49) και την προηγούμενη ισότητα, μπορούμε να γράψουμε,

$$\begin{aligned}\psi\left(\sum_{t=0}^{d_F-1} f_t\,\zeta^t\right) &= \sum_{t=0}^{d_F-1} f_t\,\{[\tau_r]_g^{\ell}(\zeta)\}^t = \sum_{t=0}^{d_F-1} f_t\,\{\tau_g^{\ell}(\zeta)\}^t = \\ &= \tau_g^{\ell}\left(\sum_{t=0}^{d_F-1} f_t\,\zeta^t\right).\end{aligned}$$

Η τελευταία ισότητα επάγει ότι $\psi = \tau_g^{\ell}$ και το συμπέρασμα προκύπτει.

§161. Έστω $\mathbf{E}, \mathbf{F}$ σώματα, $\mathbf{p}$ πρώτος αριθμός, το $\mathbf{F}$ περιέχει τις $\mathbf{p}$–οστές ρίζες της μονάδας, $\mathbf{k} \in \mathbf{E}$, $\mathbf{k} \notin \mathbf{F}$, $\mathbf{k^p} \in \mathbf{F}$. Η $\mathbf{F(k)/F}$ είναι κανονική επέκταση του $\mathbf{F}$ με διάσταση $(\mathbf{F(k)} : \mathbf{F}) = \mathbf{p}$.

Έστω ζ μία πρωταρχική p–οστή ρίζα της μονάδας. Από την §104 οι p–οστές ρίζες ρίζες της μονάδας γράφονται ως ζ^m με $m = 0, 1, 2, \ldots, p-1$. Από την υπόθεση οι ζ^m με $m = 0, 1, 2, \ldots, p-1$ ανήκουν στο F. Το $h(x) = x^p - k^p \in F[x]$ έχει ρίζες τις $k\,\zeta^m$ με $m = 0, 1, 2, \ldots, p-1$ γιατί $h(x) = k^p\,[(k^{-1}\,x)^p - 1]$. Οι $k\,\zeta^m$ με $m = 0, 1, 2, \ldots, p-1$ ανήκουν στο $F(k)$.

Έστω K σώμα με $F \subseteq K \subseteq F(k)$ το οποίο περιέχει τις ρίζες του $h(x)$. Τότε, το K περιέχει το k και το F άρα και το $F(k)$. Από την υπόθεση για το K προκύπτει $K = F(k)$. Η $F(k)/F$ είναι η μικρότερη επέκταση του F εντός του E που περιέχει τις ρίζες του $h(x)$. Το $F(k)$ είναι το σώμα διαχωρισμού του $h(x)$ στην επέκταση E/F και από την §140 η $F(k)/F$ είναι κανονική επέκταση του F και $|\mathcal{G}(F(k)/F)| = (F(k) : F)$.

Αν $(F(k) : F) = 1$, τότε $F(k) = F$ και $k \in F$ άτοπο από την υπόθεση. Άρα, $(F(k) : F) \geq 2$ και $|\mathcal{G}(F(k)/F)| \geq 2$. Αν για κάθε $\tau \in \mathcal{G}(F(k)/F)$ ισχύει $\tau(k) = k$, τότε από την §143 προκύπτει ότι όλα τα στοιχεία της $\mathcal{G}(F(k)/F)$ είναι ο ταυτοτικός αυτομορφισμός και άρα $|\mathcal{G}(F(k)/F)| = 1$ άτοπο. Υπάρχει λοιπόν $\tau \in \mathcal{G}(F(k)/F)$ ώστε $\tau(k) \neq k$. Από την §123,

$$0 = \tau(0) = \tau(h(k)) = \tau(k^p - k^p) = \tau(k^p) - \tau(k^p) = [\tau(k)]^p - k^p,$$

γιατί το $k^p \in F$ και ο τ είναι ταυτοτικός στο F. Άρα, το $\tau(k) \in \{k, k\,\zeta, k\,\zeta^2, \ldots, k\,\zeta^{p-1}\}$. Όμως $\tau(k) \neq k$ οπότε, $\tau(k) = k\,\zeta^m$ για κάποιο $m \in \{1, 2, \ldots, p-1\}$, και $\zeta^m = \frac{\tau(k)}{k}$ για κάποιο $m \in \{1, 2, \ldots, p-1\}$. Οι m, p είναι πρώτοι μεταξύ τους και από τις §96, §104 η ζ^m είναι πρωταρχική p–οστή ρίζα της μονάδας. Θέτουμε $\omega = \frac{\tau(k)}{k} = \zeta^m$. Η ω ανήκει στο F από την υπόθεση της §161. Οπότε,

$$\begin{aligned}
\tau(k) &= \omega\,k, \\
\tau^2(k) &= \tau(\tau(k)) = \tau(\omega\,k) = \tau(\omega)\,\tau(k) = \omega\,(\omega\,k) = \omega^2\,k, \\
\tau^3(k) &= \tau(\tau^2(k)) = \tau(\omega^2\,k) = \tau(\omega^2)\,\tau(k) = \omega^2\,(\omega\,k) = \omega^3\,k, \\
&\vdots \\
\tau^p(k) &= \tau(\tau^{p-1}(k)) = \tau(\omega^{p-1}\,k) = \tau(\omega^{p-1})\,\tau(k) = \omega^{p-1}\,(\omega\,k) = \omega^p\,k.
\end{aligned}$$

Έστω ότι $\tau^i = \tau^j$ για κάποια i, j με $1 \leq i < j \leq p$. Τότε, $\tau^i(k) = \tau^j(k)$ ή $\omega^i\,k = \omega^j\,k$ ή $\omega^{j-i} = 1$. Από την §104, η ω ως πρωταρχική p–οστή ρίζα της μονάδας παράγει την κυκλική ομάδα $\mathcal{Z}$ των p–οστών ριζών της μονάδας η οποία από την §103 έχει p το πλήθος στοιχεία. Επειδή το σύνολο $\{1, \omega^2, \omega^3, \ldots, \omega^{j-i}\}$ είναι κυκλική υποομάδα της $\mathcal{Z}$, από την §90 η τάξη της $j - i$ διαιρεί την τάξη p της $\mathcal{Z}$ άτοπο. Άρα, οι $\tau, \tau^2, \ldots, \tau^p$ είναι p το πλήθος διακεκριμένα στοιχεία της $\mathcal{G}(F(k)/F)$ και $|\mathcal{G}(F(k)/F)| \geq p$. Έχουμε ήδη δείξει ότι $|\mathcal{G}(F(k)/F)| = (F(k) : F)$ οπότε, $(F(k) : F) \geq p$.

Από την άλλη, η §66 επάγει ότι $(F(k) : F) = deg[f(x)]$ με $f(x)$ ένα ελάχιστο πολυώνυμο του k στο $F[x]$. Επειδή το k είναι ρίζα του $h(x) = x^p - k^p \in F[x]$ έπεται ότι $deg[f(x)] \leq deg[h(x)] = p$ και $(F(k) : F) \leq p$. Τελικά, $(F(k) : F) = p$ και το συμπέρασμα προκύπτει.

§162. Έστω $\mathbf{R_j}$ σώματα, $\mathbf{j = 0, 1, \ldots, n-1}$, $\mathbf{R_{j+1} = R_j(\sqrt[p_j]{a_j})}$, $\mathbf{a_j \in R_j}$, $\mathbf{\sqrt[p_j]{a_j} \notin R_j}$, $\mathbf{p_j}$ πρώτος αριθμός, $\mathbf{\sqrt[p_j]{a_j}}$ μία $\mathbf{p_j}$–οστή ρίζα του $\mathbf{a_j}$. Τότε, για $\mathbf{n \geq 1}$, η σειρά σωμάτων,

$$\mathbf{R_0 \subset R_1 \subset \cdots \subset R_{n-1} \subset R_n},$$

επεκτείνεται σε σειρά σωμάτων,

$$\mathbf{R_0 = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{m-1} \subseteq F_m},$$

ώστε για $\mathbf{j = 0, 1, \ldots, m-1}$ η $\mathbf{F_{j+1}/F_j}$ είναι κανονική επέκταση του $\mathbf{F_j}$ με διάσταση $\mathbf{(F_{j+1} : F_j) = q_j}$ πρώτο αριθμό και $\mathbf{R_n \subseteq F_m}$.

Θεωρούμε την σειρά σωμάτων,

$$R_0 \subset R_1 \subset \cdots \subset R_{n-1} \subset R_n, \tag{50}$$

που μας δόθηκε από την υπόθεση. Συμβολίζουμε με ζ_j μία πρωταρχική p_j–στή ρίζα της μονάδας. Έστω ότι ο $n = 1$. Τότε, η σειρά σωμάτων (50) γίνεται $R_0 \subset R_1$.

1. Αν $\zeta_0 \in R_0$, τότε όλες οι p_0–οστές ρίζες της μονάδας ανήκουν στο R_0 γιατί από την §104 αυτές γράφονται ως δυνάμεις της ζ_0. Επίσης, $R_0(\sqrt[p_0]{a_0}, \zeta_0) = R_0(\sqrt[p_0]{a_0}) = R_1$. Από την υπόθεση, $\sqrt[p_0]{a_0} \notin R_0$ ενώ, $a_0 \in R_0$. Τότε, $(\sqrt[p_0]{a_0})^{p_0} = a_0 \in R_0$ και από την §161 η $R_0(\sqrt[p_0]{a_0})/R_0$ είναι κανονική επέκταση του R_0 διάστασης $(R_0(\sqrt[p_0]{a_0}) : R_0) = p_0$. Δηλαδή, υπάρχει σειρά σωμάτων,

$$R_0 = F_0 \subset F_1 = R_1 = R_0(\sqrt[p_0]{a_0}), \tag{51}$$

ώστε η F_1/F_0 είναι κανονική επέκταση του F_0 με διάσταση $(F_1 : F_0) = p_0$ πρώτο αριθμό και $R_1 \subseteq F_1$. Σε αυτή την περίπτωση το ζητούμενο συμπέρασμα ισχύει για $m = 1$ και τα σώματα F_0, F_1 της (51).

2. Έστω $\zeta_0 \notin R_0$. Από την §160 η $\mathcal{G}(R_0(\zeta_0)/R_0)$ είναι κυκλική ομάδα. Από την §126 η $\mathcal{G}(R_0(\zeta_0)/R_0)$ είναι πεπερασμένη ομάδα και από την §110 είναι επιλύσιμη ομάδα. Το $R_0(\zeta_0)$ περιέχει τις p_0–οστές ρίζες ζ_0^t της μονάδας, $t = 0, 1, 2, \ldots, p_0 - 1$. Άρα, το $R_0(\zeta_0)$ περιέχει τις ρίζες του πολυωνύμου $q(x) = \sum_{i=0}^{p_0-1} x^i \in R_0[x]$. Αν σώμα K με $R_0 \subseteq K \subseteq R_0(\zeta_0)$ περιέχει τις ρίζες του $q(x)$, τότε περιέχει την ζ_0. Οπότε, $R_0(\zeta_0) \subseteq K$. Τελικά, $K = R_0(\zeta_0)$ και το $R_0(\zeta_0)$ είναι το μικρότερο σώμα στην επέκταση $R_1(\zeta_0)/R_0$ που περιέχει τις ρίζες του $q(x)$. Το $R_0(\zeta_0)$ είναι σώμα διαχωρισμού του $q(x)$ στην επέκταση $R_1(\zeta_0)/R_0$. Εφαρμόζοντας την §153 με $L = R_1(\zeta_0)$, $E = R_0(\zeta_0)$, $F = R_0$, $f(x) = q(x)$ προκύπτει ότι, υπάρχει σειρά σωμάτων,

$$R_0 = T_{00} \subseteq T_{01} \subseteq \cdots \subseteq T_{0(\ell_0-1)} \subseteq T_{0\ell_0} = R_0(\zeta_0), \tag{52}$$

ώστε για $j = 0, 1, \ldots, \ell_0 - 1$ η $T_{0(j+1)}/T_{0j}$ είναι κανονική επέκταση του T_{0j} με διάσταση $(T_{0(j+1)} : T_{0j}) = d_{0j}$ πρώτο αριθμό.

Αν $\sqrt[p_0]{a_0} \in R_0(\zeta_0)$, τότε $R_0(\zeta_0) = R_0(\zeta_0, \sqrt[p_0]{a_0}) = (R_0(\sqrt[p_0]{a_0}))(\zeta_0) = R_1(\zeta_0)$ άτοπο γιατί $R_0 \subset R_1$. Οπότε, $\sqrt[p_0]{a_0} \notin R_0(\zeta_0)$ ενώ, $(\sqrt[p_0]{a_0})^{p_0} = a_0 \in R_0 \subset R_0(\zeta_0)$. Το $R_0(\zeta_0)$ περιέχοντας την ζ_0 περιέχει όλες τις p_0–οστές ρίζες της μονάδας. Από την §161, η επέκταση,

$$(R_0(\zeta_0))(\sqrt[p_0]{a_0})/R_0(\zeta_0) \overset{\S 51}{=} (R_0(\sqrt[p_0]{a_0}))(\zeta_0)/R_0(\zeta_0) = R_1(\zeta_0)/R_0(\zeta_0),$$

είναι κανονική επέκταση του $R_0(\zeta_0)$ με διάσταση $(R_1(\zeta_0) : R_0(\zeta_0)) = p_0$ πρώτο αριθμό. Από την (52) και το προηγούμενο αποτέλεσμα προκύπτει ότι υπάρχει σειρά σωμάτων,

$$R_0 = T_{00} \subseteq T_{01} \subseteq \cdots \subseteq T_{0(\ell_0-1)} \subseteq T_{0\ell_0} = R_0(\zeta_0) \subset R_1(\zeta_0), \tag{53}$$

ώστε για $j = 0, 1, \ldots, \ell_0 - 1$ η $T_{0(j+1)}/T_{0j}$ είναι κανονική επέκταση του T_{0j} με διάσταση $(T_{0(j+1)} : T_{0j}) = d_{0j}$ πρώτο αριθμό, η $R_1(\zeta_0)/R_0(\zeta_0)$ είναι κανονική επέκταση του $R_0(\zeta_0)$ με διάσταση $(R_1(\zeta_0) : R_0(\zeta_0)) = p_0$ πρώτο αριθμό και $R_1 \subseteq R_1(\zeta_0)$. Σε αυτή την περίπτωση το ζητούμενο συμπέρασμα ισχύει για $m = \ell_0 + 1$ και τα σώματα $F_0 = T_{00}$, $F_1 = T_{01}$, …, $F_{m-1} = T_{0\ell_0}$, $F_m = R_1(\zeta_0)$ της (53).

Προχωρώντας επαγωγικά, υποθέτουμε ότι το συμπέρασμα ισχύει για $n > 1$. Τότε, η (50) γίνεται $R_0 \subset R_1 \subset \cdots \subset R_n$. Από την προαναφερθείσα υπόθεση της επαγωγής, η σειρά σωμάτων στην (50) επεκτείνεται σε σειρά σωμάτων,

$$R_0 = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{m-1} \subseteq F_m, \tag{54}$$

ώστε για $j = 0, 1, \ldots, m - 1$ η F_{j+1}/F_j είναι κανονική επέκταση του F_j με διάσταση $(F_{j+1} : F_j) = q_j$ πρώτο αριθμό και $R_n \subseteq F_m$. Θα αποδείξουμε ότι το συμπέρασμα ισχύει και για $n + 1$. Τότε, η (50) γίνεται $R_0 \subset R_1 \subset \cdots \subset R_{n+1}$. Από την υπόθεση της επαγωγής, το μέρος της (50) που περιλαμβάνει τους πρώτους $n + 1$ όρους της δηλαδή, το $R_0 \subset R_1 \subset \cdots \subset R_n$ επεκτείνεται στην σειρά σωμάτων (54). Θα επεκτείνουμε περαιτέρω την (54) ώστε οι όροι της να ικανοποιούν της απαιτήσεις του προς απόδειξη συμπεράσματος και για $n + 1$ δηλαδή, για $n + 2$ το πλήθος όρους στην (50).

1. Αν $\zeta_n \in F_m$, τότε όλες οι p_n–οστές ρίζες της μονάδας ανήκουν στο F_m γιατί από την §104 αυτές γράφονται ως δυνάμεις της ζ_n.

1.1. Αν $\sqrt[p_n]{a_n} \in F_m$, τότε το R_{n+1}, που από την υπόθεση της §162 ισούται με $R_n(\sqrt[p_n]{a_n})$, περιέχεται στο F_m. Αυτό γιατί το F_m περιέχει τα R_n και $\sqrt[p_n]{a_n}$. Σε αυτή την περίπτωση το προς απόδειξη συμπέρασμα ισχύει για την (54) η οποία δεν χρειάζεται περαιτέρω επέκταση.

1.2. Αν $\sqrt[p_n]{a_n} \notin F_m$, τότε επειδή $(\sqrt[p_n]{a_n})^{p_n} = a_n \in R_n \subseteq F_m$, από την §161 η $F_m(\sqrt[p_n]{a_n})/F_m$ είναι κανονική επέκταση του F_m διάστασης $(F_m(\sqrt[p_n]{a_n}) : F_m) = p_n$. Δηλαδή, η (54) επεκτείνεται στην σειρά σωμάτων,

$$R_0 = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{m-1} \subseteq F_m \subseteq F_{m+1} = F_m(\sqrt[p_n]{a_n}), \tag{55}$$

ώστε για $j = 0, 1, \ldots, m$ η F_{j+1}/F_j είναι κανονική επέκταση του F_j με διάσταση $(F_{j+1} : F_j) = q_j$ πρώτο αριθμό και $R_{n+1} = R_n(\sqrt[p_n]{a_n}) \subseteq F_{m+1}$ γιατί $R_n \subseteq F_m \subseteq F_{m+1}$ και $\sqrt[p_n]{a_n} \in F_{m+1}$. Σε αυτή την περίπτωση το προς απόδειξη συμπέρασμα ισχύει για την σειρά σωμάτων (55).

2. Αν $\zeta_n \notin F_m$, τότε από την §160 η $\mathcal{G}(F_m(\zeta_n)/F_m)$ είναι κυκλική ομάδα. Από την §126 η $\mathcal{G}(F_m(\zeta_n)/F_m)$ είναι πεπερασμένη ομάδα και από την §110 είναι επιλύσιμη ομάδα. Το $F_m(\zeta_n)$ περιέχει τις p_n–οστές ρίζες ζ_n^t της μονάδας, $t = 0, 1, 2, \ldots, p_n - 1$. Άρα, το $F_m(\zeta_n)$ περιέχει τις ρίζες του πολυωνύμου $q(x) = \sum_{i=0}^{p_n-1} x^i \in F_m[x]$. Αν σώμα K με $F_m \subseteq K \subseteq F_m(\zeta_n)$ περιέχει τις ρίζες του $q(x)$, τότε περιέχει την ζ_n. Οπότε, $F_m(\zeta_n) \subseteq K$. Τελικά, $K = F_m(\zeta_n)$ και το $F_m(\zeta_n)$ είναι το μικρότερο σώμα στην επέκταση $F_m(\zeta_n)/F_m$ που περιέχει τις ρίζες του $q(x)$. Το $F_m(\zeta_n)$ είναι σώμα διαχωρισμού του $q(x)$

στην επέκταση $F_m(\zeta_n)/F_m$. Εφαρμόζοντας την §153 με $L = E = F_m(\zeta_n)$, $F = F_m$, $f(x) = q(x)$ προκύπτει ότι, υπάρχει σειρά σωμάτων,

$$F_m = T_{m0} \subseteq T_{m1} \subseteq \cdots \subseteq T_{m(\ell_m-1)} \subseteq T_{m\ell_m} = F_m(\zeta_n), \qquad (56)$$

ώστε για $j = 0, 1, \ldots, \ell_m - 1$ η $T_{m(j+1)}/T_{mj}$ είναι κανονική επέκταση του T_{mj} με διάσταση $(T_{m(j+1)} : T_{mj}) = d_{mj}$ πρώτο αριθμό.

2.1. Αν $\sqrt[p_n]{a_n} \in F_m(\zeta_n)$, τότε το R_{n+1}, που από την υπόθεση της §162 ισούται με $R_n(\sqrt[p_n]{a_n})$, περιέχεται στο $F_m(\zeta_n)$. Αυτό γιατί το $F_m(\zeta_n)$ περιέχει τα R_n και $\sqrt[p_n]{a_n}$. Σε αυτή την περίπτωση το προς απόδειξη συμπέρασμα ισχύει για την σειρά σωμάτων,

$$\begin{aligned} R_0 &= F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{m-1} \subseteq F_m = \\ &= T_{m0} \subseteq T_{m1} \subseteq \cdots \subseteq T_{m(\ell_m-1)} \subseteq T_{m\ell_m} = F_m(\zeta_n), \end{aligned}$$

που προκύπτει από την επέκταση της (54) μέσω της (56).

2.2. Αν $\sqrt[p_n]{a_n} \notin F_m(\zeta_n)$, τότε επειδή $(\sqrt[p_n]{a_n})^{p_n} = a_n \in R_n \subseteq F_m(\zeta_n)$, από την §161 η $(F_m(\zeta_n))(\sqrt[p_n]{a_n})/F_m(\zeta_n)$ είναι κανονική επέκταση του $F_m(\zeta_n)$ διάστασης $((F_m(\zeta_n))(\sqrt[p_n]{a_n}) : F_m(\zeta_n)) = p_n$. Δηλαδή, η (56) επεκτείνεται στην σειρά σωμάτων,

$$\begin{aligned} F_m &= T_{m0} \subseteq T_{m1} \subseteq \cdots \subseteq T_{m(\ell_m-1)} \subseteq T_{m\ell_m} = F_m(\zeta_n) \subseteq \\ &\subseteq (F_m(\zeta_n))(\sqrt[p_n]{a_n}), \end{aligned}$$

ή επανασυμβολίζοντας καταλλήλως τα σώματα, στην σειρά σωμάτων,

$$\begin{aligned} F_m &\subseteq F_{m+1} \subseteq \cdots \subseteq F_{m+\ell_m-1} \subseteq F_{m+\ell_m} = F_m(\zeta_n) \subseteq \\ &\subseteq F_{m+\ell_m+1} = (F_m(\zeta_n))(\sqrt[p_n]{a_n}), \end{aligned} \qquad (57)$$

ώστε για $j = 0, 1, \ldots, \ell_m$ η F_{m+j+1}/F_{m+j} είναι κανονική επέκταση του F_{m+j} με διάσταση $(F_{m+j+1} : F_{m+j}) = q_{m+j}$ πρώτο αριθμό και $R_{n+1} = R_n(\sqrt[p_n]{a_n}) \subseteq F_{m+\ell_m+1}$ γιατί $R_n \subseteq F_m \subseteq F_{m+\ell_m} \subseteq F_{m+\ell_m+1}$ και $\sqrt[p_n]{a_n} \in F_{m+\ell_m+1}$. Σε αυτή την περίπτωση το προς απόδειξη συμπέρασμα ισχύει για την σειρά σωμάτων,

$$\begin{aligned} R_0 &= F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{m-1} \subseteq F_m \subseteq \\ &\subseteq F_{m+1} \subseteq \cdots \subseteq F_{m+\ell_m-1} \subseteq F_{m+\ell_m} = F_m(\zeta_n) \subseteq \\ &\subseteq F_{m+\ell_m+1} = (F_m(\zeta_n))(\sqrt[p_n]{a_n}), \end{aligned}$$

που προκύπτει από την επέκταση της (54) μέσω της (57).

Τελικά, αποδείξαμε επαγωγικώς το συμπέρασμα της §162 σε κάθε περίπτωση.

§163. Έστω $\mathbf{L, E, F}$ σώματα, $\mathbf{L \supseteq E \supset F}$, $\mathbf{f(x) \in F[x]}$, $\mathbf{E}$ το σώμα διαχωρισμού του $\mathbf{f(x)}$ στην επέκταση $\mathbf{L/F}$, η $\mathbf{f(x) = 0}$ είναι επιλύσιμη δια ριζικών. Τότε υπάρχει σειρά σωμάτων,

$$\mathbf{F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{m-1} \subseteq F_m},$$

ώστε, $\mathbf{E \subseteq F_m}$ και για $\mathbf{j = 0, 1, \ldots, m-1}$ η $\mathbf{F_{j+1}/F_j}$ είναι κανονική επέκταση του $\mathbf{F_j}$ με διάσταση $\mathbf{(F_{j+1} : F_j) = q_j}$ πρώτο αριθμό.

Από τις §77, §78 υπάρχει σειρά σωμάτων,

$$F = R_0 \subset R_1 \subset \cdots \subset R_{n-1} \subset R_n, \tag{58}$$

ώστε για $j = 0, 1, \ldots, n-1$, $R_{j+1} = R_j(\sqrt[p_j]{a_j})$, $a_j \in R_j$, $\sqrt[p_j]{a_j} \notin R_j$, p_j πρώτος αριθμός, $\sqrt[p_j]{a_j}$ μία p_j–οστή ρίζα του a_j, $E \subseteq R_n$.

Αν η σειρά (58) περιέχει μόνο έναν όρο δηλαδή, $n = 0$, τότε $E \subseteq R_0 = F$ και η εξίσωση $f(x) = 0$ είναι επιλύσιμη δια ριζικών στο $F[x]$. Το σώμα διαχωρισμού του $f(x)$ στην επέκταση L/F είναι το F γιατί από τα προηγούμενα και την υπόθεση προκύπτει $F \subset E \subseteq F$. Άτοπο γιατί από την υπόθεση $F \subset E$.

Άρα, στην (58) έχουμε $n \geq 1$ και από την §162 προκύπτει ότι η (58) επεκτείνεται σε σειρά σωμάτων,

$$R_0 = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{m-1} \subseteq F_m,$$

ώστε για $j = 0, 1, \ldots, m-1$ η F_{j+1}/F_j είναι κανονική επέκταση του F_j με διάσταση $(F_{j+1} : F_j) = q_j$ πρώτο αριθμό και $R_n \subseteq F_m$. Από τις ιδιότητες της (58) όμως $E \subseteq R_n \subseteq F_m$ και το συμπέρασμα προκύπτει.

§164. Έστω $\mathbf{L, E, F}$ σώματα, $\mathbf{L \supseteq E \supset F}$, $\mathbf{f(x) \in F[x]}$, $\mathbf{E}$ το σώμα διαχωρισμού του $\mathbf{f(x)}$ στην επέκταση $\mathbf{L/F}$, η $\mathbf{f(x) = 0}$ είναι επιλύσιμη δια ριζικών. Τότε υπάρχει σειρά σωμάτων,

$$\mathbf{F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_{n-1} \subseteq E_n},$$

ώστε, $\mathbf{E = E_n}$ και για $\mathbf{j = 0, 1, \ldots, n-1}$ η $\mathbf{E_{j+1}/E_j}$ είναι κανονική επέκταση του $\mathbf{E_j}$ με διάσταση $\mathbf{(E_{j+1} : E_j) = p_j}$ πρώτο αριθμό.

Από την §163, υπάρχει σειρά σωμάτων,

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{m-1} \subseteq F_m, \tag{59}$$

ώστε, $E \subseteq F_m$ και για $j = 0, 1, \ldots, m-1$ η F_{j+1}/F_j είναι κανονική επέκταση του F_j με διάσταση $(F_{j+1} : F_j) = q_j$ πρώτο αριθμό. Για $j = 0, 1, \ldots, m$ θεωρούμε τα σώματα, $E_j = F_j \cap E$. Έτσι, προκύπτει η ακολουθία σωμάτων,

$$F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_{m-1} \subseteq E_m = E,$$

Θα δείξουμε ότι για $j = 0, 1, \ldots, m-1$ είτε $E_{j+1} = E_j$ είτε η E_{j+1}/E_j είναι κανονική επέκταση του E_j με διάσταση $(E_{j+1} : E_j)$ πρώτο αριθμό. Από την (59) και την §49 προκύπτει ότι,

$$(F_{j+1} : F_0) = \prod_{i=0}^{j} (F_{i+1} : F_i). \tag{60}$$

Οι διαστάσεις $(F_{i+1} : F_i)$ είναι πρώτοι αριθμοί άρα πεπερασμένες. Οπότε και η διάσταση $(F_{j+1} : F_0)$ είναι πεπερασμένη. Επιπλέον,

$$F_0 = F_0 \cap E \subseteq E_j = F_j \cap E \subseteq E_{j+1} = F_{j+1} \cap E \subseteq F_{j+1} \Rightarrow$$
$$F_0 \subseteq E_j \subseteq E_{j+1} \subseteq F_{j+1}.$$

Οπότε,

$$(F_{j+1} : F_0) = (F_{j+1} : E_{j+1})\,(E_{j+1} : E_j)\,(E_j : F_0). \tag{61}$$

Από την (60) το γινόμενο (61) είναι πεπερασμένο. Άρα, και κάθε παράγοντας του γινομένου (61) είναι πεπερασμένος. Έπεται ότι η διάσταση $(E_{j+1} : E_j)$ είναι πεπερασμένη και από την §75, υπάρχει $e \in E_{j+1}$ αλγεβρικό επί του E_j ώστε $E_{j+1} = E_j(e)$. Επειδή, $E_{j+1} \subseteq E_m = E$ έπεται $E_j(e) \subseteq E$ και $e \in E$.

1. Αν επιπλέον $e \in F_j$, τότε $e \in F_j \cap E = E_j$ και $E_{j+1} = E_j(e) = E_j$ οπότε, προκύπτει η πρώτη περίπτωση που θέλαμε να αποδείξουμε.

2. Έστω $e \notin F_j$. Όμως $e \in E_{j+1} = F_{j+1} \cap E$ και $e \in E$ που επάγει $e \in F_{j+1}$. Επιπλέον, $F_j \subseteq F_{j+1}$. Οπότε, $F_j \subseteq F_j(e) \subseteq F_{j+1}$. Όμως, από την §49,

$$q_j = (F_{j+1} : F_j) = (F_{j+1} : F_j(e))\,(F_j(e) : F_j).$$

   Επειδή ο q_j είναι πρώτος αριθμός, η τελευταία ισότητα σημαίνει ότι είτε $(F_j(e) : F_j) = 1$ είτε $(F_j(e) : F_j) = q_j$. Η πρώτη περίπτωση απορρίπτεται γιατί αλλιώς θα ήταν $F_j(e) = F_j$ και $e \in F_j$ άτοπο. Άρα, $(F_j(e) : F_j) = q_j$ και $(F_{j+1} : F_j(e)) = 1$ που με την σειρά του συνεπάγεται $F_{j+1} = F_j(e)$. Επειδή η F_{j+1}/F_j είναι κανονική επέκταση του F_j από την §140 προκύπτει ότι $|\mathcal{G}(F_{j+1}/F_j)| = (F_{j+1} : F_j) = q_j$.

   Προηγουμένως αποδείξαμε ότι $(F_j(e) : F_j) = q_j$. Δηλαδή, η $F_j(e)/F_j$ είναι πεπερασμένη επέκταση του F_j και από την §75 η $F_j(e)/F_j$ είναι αλγεβρική επέκταση του F_j. Από την §63, κάθε στοιχείο του $F_j(e)$ είναι αλγεβρικό επί του F_j. Άρα, το e είναι αλγεβρικό επί του F_j και έστω $h_{F_j}(x)$ ένα ελάχιστο πολυώνυμο του e στο $F_j[x]$. Επειδή $(F_j(e) : F_j) = q_j$ από την §66 έπεται $deg[h_{F_j}(x)] = q_j$

   Από την §126, η $\mathcal{G}(F_{j+1}/F_j)$ περιέχει τόσα στοιχεία όσο το πλήθος των ριζών του $h_{F_j}(x)$ που ανήκουν στο $F_{j+1} = F_j(e)$. Επειδή $|\mathcal{G}(F_{j+1}/F_j)| = q_j$, έπεται ότι στο F_{j+1} ανήκουν οι q_j το πλήθος ρίζες του $h_{F_j}(x)$. Από την υπόθεση για το e, αυτό είναι αλγεβρικό επί του E_j. Έστω $h_{E_j}(x)$ ένα ελάχιστο πολυώνυμο του e στο $E_j[x]$.

   Το $h_{E_j}(x)$ είναι πολυώνυμο και του $F_j[x]$ αφού $E_j \subseteq F_j$ και $E_j[x] \subseteq F_j[x]$. Από την §65, το $h_{F_j}(x)$ είναι ανάγωγο στο $F_j[x]$. Άρα, τα $h_{F_j}(x)$, $h_{E_j}(x)$ είναι πολυώνυμα του $F_j[x]$ με κοινή ρίζα e και το $h_{F_j}(x)$ είναι ανάγωγο στο $F_j[x]$. Από το τελευταίο μέρος της απόδειξης της §139, το $h_{F_j}(x)$ διαιρεί το $h_{E_j}(x)$. Οι ρίζες του $h_{F_j}(x)$ είναι και ρίζες του $h_{E_j}(x)$. Άρα, οι q_j το πλήθος ρίζες του $h_{F_j}(x)$ που όπως προείπαμε ανήκουν στο F_{j+1} είναι και ρίζες του $h_{E_j}(x)$. Ας συμβολίσουμε τις ρίζες αυτές με $e_1 = e, e_2, \ldots, e_{q_j}$.

   Από την §140, η $E/F = E/F_0$ είναι κανονική επέκταση του F_0 γιατί το E είναι το σώμα διαχωρισμού του $f(x) \in F[x] = F_0[x]$ στην επέκταση L/F_0. Επιπλέον, επειδή, $F_0 \subseteq E_j = F_j \cap E \subseteq E$ από την §140 έπεται ότι η E/E_j είναι κανονική επέκταση του E_j. Το E περιέχει μία ρίζα, την $e_1 = e$, του $h_{E_j}(x)$. Από την §65 το $h_{E_j}(x)$ είναι ανάγωγο πολυώνυμο στο $E_j[x]$. Από την §131, το E περιέχει όλες τις ρίζες του $h_{E_j}(x)$. Άρα, το E περιέχει και τις $e_1 = e, e_2, \ldots, e_{q_j}$. Οι $e_1 = e, e_2, \ldots, e_{q_j}$ ανήκουν στα F_{j+1}, E άρα και στο $E_{j+1} = F_{j+1} \cap E$.

   Έχουμε λοιπόν αποδείξει ότι, όλες οι ρίζες ενός ελαχίστου πολυωνύμου του e στο $F_j[x]$ ανήκουν στα $F_j(e)$ και $E_j(e)$. Εφαρμόζοντας την §159 για $L = F_{j+1}$, $E = F_j$, $F = E_j$, $k = e$, $q_E(x) = h_{F_j}(x)$, $\mathcal{K} = \{e_1 =$

$e, e_2, \ldots, e_{q_j}\}$ προκύπτει ότι το σύνολο $P = \{\tau_r : \tau \in \mathcal{G}(F_j(e)/F_j)\}$ των περιορισμών τ_r των στοιχείων τ της $\mathcal{G}(F_j(e)/F_j)$ στο $E_j(e)$ είναι υποομάδα της $\mathcal{G}(E_j(e)/E_j)$.

Έστω K_P, K_{E_j} τα σταθερά σώματα των P, $\mathcal{G}(E_j(e)/E_j)$ αντιστοίχως. Κάθε στοιχείο της $\mathcal{G}(E_j(e)/E_j)$ είναι ταυτοτικό στο E_j αφήνοντας κάθε στοιχείο του E_j αναλλοίωτο. Άρα,

$$E_j \subseteq K_{E_j}. \tag{62}$$

Κάθε στοιχείο του K_{E_j} μένει αναλλοίωτο από την επί αυτού δράση των στοιχείων της $\mathcal{G}(E_j(e)/E_j)$. Τα στοιχεία της P είναι και στοιχεία της $\mathcal{G}(E_j(e)/E_j)$. Οπότε, τα στοιχεία της P δρουν επί των στοιχείων του K_{E_j} κατά τρόπο ίδιο με τον τρόπο δράσης των στοιχείων της $\mathcal{G}(E_j(e)/E_j)$. Άρα, κάθε στοιχείο του K_{E_j} μένει αναλλοίωτο από την επί αυτού δράση των στοιχείων της P και,

$$K_{E_j} \subseteq K_P. \tag{63}$$

Από την (59) η F_{j+1}/F_j είναι κανονική επέκταση του F_j. Στην πορεία δείξαμε ότι $F_{j+1} = F_j(e)$. Άρα, από την κανονικότητα της επέκτασης $F_j(e)/F_j$ και την §140 προκύπτει ότι το σταθερό σώμα της $\mathcal{G}(F_j(e)/F_j)$ είναι το F_j. Έστω $a \in K_P$. $\tau_r(a) = a$ για κάθε $\tau_r \in P$. Κάθε τ_r είναι περιορισμός επί του $E_j(e)$ στοιχείου τ της $\mathcal{G}(F_j(e)/F_j)$. Έτσι, τα $\tau \in \mathcal{G}(F_j(e)/F_j)$ δρουν επί των στοιχείων του $E_j(e)$ κατά τρόπο ίδιο με τον τρόπο δράσης των τ_r.

Η P ως υποομάδα της $\mathcal{G}(E_j(e)/E_j)$ αποτελείται από αυτομορφισμούς του $E_j(e)$ ταυτοτικούς επί του E_j. Το σταθερό σώμα της P, το K_P, από τον ορισμό της έννοιας του σταθερού σώματος, περιέχει εκείνα τα στοιχεία του $E_j(e)$, (δηλαδή, εκείνα τα στοιχεία του πεδίου ορισμού των αυτομορφισμών της P), που παραμένουν αναλλοίωτα από την επί αυτών δράση κάθε στοιχείου της P. Άρα, $K_P \subseteq E_j(e) = E_{j+1} \subseteq F_j(e)$ και τα $\tau \in \mathcal{G}(F_j(e)/F_j)$ δρουν επί των στοιχείων του K_P κατά τρόπο ίδιο με τον τρόπο δράσης των τ_r.

Άρα, $\tau(a) = \tau_r(a) = a$ για κάθε $a \in K_P$ και $\tau \in \mathcal{G}(F_j(e)/F_j)$ και τα $a \in K_P$ ανήκουν στο σταθερό σώμα της $\mathcal{G}(F_j(e)/F_j)$ το F_j. Από τα προηγούμενα, τα $a \in K_P$, ανήκουν στα $E_{j+1} \subseteq E$ και F_j δηλαδή, $a \in F_j \cap E = E_j$ και,

$$K_P \subseteq E_j. \tag{64}$$

Οι (62), (63), (64) επάγουν ότι $K_P = K_{E_j} = E_j$. Το σταθερό σώμα της $\mathcal{G}(E_j(e)/E_j)$ είναι το E_j. Από την §140, η $E_j(e)/E_j = E_{j+1}/E_j$ είναι κανονική επέκταση του E_j και,

$$(E_{j+1} : E_j) = |\mathcal{G}(E_{j+1}/E_j)| = |\mathcal{G}(E_j(e)/E_j)|. \tag{65}$$

Από την §141, έπεται ότι σε κάθε ενδιάμεσο σώμα των $E_j(e)$, E_j αντιστοιχεί μοναδική υποομάδα της $\mathcal{G}(E_j(e)/E_j)$ που έχει το σώμα αυτό ως σταθερό σώμα και αντιστρόφως. Στα ενδιάμεσα σώματα K_P, E_j των $E_j(e)$, E_j αντιστοιχούν οι P, $\mathcal{G}(E_j(e)/E_j)$ που έχουν τα K_P, E_j ως σταθερά σώματα, αντιστοίχως. Όμως $K_P = E_j$ επάγει $P = \mathcal{G}(E_j(e)/E_j)$ λόγω της μοναδικότητας.

Από τον ορισμό του το P περιέχει όλα τα στοιχεία της $\mathcal{G}(F_j(e)/F_j)$ περιορισμένα στο $E_j(e)$. Κατ΄ αναλογία με τα όσα αναφέραμε στην απόδειξη της §160, τα στοιχεία της P βρίσκονται σε ένα προς ένα και επί αντιστοιχία με τα στοιχεία της $\mathcal{G}(F_j(e)/F_j)$. Άρα,

$$|P| = |\mathcal{G}(E_j(e)/E_j)| = |\mathcal{G}(F_j(e)/F_j)| = q_j. \tag{66}$$

Οι (65), (66) επάγουν ότι $(E_{j+1} : E_j) = q_j$ και προκύπτει η δεύτερη περίπτωση που θέλαμε να αποδείξουμε.

Μετά από όσα προηγήθηκαν, αν στην σειρά σωμάτων,

$$F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_{m-1} \subseteq E_m = E,$$

παραλείψουμε τις ισότητες μεταξύ των E_j προκύπτει σειρά σωμάτων,

$$F = E_0 \subset E_1 \subset \cdots \subset E_{n-1} \subset E_n,$$

ώστε, $E = E_n$ και για $j = 0, 1, \ldots, n-1$ η E_{j+1}/E_j είναι κανονική επέκταση του E_j με διάσταση $(E_{j+1} : E_j)$ πρώτο αριθμό.

§165. Έστω $\mathbf{L}, \mathbf{E}, \mathbf{F}$ σώματα, $\mathbf{L} \supseteq \mathbf{E} \supseteq \mathbf{F}$, $\mathbf{f(x)} \in \mathbf{F[x]}$, $\mathbf{E}$ το σώμα διαχωρισμού του $\mathbf{f(x)}$ στην επέκταση $\mathbf{L/F}$, η $\mathbf{f(x) = 0}$ είναι επιλύσιμη δια ριζικών. Τότε η $\mathcal{G}(\mathbf{E/F})$ είναι επιλύσιμη.

Αν $E = F$, η $\mathcal{G}(E/F) = \mathcal{G}(F/F) = \{id\}$ γιατί από τον ορισμό της ομάδας Galois η $\mathcal{G}(F/F)$ περιέχει τους αυτομορφισμούς του F που είναι ταυτοτικοί στο F. Η $\mathcal{G}(F/F)$ είναι τετριμμένη ομάδα και από την §107 είναι τετριμμένως επιλύσιμη.

Αν $E \supset F$, από την §164, υπάρχει σειρά σωμάτων,

$$F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_{n-1} \subseteq E_n = E, \tag{67}$$

ώστε, $E = E_n$ και για $j = 0, 1, \ldots, n-1$ η E_{j+1}/E_j είναι κανονική επέκταση του E_j με διάσταση $(E_{j+1} : E_j) = p_j$ πρώτο αριθμό. Αν $n = 0$, τότε $E = F$ άτοπο εφ΄ όσον έχουμε υποθέσει $E \supset F$.

Έστω $n \geq 1$. Επειδή το E είναι σώμα διαχωρισμού για κάποιο πολυώνυμο $f(x) \in F[x]$ από την §140 προκύπτει ότι η $E/F = E_n/E_0$ είναι κανονική επέκταση του $F = E_0$. Επειδή τα E_j είναι ενδιάμεσα σώματα των E_n, E_0 από την §140 προκύπτει ότι και οι E_n/E_j είναι κανονικές επεκτάσεις των E_j. Οπότε, από την §140 για ακόμη μία φορά προκύπτει ότι $(E_n : E_j) = |\mathcal{G}(E_n/E_j)|$. Από την §141 προκύπτει ότι υπάρχει σειρά ομάδων,

$$\{id\} = \mathcal{G}(E_n/E_n) \subseteq \mathcal{G}(E_n/E_{n-1}) \subseteq \cdots \subseteq \mathcal{G}(E_n/E_1) \subseteq \mathcal{G}(E_n/E_0) = \mathcal{G}(E/F).$$

Οπότε, για $j = 0, 1, \ldots, n-1$ από τα προηγούμενα έχουμε, E_n/E_j κανονική επέκταση του E_j, E_{j+1}/E_j κανονική επέκταση του E_j, (από τις ιδιότητες της (67)), και E_{j+1} ενδιάμεσο σώμα των E_n και E_j. Από την §149, για $E = E_n$, $K = E_{j+1}$, $F = E_j$ προκύπτει ότι, η $\mathcal{G}(E_n/E_{j+1})$ είναι κανονική υποομάδα της $\mathcal{G}(E_n/E_j)$. Ο δείκτης της $\mathcal{G}(E_n/E_{j+1})$ στην $\mathcal{G}(E_n/E_j)$ είναι,

$$\begin{aligned}[\mathcal{G}(E_n/E_j) : \mathcal{G}(E_n/E_{j+1})] &\overset{\S 90}{=} \frac{|\mathcal{G}(E_n/E_j)|}{|\mathcal{G}(E_n/E_{j+1})|} = \frac{(E_n : E_j)}{(E_n : E_{j+1})} \overset{\S 49}{=} \\ &= \frac{(E_n : E_{j+1})\,(E_{j+1} : E_j)}{(E_n : E_{j+1})} = (E_{j+1} : E_j) = p_j,\end{aligned}$$

πρώτος αριθμός. Από την §107, η $\mathcal{G}(E_n/E_0) = \mathcal{G}(E/F)$ είναι επιλύσιμη και το συμπέρασμα προκύπτει.

Επιλυσιμότητα δια Ριζικών Πολυωνυμικών Εξισώσεων Εφαρμογές

§166. Τώρα έχουμε ένα ικανό και αναγκαίο κριτήριο ώστε να μπορούμε να απαντήσουμε κατά πόσο μία πολυωνυμική εξίσωση με συντελεστές από κάποιο σώμα F χαρακτηριστικής 0 είναι επιλύσιμη δια ριζικών. Το ερώτημα όμως είναι, πώς εφαρμόζεται στην πράξη ένα τέτοιο κριτήριο;

Σύμφωνα με όσα παραθέσαμε στις προηγούμενες ενότητες, για να αποφανθούμε κατά πόσο μία πολυωνυμική εξίσωση με συντελεστές από κάποιο σώμα F χαρακτηριστικής 0 είναι επιλύσιμη δια ριζικών πρέπει η ομάδα Galois του πολυωνύμου της εξίσωσης να είναι επιλύσιμη. Άρα, το ερώτημα της επιλυσιμότητας δια ριζικών ανάγεται στην δυνατότητα εύρεσης της ομάδας Galois του πολυωνύμου της εξίσωσης.

Έστω E το σώμα διαχωρισμού του πολυωνύμου της εξίσωσης σε μία επέκταση L/F του F που περιέχει τις ρίζες του πολυωνύμου αυτού. Εφ΄ όσον η ομάδα Galois ενός πολυωνύμου έχει ως στοιχεία της τους αυτομορφισμούς του E που είναι ταυτοτικοί στο F, οδηγούμαστε στο να πρέπει να προσδιορίσουμε την δομή του E που όπως ξέρουμε προκύπτει από το F με προσάρτηση των ριζών του πολυωνύμου. Δηλαδή, οδηγούμαστε στο συμπέρασμα ότι πρέπει να γνωρίζουμε τις ρίζες του πολυωνύμου.

Αυτό φυσικά είναι αντιφατικό διότι αν γνωρίζουμε τις ρίζες του πολυωνύμου δεν χρειάζεται να ασχοληθούμε με κάποιο επιπλέον κριτήριο για να συμπεράνουμε κατά πόσο αυτές εκφράζονται δια ριζικών. Αυτή η φαινομενική αντίφαση αρχικά, (μέσα του 19ου αιώνα), οδήγησε την Μαθηματική κοινότητα στο να είναι επιφυλακτική απέναντι στην χρησιμότητα του ικανού και αναγκαίου κριτηρίου που διατυπώνει η θεωρία Galois σε σχέση με την επιλυσιμότητα δια ριζικών πολυωνυμικών εξισώσεων.

Στην πορεία όμως, η θεωρία Galois αναπτύχθηκε, μετασχηματίσθηκε και απετέλεσε χρήσιμο εργαλείο για πολλούς κλάδους της Άλγεβρας όπως ο αναγνώστης μπορεί να δει στην βιβλιογραφία. Επιπλέον, σε ότι αφορά την εύρεση της ομάδας Galois ενός πολυωνύμου, στο [**7**] της βιβλιογραφίας παρατίθεται αλγόριθμος που αποδεικνύει ότι, «θεωρητικώς» μπορούμε να βρούμε την ομάδα Galois ενός πολυωνύμου χωρίς να γνωρίζουμε τις ρίζες του.

Γράφουμε «θεωρητικώς» γιατί στην πράξη η εφαρμογή του αλγορίθμου αυτού απαιτεί πολύ μεγάλη υπολογιστική δύναμη γεγονός, που τον καθιστά όχι πρακτικώς εφαρμόσιμο ακόμη και για πολυώνυμα που έχουν σχετικά μικρούς βαθμούς. Όμως η ύπαρξη του αλγορίθμου αυτού αποδεικνύει ότι το πρόβλημα της εύρεσης της ομάδας Galois ενός πολυωνύμου, χωρίς την προηγούμενη γνώση των ριζών του, είναι επιλύσιμο και η εφαρμογή της λύσης αυτής απλώς εξαρτάται από την υπολογιστική δύναμη που διαθέτει κάποιος.

Στην πορεία αναπτύχθηκαν, πρακτικώς, πιο εφαρμόσιμοι αλγόριθμοι για την εύρεση της ομάδας Galois ενός πολυωνύμου όταν το πολυώνυμο αυτό έχει συντελεστές από συγκεκριμένα σώματα, όπως το $\mathbb{Q}$ ή το $\mathbb{Q}(k)$ με $k \notin \mathbb{Q}$, [**10**].

Από τα Μαθηματικά της δευτεροβάθμιας εκπαίδευσης γνωρίζουμε πως όλες οι πολυωνυμικές εξισώσεις 1ου έως και τετάρτου βαθμού με συντελεστές ρητούς

είναι επιλύσιμες δια ριζικών. Είναι εύλογο να τεθεί το ερώτημα, είναι όλες οι πολυωνυμικές εξισώσεις με συντελεστές από κάποιο σώμα επιλύσιμες δια ριζικών; Η κοινή λογική μας λέει πως κάτι τέτοιο μάλλον είναι αδύνατο. Θα παραθέσουμε αμέσως μετά ένα αποτέλεσμα που δηλώνει ότι υπάρχουν πολυωνυμικές εξισώσεις με συντελεστές ρητούς που δεν είναι επιλύσιμες δια ριζικών.

§167. Έστω $\mathbf{p(x)}$ ανάγωγο πολυώνυμο του $\mathbb{Q}[\mathbf{x}]$, βαθμού $\mathbf{q}$, με $\mathbf{q}$ πρώτο αριθμό και $\mathbf{q-2}$ το πλήθος πραγματικές ρίζες. Η ομάδα Galois του $\mathbf{p(x)}$ στο $\mathbb{Q}$ είναι η $\mathbf{S_q}$.

Από την §71 το $p(x)$ έχει διακεκριμένες ρίζες. Αφού οι $q-2$ το πλήθος από αυτές είναι πραγματικές οι υπόλοιπες δύο είναι συζυγής μιγαδικές. Έστω k_1, k_2 οι συζυγής μιγαδικές και $k_3, \ldots, k_q$ οι πραγματικές ρίζες του $p(x)$. Από το Θεμελιώδες Θεώρημα της Άλγεβρας, η επέκταση $\mathbb{C}/\mathbb{Q}$ περιέχει τις ρίζες όλων των πολυωνύμων με ρητούς συντελεστές. Άρα, από την §60 το σώμα διαχωρισμού του $p(x)$ στην επέκταση $\mathbb{C}/\mathbb{Q}$ είναι το $E = \mathbb{Q}(k_1, \ldots, k_q)$. Μπορούμε να δουλέψουμε με το E γιατί από την §62, αυτό είναι ισομορφικό με κάθε σώμα διαχωρισμού του $p(x)$ σε οποιαδήποτε άλλη επέκταση του $\mathbb{Q}$ που περιέχει τις ρίζες του $p(x)$.

Από τις §121, §122, η ομάδα Galois του $p(x)$ στο $\mathbb{Q}$ είναι η $\mathcal{G}(E/\mathbb{Q})$. Από το τελευταίο συμπέρασμα της απόδειξης της §124 η $\mathcal{G}(E/\mathbb{Q})$ έχει πεπερασμένη τάξη, έστω μ. Για $j = 1, 2, \ldots, \mu$ θεωρούμε τα στοιχεία τ_j της $\mathcal{G}(E/\mathbb{Q})$ καθώς και το τυχαίο στοιχείο τ επίσης της $\mathcal{G}(E/\mathbb{Q})$. Επειδή $\tau_j \neq \tau_\ell$ προκύπτει $\tau\,\tau_j \neq \tau\,\tau_\ell$ για κάθε $j, \ell = 1, 2, \ldots, \mu$ και $j \neq \ell$. Τα $\tau\,\tau_j$ ως «γινόμενα» στοιχείων της $\mathcal{G}(E/\mathbb{Q})$ είναι στοιχεία της $\mathcal{G}(E/\mathbb{Q})$ και διακεκριμένα μεταξύ τους. Έτσι,

$$\mathcal{G}(E/\mathbb{Q}) = \{\tau_1, \tau_2, \ldots, \tau_\mu\} = \{\tau\,\tau_1, \tau\,\tau_2, \ldots, \tau\,\tau_\mu\}.$$

Άρα η δράση ενός στοιχείου της $\mathcal{G}(E/\mathbb{Q})$ σε όλα τα στοιχεία της $\mathcal{G}(E/\mathbb{Q})$ μας δίνει εκ' νέου τα στοιχεία της $\mathcal{G}(E/\mathbb{Q})$ με διαφορετική ενδεχομένως σειρά δηλαδή, το $\tau\,\tau_j$ είναι το τ_ℓ με ενδεχομένως $j \neq \ell$.

Έστω k_i ρίζα του $p(x)$. Οι εικόνες $\tau_j(k_i)$ της k_i μέσω όλων των στοιχείων τ_j της $\mathcal{G}(E/\mathbb{Q})$ περιέχουν κάποιες τιμές ίδιες και κάποιες διακεκριμένες. Άρα, στη σειρά τιμών,

$$\tau_1(k_i), \tau_2(k_i), \ldots, \tau_\nu(k_i), \tag{68}$$

έστω ότι m το πλήθος από αυτές είναι οι διακεκριμένες. Τις συμβολίζουμε με k_{i_j}, $j = 1, 2, \ldots, m$. Χωρίς βλάβη της γενικότητας επανατοποθετούμε τις τιμές της (68) ώστε οι m διακεκριμένες να είναι πρώτες στην σειρά και παίρνουμε,

$$\tau_{j_1}(k_i) = k_{i_1}, \tau_{j_2}(k_i) = k_{i_2}, \ldots, \tau_{j_m}(k_i) = k_{i_m}, \tau_{j_{m+1}}(k_i), \ldots, \tau_{j_\mu}(k_i). \tag{69}$$

Τότε, από όσα προαναφέραμε και επειδή οι τ είναι ένα προς ένα, οι τιμές,

$$\begin{aligned}&(\tau\,\tau_{j_1})(k_i) = \tau(k_{i_1}), (\tau\,\tau_{j_2})(k_i) = \tau(k_{i_2}), \ldots, (\tau\,\tau_{j_m})(k_i) = \tau(k_{i_m}),\\ &(\tau\,\tau_{j_{m+1}})(k_i), \ldots, (\tau\,\tau_{j_\mu})(k_i).\end{aligned} \tag{70}$$

είναι ίδιες με τις τιμές στην σειρά τιμών (69) με ενδεχομένως διαφορετική σειρά εμφάνισης. Δηλαδή, στην σειρά τιμών (70) έχουμε μία μετάθεση της σειράς τιμών (69) και άρα μία μετάθεση των τιμών k_{i_j}, $j = 1, 2, \ldots, m$. Δηλαδή, από την (70), κάθε στοιχείο τ της $\mathcal{G}(E/\mathbb{Q})$ δρα πάνω στα k_{i_j}, $j = 1, 2, \ldots, m$ ως μετάθεσή τους.

Ένας ακόμη τρόπος για να καταλάβουμε το τελευταίο αποτέλεσμα είναι ο εξής. Από την υπόθεση τα k_{i_j}, $j = 1, 2, \ldots, m$ είναι τα μόνα διακεκριμένα στοιχεία στην σειρά τιμών (69). Ο τ είναι ένα προς ένα. Άρα, οι εικόνες $\tau(k_{i_j})$, $j = 1, 2, \ldots, m$ είναι διακεκριμένες με ενδεχομένως διαφορετική επανατοποθέτηση στην σειρά τιμών (70).

Από την απόδειξη της §124, οι εικόνες των ριζών του $p(x)$ μέσω των στοιχείων τ της $\mathcal{G}(E/\mathbb{Q})$ είναι εκ΄ νέου ρίζες του $p(x)$. Άρα, οι k_{i_j}, $j = 1, 2, \ldots, m$ είναι ρίζες του $p(x)$. Θα δείξουμε ότι,

$$\{k_{i_1}, k_{i_2}, \ldots, k_{i_m}\} = \{k_1, k_2, \ldots, k_q\}. \tag{71}$$

Θεωρούμε το πολυώνυμο,

$$h(x) = \prod_{j=1}^{m} (x - k_{i_j}) = x^m + \sum_{\nu=1}^{m} (-1)^\nu \, e_\nu(k_{i_1}, k_{i_2} \ldots, k_{i_m}) \, x^{m-\nu},$$

με $e_\nu(k_{i_1}, k_{i_2}, \ldots, k_{i_m})$ η τιμή του στοιχειώδους συμμετρικού πολυωνύμου $e_\nu(x_1, x_2, \ldots, x_m)$ στη m–άδα $(k_{i_1}, k_{i_2}, \ldots, k_{i_m})$. Έστω $\tau \in \mathcal{G}(E/\mathbb{Q})$. Τότε,

$$\tau(e_\nu(k_{i_1}, k_{i_2}, \ldots, k_{i_m})) = \tau \left(\sum_{1 \le i_1 < i_2 < \cdots < i_\nu \le m} k_{i_1} \, k_{i_2} \ldots k_{i_\nu} \right) \quad =$$

$$= \sum_{1 \le i_1 < i_2 < \cdots < i_\nu \le m} \tau(k_{i_1}) \, \tau(k_{i_2}) \ldots \tau(k_{i_\nu}) = e_\nu(\tau(k_{i_1}), \tau(k_{i_2}), \ldots, \tau(k_{i_m})) \quad =$$

$$= e_\nu(k_{i_1}, k_{i_2}, \ldots, k_{i_m}),$$

γιατί όπως προαναφέραμε τα $\tau(k_{i_1}), \tau(k_{i_2}), \ldots, \tau(k_{i_m})$ είναι μία μετάθεση των $k_{i_1}, k_{i_2}, \ldots, k_{i_m}$ και τα $e_\nu(x_1, x_2, \ldots, x_m)$ ως συμμετρικά πολυώνυμα αμετάβλητα στις μεταθέσεις m στοιχείων. Άρα, τα $e_\nu(k_{i_1}, k_{i_2}, \ldots, k_{i_m})$ παραμένουν αμετάβλητα ως προς την δράση των στοιχείων της $\mathcal{G}(E/\mathbb{Q})$ και από τις §129, §130 ανήκουν στο σταθερό σώμα της $\mathcal{G}(E/\mathbb{Q})$.

Από την §140, το E ως σώμα διαχωρισμού του $p(x) \in \mathbb{Q}[x]$ είναι κανονική επέκταση του $\mathbb{Q}$. Εκ΄ νέου από την §140, το σταθερό σώμα της $\mathcal{G}(E/\mathbb{Q})$ είναι το $\mathbb{Q}$. Από τα προηγούμενα, τα $e_\nu(k_{i_1}, k_{i_2}, \ldots, k_{i_m})$ ανήκουν στο $\mathbb{Q}$ και κατ΄ επέκταση, το $h(x) \in \mathbb{Q}[x]$.

Οι ρίζες k_{i_j} του $h(x)$ όπως προείπαμε είναι και ρίζες του $p(x)$. Το $h(x)$ είναι παράγοντας του $p(x)$ που ως ανάγωγο στο $\mathbb{Q}[x]$ επάγει ότι $p(x) = a\, h(x)$ με $a \in \mathbb{Q} - \{0\}$. Τελικά, $m = q$ και οι q το πλήθος διακεκριμένες ρίζες του $h(x)$ είναι οι q το πλήθος ρίζες του $p(x)$. Η (71) προκύπτει.

Συνέπεια της (71) είναι ότι αν k_α, k_β είναι δύο ρίζες του $p(x)$, υπάρχουν k_{i_γ}, k_{i_δ} και τ_{j_γ}, τ_{j_δ} στοιχεία της $\mathcal{G}(E/\mathbb{Q})$ ώστε,

$$\begin{aligned} k_\alpha = k_{i_\gamma} = \tau_{j_\gamma}(k_i) \quad &\text{και} \quad k_\beta = k_{i_\delta} = \tau_{j_\delta}(k_i), \\ \tau_{j_\gamma}^{-1}(k_\alpha) = k_i \quad &\text{και} \quad k_\beta = \tau_{j_\delta}(\tau_{j_\gamma}^{-1}(k_\alpha)), \\ &\qquad k_\beta = (\tau_{j_\delta} \, \tau_{j_\gamma}^{-1})(k_\alpha), \end{aligned}$$

από όπου προκύπτει ότι, επειδή το $\tau_{j_\delta} \, \tau_{j_\gamma}^{-1} \in \mathcal{G}(E/\mathbb{Q})$ ως «γινόμενο» στοιχείων της $\mathcal{G}(E/\mathbb{Q})$, για κάθε ζεύγος ριζών k_α, k_β του $p(x)$ υπάρχει στοιχείο $\tau \in \mathcal{G}(E/\mathbb{Q})$ ώστε $k_\beta = \tau(k_\alpha)$.

Τα στοιχεία του $\mathbb{C}$ γράφονται ως $a+b\,i$ με $a,b\in\mathbb{R}$. Θεωρούμε την συνάρτηση $\psi:\mathbb{C}\mapsto\mathbb{C}$ με $\psi(a+b\,i)=a-b\,i$. Αν $\psi(a_1+b_1\,i)=\psi(a_2+b_2\,i)$, τότε $a_1-b_1\,i=a_2-b_2\,i$ ή $a_1=a_2$ και $b_1=b_2$ οπότε, $a_1+b_1\,i=a_2+b_2\,i$. Η ψ είναι ένα προς ένα.

Έστω $a+b\,i\in\mathbb{C}$. Το $a-b\,i\in\mathbb{C}$ και $\psi(a-b\,i)=a+b\,i$. Η ψ είναι επί. Για τα $a+b\,i\in\mathbb{Q}$ έπεται $b=0$ οπότε, $\psi(a+b\,i)=\psi(a+0\,i)=a=a+0\,i=a+b\,i$. Η ψ είναι ταυτοτική στο $\mathbb{Q}$. Από την Θεωρία Μιγαδικών γνωρίζουμε ότι η ψ διατηρεί τις πράξεις του $\mathbb{C}$ δηλαδή, $\psi((a_1+b_1\,i)+(a_2+b_2\,i))=\psi(a_1+b_1\,i)+\psi(a_2+b_2\,i)$ και $\psi((a_1+b_1\,i)\,(a_2+b_2\,i))=\psi(a_1+b_1\,i)\,\psi(a_2+b_2\,i)$. Η ψ είναι αυτομορφισμός του $\mathbb{C}$ ταυτοτικός στο $\mathbb{Q}$.

Από την §51, το $E=\mathbb{Q}(k_1,\ldots,k_q)=(((\mathbb{Q}(k_1))(k_2))\cdots)(k_q)$. Το k_1 είναι αλγεβρικό επί του $\mathbb{Q}$ ως ρίζα του $p(x)\in\mathbb{Q}[x]$. Από την §66, τα στοιχεία του $\mathbb{Q}(k_1)$ είναι της μορφής $b(k_1)$ με $b(x)$ τα πολυώνυμα του $\mathbb{Q}[x]$.

Το k_2 είναι αλγεβρικό επί του $\mathbb{Q}(k_1)$ ως ρίζα του $p(x)\in(\mathbb{Q}(k_1))[x]$. Από την §66, τα στοιχεία του $(\mathbb{Q}(k_1))(k_2)$ είναι της μορφής $g(k_2)$ με $g(x)$ τα πολυώνυμα του $(\mathbb{Q}(k_1))[x]$. Τα πολυώνυμα του $(\mathbb{Q}(k_1))[x]$ έχουν ως συντελεστές στοιχεία του $\mathbb{Q}(k_1)$. Οπότε τα $g(k_2)$ είναι πολυωνυμικές εκφράσεις ως προς k_2 με συντελεστές πολυωνυμικές εκφράσεις ως προς k_1 με συντελεστές από το $\mathbb{Q}$. Τελικά τα στοιχεία του $(\mathbb{Q}(k_1))(k_2)$ είναι της μορφής $d(k_1,k_2)$ με $d(x_1,x_2)$ τα πολυώνυμα του $\mathbb{Q}[x_1,x_2]$.

Επαγωγικά προκύπτει ότι, τα στοιχεία του $E=(((\mathbb{Q}(k_1))(k_2))\cdots)(k_q)$ είναι της μορφής $z(k_1,k_2,\ldots,k_q)$ με $z(x_1,x_2,\ldots,x_q)$ τα πολυώνυμα του $\mathbb{Q}[x_1,x_2,\ldots,x_q]$. Δηλαδή, τα στοιχεία του E είναι της μορφής,

$$z(k_1,k_2,\ldots,k_q)=\sum_{i_1=0}^{m_1}\sum_{i_2=0}^{m_2}\cdots\sum_{i_n=0}^{m_n}a_{i_1i_2\ldots i_n}\,k_1^{i_1}\,k_2^{i_2}\,\cdots\,k_n^{i_n},$$

με $a_{i_1i_2\ldots i_n}\in\mathbb{Q}$. Επειδή οι k_1, k_2 είναι συζυγής, μπορούμε να γράψουμε,

$$z(k_1,k_2,\ldots,k_q)=\sum_{i_1=0}^{m_1}\sum_{i_2=0}^{m_2}\cdots\sum_{i_n=0}^{m_n}a_{i_1i_2\ldots i_n}\,k_1^{i_1}\,\overline{k_1}^{i_2}\,\cdots\,k_n^{i_n},$$

με $a_{i_1i_2\ldots i_n}\in\mathbb{Q}$. Θεωρούμε τον περιορισμό ψ_E του αυτομορφισμού ψ στο E. Ο ψ_E είναι ένα προς ένα ως περιορισμός συνάρτησης ένα προς ένα. Διατηρεί τις πράξεις του E επειδή το E είναι υποσώμα του $\mathbb{C}$ και ο ψ_E είναι περιορισμός αυτομορφισμού που διατηρεί τις πράξεις του $\mathbb{C}$ που είναι ίδιες με τις πράξεις του E. Έστω $z(k_1,k_2,\ldots,k_q)$ στοιχείο του E με,

$$\begin{aligned}z(k_1,k_2,\ldots,k_q)&=\sum_{i_1=0}^{m_1}\sum_{i_2=0}^{m_2}\cdots\sum_{i_n=0}^{m_n}a_{i_1i_2\ldots i_n}\,k_1^{i_1}\,k_2^{i_2}\,\cdots\,k_n^{i_n}=\\&=\sum_{i_1=0}^{m_1}\sum_{i_2=0}^{m_2}\cdots\sum_{i_n=0}^{m_n}a_{i_1i_2\ldots i_n}\,k_1^{i_1}\,\overline{k_1}^{i_2}\,\cdots\,k_n^{i_n}.\end{aligned}$$

Θεωρούμε το στοιχείο του E,

$$\theta(k_1,k_2,\ldots,k_q)=\sum_{i_1=0}^{m_1}\sum_{i_2=0}^{m_2}\cdots\sum_{i_n=0}^{m_n}a_{i_1i_2\ldots i_n}\,k_2^{i_1}\,k_1^{i_2}\,\cdots\,k_n^{i_n}=$$

$$= \sum_{i_1=0}^{m_1} \sum_{i_2=0}^{m_2} \cdots \sum_{i_n=0}^{m_n} a_{i_1 i_2 \ldots i_n} \, \overline{k_1}^{i_1} \, k_1^{i_2} \, \cdots \, k_n^{i_n}.$$

Τότε επειδή, το $a_{i_1 i_2 \ldots i_n} \in \mathbb{Q}$ και ο ψ_E είναι ταυτοτικός στο $\mathbb{Q}$ ως περιορισμός αυτομορφισμού ταυτοτικού στο $\mathbb{Q}$, τα $k_3, \ldots, k_q \in \mathbb{R}$ με $\psi(k_j) = \psi(k_j + 0\,i) = k_j - 0\,i = k_j$, $j = 3, 4, \ldots, q$ και επιπλέον ο ψ_E διατηρεί τις πράξεις του E παίρνουμε,

$$\begin{aligned}
\psi_E(\theta(k_1, k_2, \ldots, k_q)) &= \psi_E \left(\sum_{i_1=0}^{m_1} \sum_{i_2=0}^{m_2} \cdots \sum_{i_n=0}^{m_n} a_{i_1 i_2 \ldots i_n} \, \overline{k_1}^{i_1} \, k_1^{i_2} \, \cdots \, k_n^{i_n} \right) \\
&= \sum_{i_1=0}^{m_1} \sum_{i_2=0}^{m_2} \cdots \sum_{i_n=0}^{m_n} \psi(a_{i_1 i_2 \ldots i_n}) \, \psi(\overline{k_1}^{i_1}) \, \psi(k_1^{i_2}) \, \cdots \, \psi(k_n^{i_n}) = \\
&= \sum_{i_1=0}^{m_1} \sum_{i_2=0}^{m_2} \cdots \sum_{i_n=0}^{m_n} a_{i_1 i_2 \ldots i_n} \, \psi(\overline{k_1})^{i_1} \, \psi(k_1)^{i_2} \, \cdots \, \psi(k_n)^{i_n} = \\
&= \sum_{i_1=0}^{m_1} \sum_{i_2=0}^{m_2} \cdots \sum_{i_n=0}^{m_n} a_{i_1 i_2 \ldots i_n} \, \overline{\overline{k_1}}^{i_1} \, \overline{k_1}^{i_2} \, \cdots \, k_n^{i_n} = \\
&= \sum_{i_1=0}^{m_1} \sum_{i_2=0}^{m_2} \cdots \sum_{i_n=0}^{m_n} a_{i_1 i_2 \ldots i_n} \, k_1^{i_1} \, \overline{k_1}^{i_2} \, \cdots \, k_n^{i_n} = \\
&= z(k_1, k_2, \ldots, k_q).
\end{aligned}$$

Δείξαμε ότι ο ψ_E είναι επί του E. Συνολικά ο ψ_E είναι ένας αυτομορφισμός του E ταυτοτικός επί του $\mathbb{Q}$. Ο ψ_E είναι στοιχείο της $\mathcal{G}(E/\mathbb{Q})$ που δρώντας πάνω στις $k_1, k_2 = \overline{k_1}, \ldots, k_q$ μας δίνει $\overline{k_1} = k_2, \overline{k_2} = k_1, k_3, \ldots, k_q$. Από την §124 τα στοιχεία της $\mathcal{G}(E/\mathbb{Q})$ είναι στοιχεία της S_q δηλαδή, μεταθέσεις των $k_1, k_2, \ldots, k_q$. Ο ψ_E είναι μία αντιμετάθεση εφόσον αντιμεταθέτει τις ρίζες k_1, k_2 και αφήνει τις υπόλοιπες αμετάβλητες. Μπορούμε να ταυτίσουμε τον ψ_E με τον 2 κύκλο $(1\,2)$.

Θεωρούμε το σύνολο $\Sigma = \{1, 2, \ldots, q\}$ και την σχέση $(\sim)$ μεταξύ των στοιχείων του $\sum$ που ορίζεται ως, $i \sim j$ αν και μόνο αν $i = j$ ή αν $i \neq j$, υπάρχει στοιχείο $\tau \in \mathcal{G}(E/\mathbb{Q})$ ώστε $\tau(k_i) = k_j$, $\tau(k_j) = k_i$ και $\tau(k_\mu) = k_\mu$ για $\mu \neq i, j$. Δηλαδή, $i \sim j$ αν και μόνο αν $i = j$ ή αν $i \neq j$, υπάρχει στοιχείο $\tau \in \mathcal{G}(E/\mathbb{Q})$ που είναι αντιμετάθεση των k_i, k_j ή ισοδυνάμως των i, j. Μπορούμε λοιπόν να επαναδιατυπώσουμε την συνθήκη ως εξής, $i \sim j$ αν και μόνο αν $i = j$ ή αν $i \neq j$ ο 2 κύκλος $(i\,j) \in \mathcal{G}(E/\mathbb{Q})$. Θα δείξουμε ότι η $(\sim)$ είναι σχέση ισοδυναμίας.

- Η $(\sim)$ είναι αυτοπαθής αφού, $i \sim i$ γιατί $i = i$.
- Η $(\sim)$ είναι συμμετρική αφού, $i \sim j$ σημαίνει είτε $i = j$ οπότε και $j = i$ δηλαδή, $j \sim i$ είτε, $i \neq j$ και $(i\,j) \in \mathcal{G}(E/\mathbb{Q})$ οπότε, $(j\,i) = (i\,j)^{-1} \in \mathcal{G}(E/\mathbb{Q})$ που επάγει $j \sim i$.
- Η $(\sim)$ είναι μεταβατική αφού, $i \sim j$ και $j \sim t$ σημαίνει,
  - είτε $i = j$ και $j = t$ οπότε, $i = t$ και $i \sim t$,
  - είτε $i = j$ και $j \neq t$ οπότε, $(j\,t) \in \mathcal{G}(E/\mathbb{Q})$ που επάγει $(i\,t) \in \mathcal{G}(E/\mathbb{Q})$ και $i \sim t$,

– είτε $i \neq j$ και $j = t$ οπότε, $(i\,j) \in \mathcal{G}(E/\mathbb{Q})$ που επάγει $(i\,t) \in \mathcal{G}(E/\mathbb{Q})$ και $i \sim t$,

– είτε $i \neq j$ και $j \neq t$ οπότε, $(i\,j), (j\,t) \in \mathcal{G}(E/\mathbb{Q})$ και

$$(i\,t) = (j\,t)\,(i\,j)\,(j\,t) \in \mathcal{G}(E/\mathbb{Q}),$$

ως «γινόμενο» στοιχείων της $\mathcal{G}(E/\mathbb{Q})$ και $i \sim t$.

Τα στοιχεία του Σ, μέσω της $(\sim)$, κατανέμονται σε ξένες μεταξύ τους κλάσεις ισοδυναμίας τις οποίες και συμβολίζουμε με c_i. Θεωρούμε τις c_i, c_j. Έστω $t \in c_i$ και $t \neq i$. Από τα προαναφερθέντα σχετικώς με την (71), υπάρχει $\chi \in \mathcal{G}(E/\mathbb{Q})$ ώστε $\chi(k_i) = k_j$. Θεωρούμε την τιμή $\chi(k_t)$ του χ στην ρίζα k_t του $p(x)$. Από την απόδειξη της §124, η $\chi(k_t)$ είναι ρίζα του $p(x)$. Επειδή $t \neq i$ έπεται και $k_t \neq k_i$ οπότε και $\chi(k_t) \neq \chi(k_i) = k_j$ λόγω του ένα προς ένα του χ.

Θέτουμε $k_s = \chi(k_t)$ που όπως προείπαμε είναι ρίζα του $p(x)$ διαφορετική της k_j. Αφού $t \in c_i$ και $t \neq i$ έπεται ότι ο 2 κύκλος $(i\,t) \in \mathcal{G}(E/\mathbb{Q})$ δηλαδή, υπάρχει στοιχείο $\tau \in \mathcal{G}(E/\mathbb{Q})$ ώστε, $\tau(k_i) = k_t$, $\tau(k_t) = k_i$ και $\tau(k_\mu) = k_\mu$ για $\mu \neq i, t$. Θεωρούμε το $\chi\,\tau\,\chi^{-1}$ στοιχείο της $\mathcal{G}(E/\mathbb{Q})$ ως «γινόμενο» στοιχείων της $\mathcal{G}(E/\mathbb{Q})$. Για τον $\chi\,\tau\,\chi^{-1}$ ισχύει,

- $(\chi\,\tau\,\chi^{-1})(k_s) = \chi(\tau(\chi^{-1}(k_s))) = \chi(\tau(k_t)) = \chi(k_i) = k_j$.
- $(\chi\,\tau\,\chi^{-1})(k_j) = \chi(\tau(\chi^{-1}(k_j))) = \chi(\tau(k_i)) = \chi(k_t) = k_s$.
- Για $\ell \neq j, s$ έπεται $k_\ell \neq k_j, k_s$ ή, $k_\ell \neq \chi(k_i), \chi(k_t)$ ή, $\chi^{-1}(k_\ell) \neq k_i, k_t$. Από την απόδειξη της §124 και επειδή ο $\chi^{-1} \in \mathcal{G}(E/\mathbb{Q})$, η εικόνα $\chi^{-1}(k_\ell)$ είναι κάποια ρίζα k_μ του $p(x)$. Οπότε, $k_\mu \neq k_i, k_t$ ή, $\mu \neq i, t$ και, $(\chi\,\tau\,\chi^{-1})(k_\ell) = \chi(\tau(\chi^{-1}(k_\ell))) = \chi(\tau(k_\mu)) = \chi(k_\mu) = k_\ell$.

Αποδείξαμε ότι για το στοιχείο $\chi\,\tau\,\chi^{-1}$ της $\mathcal{G}(E/\mathbb{Q})$ ισχύει, $\chi\,\tau\,\chi^{-1}(k_j) = k_s$, $\chi\,\tau\,\chi^{-1}(k_s) = k_j$ και $\chi\,\tau\,\chi^{-1}(k_\ell) = k_\ell$ για $\ell \neq j, s$. Δηλαδή, ο $\chi\,\tau\,\chi^{-1} \in \mathcal{G}(E/\mathbb{Q})$ είναι ο 2 κύκλος $(j\,s)$ οπότε, $j \sim s$. Άρα, $s \in c_j$.

Από την έως τώρα ανάλυσή μας συμπεραίνουμε ότι, για κάθε δύο κλάσεις ισοδυναμίας c_i, c_j υπάρχει στοιχείο $\chi \in \mathcal{G}(E/\mathbb{Q})$ ώστε για τις ρίζες k_i, k_j να ισχύει $\chi(k_i) = k_j$ και για κάθε στοιχείο $t \in c_i$ υπάρχει στοιχείο $s \in c_j$ ώστε $\chi(k_t) = k_s$ με k_i, k_j, k_t, k_s ρίζες του $p(x)$. Με ακριβώς ανάλογο τρόπο μπορούμε να συμπεράνουμε ότι, για κάθε δύο κλάσεις ισοδυναμίας c_j, c_i υπάρχει στοιχείο $\chi^{-1} \in \mathcal{G}(E/\mathbb{Q})$ ώστε για τις ρίζες k_j, k_i να ισχύει $\chi^{-1}(k_j) = k_i$ και για κάθε στοιχείο $s \in c_j$ υπάρχει στοιχείο $t \in c_i$ ώστε $\chi^{-1}(k_s) = k_t$ με k_i, k_j, k_t, k_s ρίζες του $p(x)$.

Τελικά, για κάθε δύο κλάσεις ισοδυναμίας c_i, c_j υπάρχει μία ένα προς ένα και επί αντιστοιχία ανάμεσα στα στοιχεία τους και οι c_i, c_j έχουν το ίδιο πλήθος στοιχείων. Όλα τα στοιχεία του Σ κατανέμονται στις κλάσεις ισοδυναμίας c_i που όπως προείπαμε είναι ξένες μεταξύ τους και πεπερασμένου πλήθους εφ΄ όσον το Σ έχει πεπερασμένου πλήθους στοιχεία.

Έστω ότι το πλήθος των c_i είναι $\omega \in \mathbb{N} - \{0\}$ και κάθε κλάση περιέχει $\lambda \in \mathbb{N} - \{0\}$ το πλήθος στοιχεία. Επειδή, $\cup_{i=1}^{\omega} c_i = \Sigma$ έπεται ότι, $\sum_{i=1}^{\omega} |c_i| = |\Sigma|$ ή $\omega\,\lambda = q$. Η τελευταία ισότητα επάγει ότι, είτε $\omega = q$ και $\lambda = 1$ είτε, $\omega = 1$ και $\lambda = q$. $\omega = q$ και $\lambda = 1$ σημαίνει ότι έχουμε q το πλήθος κλάσεις με ένα στοιχείο η κάθε μία. Όμως σε όσα προηγήθηκαν αποδείξαμε ότι ο $\psi_E = (1\,2)$

είναι στοιχείο της $\mathcal{G}(E/\mathbb{Q})$. Αυτό, από τον ορισμό της ($\sim$) σημαίνει ότι, $1 \sim 2$ και τα 1, 2 ανήκουν στην ίδια κλάση. Άρα, δεν μπορεί όλες οι κλάσεις να έχουν ένα στοιχείο και το συμπέρασμα $\omega = q$ και $\lambda = 1$ δεν ισχύει.

Οπότε, ισχύει $\omega = 1$ και $\lambda = q$ δηλαδή, όλο το Σ είναι μία κλάση και όλα τα στοιχεία του είναι ισοδύναμα μεταξύ τους. Από τον ορισμό της ($\sim$), αυτό σημαίνει πως όλοι οι 2 κύκλοι που δημιουργούνται από τα $1, 2, \ldots, q$ ανήκουν στην $\mathcal{G}(E/\mathbb{Q})$. Οπότε, επειδή η $\mathcal{G}(E/\mathbb{Q})$ είναι ομάδα ως προς την πράξη «γινόμενο», και όλα τα «γινόμενα» των 2 κύκλων που δημιουργούνται από τα $1, 2, \ldots, q$ ανήκουν στην $\mathcal{G}(E/\mathbb{Q})$. Από τις §111, §112, §113 προκύπτει ότι τα στοιχεία της S_q γράφονται ως «γινόμενο» των 2 κύκλων που δημιουργούνται από τα $1, 2, \ldots, q$. Άρα, όλα τα στοιχεία της S_q είναι και στοιχεία της $\mathcal{G}(E/\mathbb{Q})$ ή ότι $S_q \subseteq \mathcal{G}(E/\mathbb{Q})$.

Από την §124, $\mathcal{G}(E/\mathbb{Q}) \subseteq S_q$. Τελικά $\mathcal{G}(E/\mathbb{Q}) = S_q$ και το συμπέρασμα προκύπτει.

§168. Το συμπεράσματα των §118, §154, §165, §167 επάγουν ότι υπάρχουν πολυώνυμα του $\mathbb{Q}[x]$ που η ομάδα Galois τους δεν είναι επιλύσιμη οπότε, και οι πολυωνυμικές εξισώσεις που αυτά επάγουν δεν είναι επιλύσιμες δια ριζικών. Π.χ. το πολυώνυμο $p(x) = x^5 - 2\,x^3 - 2\,x - 2$ ικανοποιεί τις προϋποθέσεις της §167 και η εξίσωση $p(x) = 0$ δεν είναι επιλύσιμη δια ριζικών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

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

[2] Edwards H.M., *"Galois Theory"*, Springer, 1984, Rep., 1994.

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

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

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

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

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

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

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

[10] Hulpke A., *"Techniques for the Computation of Galois Groups"*, Algorithmic Algebra and Number Theory, Springer Verlag, 1999.