ΕΠΕΚΤΑΣΕΙΣ ΣΩΜΑΤΟΣ

1. Προκαταρκτικά. Σώμα = Αντιμεταθετικό σώμα, χαρακτηριστικής μηδενός. Τα σώματα αυτά καλούνται και ***αριθμητικά σώματα.*** Θα τα συμβολίζουμε με τα γράμματα F, F, L κλπ.
Έστω ότι κάποια ανάγκη μας επιβάλει την χρησιμοποίηση νέων συμβόλων σε συνάρτηση με τα στοιχεία ενός σώματος. Παράδειγμα: Το σώμα των ρητών $\mathbb{Q}$, νέο σύμβολο το $\sqrt{2}$, επιβαλομένη ανάγκη, αυτή που περιγράφεται στην ενότητα "Γεωμετρικές Κατασκευές".
Η αντιμετώπιση της ανάγκης αυτής, γίνεται με την επέκταση του αρχικού σώματος F, (π.χ. του $\mathbb{Q}$), επέκταση, που οδηγεί στην κατασκευή του σώματος $L = F(a)$ [a το νέο στοιχείο, π.χ. του $\mathbb{Q}(\sqrt{2})$]. Το σώμα αυτό L περιέχει ως υπόσωμα το F, και, επίσης, περιέχει όποιο άλλο στοιχείο απαιτείται για να λητουργεί ως σώμα με πράξεις τις πράξεις του F, κατάλληλα τροποποιημένες, ώστε να ισχύουν και για τα πρόσθετα στοιχεία που έχει το L.

ΠΑΡΑΔΕΙΓΜΑ. Ξεκινάμε από το σώμα F. Επιλέγουμε τυχόν στοιχείο $k \in F$, $k > 0$, εισάγουμε το νέο σύμβολο $\sqrt{k}$ που να έχει την επιθυμητή ιδιότητα $\left(\sqrt{k}\right)^2 = k$, εφ' όσον βέβαια στοιχείο του F με την ιδιότητα αυτή δεν υπάρχει, και στην συνέχεια θεωρούμε και όλα τα στοιχεία της μορφής $a + b\sqrt{k}$, $a, b \in F$ και στην συνέχεια σχηματίζουμε το σύνολο $L = F \cup \left\{a + b\sqrt{k}\right\}$. Είναι, $1 \in F$, άρα και $1 \in L$. Επεκτείνουμε τις πράξεις του F έτσι ώστε αυτές να ισχύουν και εν L, και μάλιστα να καθιστούν το σύνολο L σώμα. Τούτο γίνεται αν ορίσουμε την πρόσθεση:
$(a + b\sqrt{k}) \pm (c + d\sqrt{k}) = (a \pm b) + (b \pm d)\sqrt{k}$, και τον πολλαπλασιασμό:
$(a + b\sqrt{k})(c + d\sqrt{k}) = (ac + bdk) + (ad + bc)\sqrt{k}$. Για την διαίρεση έχουμε,
$\frac{a + b\sqrt{k}}{c + d\sqrt{k}} = \frac{a + b\sqrt{k}}{c + d\sqrt{k}} \frac{c - d\sqrt{k}}{c - d\sqrt{k}} = \left(\frac{ac - bdk}{c^2 - d^2k}\right) + \left(\frac{bc - ad}{c^2 - d^2k}\right)\sqrt{k}$ στοιχείο και αυτό της προβλεπόμενης μορφής. Βέβαια, θα πρέπει $c + d\sqrt{k} \neq 0$. Το αντίστροφο, λοιπόν, του στοιχείου $0 \neq a + b\sqrt{k} \in L$, είναι το στοιχείο $\frac{a - b\sqrt{k}}{a^2 - b^2k}$ του L.

2. Επεκτάσεις σώματος. Ένα σώμα L καλείται ***επέκταση*** του σώματος F, ανν το F είναι υπόσωμα του L. Γράφουμε, $F \subseteq L$. Το L είναι δυνατόν να θεωρηθεί και ως ανυσματικός χώρος επί του F με πρόσθεση την πρόσθεση του L και μονόμετρο πολλαπλασιασμό $F \times L \to L$ τον περιορισμό του πολλαπλασιασμού του L στο F.
Λέμε ότι το L είναι μία ***πεπερασμένη επέκταση*** του F, αν και μόνον αν, υπάρχουν $a_1, a_2, \ldots, a_n \in L$ τέτοια ώστε κάθε $b \neq a_i$, $b \in L$ να γράφεται ως μία γραμμική έκφρασις $b = \beta_1 a_1 + \beta_2 a_2 + \ldots + \beta_n a_n$, $\beta_i \in F$ των a_i, που καλούνται και βάση της επέκτασης L, πάνω στο σώμα F. Το πλήθος n των a_i καλείται βαθμός $[L : F]$ της επέκτασης L του F. (**Σημείωση.** Ο βαθμός $[L : F]$ δεν είναι τίποτα άλλο, από την διάσταση του διανυσματικού χώρου L). Παρατηρούμε ότι, $[L : F] = 1$ ανν $L = F$. Έστω $n = [L : F]$.
Επειδή σε έναν ανυσματικό χώρο με διάσταση n τα $n + 1$ διανύσματα είναι γραμμικά εξαρτημένα, αν $a, a^2, \ldots, a^n \in L$, υπάρχουν τότε $\beta_0, \beta_1, \beta_2, \ldots, \beta_n \in F$, τέτοια ώστε να ισχύει η $\beta_0 + \beta_1 a + \beta_2 a^2 + \ldots + a^n \beta_n = 0$
Αντίστοιχες έννοιες προκύπτουν αν αντικαταστήσουμε την έννοια "σώμα F", με την έννοια "δακτύλιος F".

Απλή αλγεβρική επέκταση του σώματος F, καλείται το σώμα $L = F(a)$, $a \notin F$. Ο όρος "απλή" είναι φανερό γιατί τίθεται. Ο όρος "αλγεβρική" δικαιολογείται από το Θεώρημα του FronecFer (βλέπε ενότητα "Πολυωνυμικός δακτύλιος" §10.

Θεώρημα 1. Το $f \in F[x]$ είναι ελάχιστο πολυώνυμο του a επί το F, ανν το f είναι ανάγωγο εν $F[x]$. (Βλέπε ενότητα "Πολυωνυμικός δακτύλιος" §10)

Απόδειξη. Αν το f ελάχιστο, τότε είναι και ανάγωγο, μια και αν $f = gh$, $g, h \in F[x]$, το a θα είναι ρίζα είτε του f είτε του g, και ο βαθμός αυτών είναι μικρότερος του ελαχίστου βαθμού του f, πράγμα άτοπον.

Αντίθετα, έστω το f ανάγωγο εν $F[x]$, και g το ελάχιστο πολυώνυμο του a επί το F. Διαιρούμε το f με το g και έχουμε, $f = qg + r$. Είναι, $f(a) = g(a) = 0$, οπότε και $r(a) = 0$. Όμως ο βαθμός του r είναι μικρότερος του βαθμού του g. Το r είναι, λοιπόν, αναγκαστικά το μηδενικό πολυώνυμο, και έτσι οδηγούμεθα εις το άτοπον $f = qg$.

ΠΑΡΑΔΕΙΓΜΑ. 1) Το σώμα $Q\left(\sqrt{k}\right) = \left\{\beta_1 + \beta_2\sqrt{k}\right\}$, $\beta_1, \beta_2 \in Q$, $\sqrt{k} \notin Q$ είναι μία πεπερασμένη επέκταση του σώματος Q των ρητών. Τα στοιχεία $1, \sqrt{k} \in Q(\sqrt{k})$, αποτελούν βάση του διανυσματικού χώρου $Q(\sqrt{k})$. Άρα $\left[Q\left(\sqrt{k}\right) : Q\right] = 2$ είναι ο βαθμός της επέκτασης.. Στην περίπτωση, που $\sqrt{k} \in Q$, $Q(\sqrt{k}) = Q$ και ο βαθμός του Q είναι 1. Η $Q(\sqrt{k})$, $\sqrt{k} \notin Q$ καλείται ***τετραγωνική επέκτασις*** του σώματος των ρητών.

2) Το σώμα $Q\left(\sqrt{2}\right) = \left\{\beta_1 + \beta_2\sqrt{k}\right\}$, $\beta_1, \beta_2 \in Q$

Συμβολισμός. Με $L = F(a_1, a_2, \ldots, a_n)$ συμβολίζουμε την ***ελαχίστη πεπερασμένη επέκταση,*** που περιέχει τα στοιχεία $a_1, a_2, \ldots, a_n \in L$. Με τον όρο ελαχίστη επέκταση, νοούμε ότι, κάθε άλλη επέκταση του F, η οποία περιέχει τα στοιχεία a_i, περιέχει και το L. Μπορούμε συνεπώς να λέμε ότι, το L είναι η τομή όλων των επεκτάσεων του F, που περιέχουν τα στοιχεία a_i. Με $L = F(a_1, a_2, \ldots, a_n)$ συμβολίζουμε την ***ελαχίστη πεπερασμένη επέκταση*** L του δακτυλίου F.

ΠΑΡΑΔΕΙΓΜΑ. Είναι, $Q\left(\sqrt{2}, \sqrt{3}\right) : Q = 4$, μια και τα στοιχεία 1, $\sqrt{2}$, $\sqrt{3}$ και $\sqrt{6}$, αποτελούν βάση του $Q\left(\sqrt{2}, \sqrt{3}\right)$.

Πρόταση 1. Αν $L = F(a_1, a_2, \ldots, a_n)$ μία πεπερασμένη επέκταση του σώματος F, τότε μπορούμε να βρούμε ένα στοιχείο $a \in L$, τέτοιο ώστε, $L = F(a)$, ώστε το L να είναι απλή επέκταση του σώματος F.

Απόδειξη. Θεωρούμε την περίπτωση $L = F(a_1, a_2)$. Έστω τα ελάχιστα πολυώνυμα $f_1 \in F(a_1)$ και $f_2 \in F(a_2)$. Τα πολυώνυμα αυτά, είναι (βλέπε ενότητα "Πολυωνυμικός δακτύλιος" §10) ανάγωγα, και έχουν απλές ρίζες, μία των οποίων είναι η a_1 (αντ. a_2). Έστω, αντιστοίχως οι ρίζες τους, $a_1 = b_1, b_2, \ldots, b_n$ και $a_2 = c_1, c_2, \ldots, c_m$. Θεωρούμε τα στοιχεία $\dfrac{b_i - a_1}{a_2 - c_j}$, $1 \le i \le n$, $2 \le j \le m$. Το πλήθος των στοιχείων αυτών είναι $n(m-1)$ και, συνεπώς, μέσα στο σώμα F, υπάρχουν στοιχεία c διαφορετικά απ' αυτά. Θέτουμε $a = a_1 + ca_2$ Είναι, $a \ne b_i + cc_j$ για όλα τα $1 \le i \le n$ και $2 \le j \le m$. Επειδή $a \in F$, ο a

είναι αλγεβρικός αριθμός. Η απλή αλγεβρική επέκταση $F(a)$ που παράγεται απ' αυτόν είναι, λοιπόν, $F(a) \subseteq L$. Θεωρούμε, τώρα, το πολυώνυμο $g(x) = f_1(a - cx) \in F(a)$. Όμως, και το $f_2 \in F(a)$. Το πολυώνυμο αυτό, έχει κοινή ρίζα με το f_2 την a_2. Από την $a \neq b_i + cc_j$, έπεται ότι τα πολυώνυμα g_1 και f_2 δεν έχουν άλλη κοινή ρίζα, μια και αν είχαμε ότι $g_1(c_j) = 0$, ο $a - cc_j$ θα ήταν ρίζα του f_1, δηλαδή, για κάποιον δείκτη i, θα είχαμε $b_i = a - cc_j$, πράγμα αδύνατον, εκτός της τιμής $i = 1$. Συνεπώς ο μ.κ.δ. των πολυωνύμων αυτών, είναι το $x - a_2$. Άρα, αφού ο μ.κ.δ. δύο πολυωνύμων επί ενός σώματος ανήκει και αυτός στο σώμα (μιά και ισχύει η ταυτότης του Bezout, βλέπε ενότητα "Πολυωνυμικός Δακτύλιος") ισχύει ότι $a_2 \in F(a)$, και άρα, $a_1 = a - ca_2 \in F(a)$. Η επέκταση $F(a_1, a_2)$, λόγω του ότι είναι "ελαχίστη", περιέχεται στην $F(a)$. Είναι, λοιπόν, $L \subseteq F(a)$ οπότε και $L = F(a)$.

Πρόταση 2.. Αν F, L, M πεπερασμένες επεκτάσεις, $F \subset L \subset M$, τότε και

$$[M : F] = [M : L] \times [L : F].$$

Απόδειξη. Εξ ορισμού, το στοιχείο $c \in M$ γράφεται στην μορφή

$c = \gamma_1 c_1 + \gamma_2 c_2 + \ \ldots \ + \gamma_m c_m = \sum_{i=1}^{m} \gamma_i c_i$, όπου $m = [M : F]$, $c_i \in M$ και $\gamma_i \in L$. Κάθε $\gamma_i \in L$ γράφεται $\gamma_i = \sum_{j=1}^{n} \beta_{ij} a_j$, όπου $n = [L : F]$, $\beta_{ij} \in F$ και $a_j \in L$. Είναι, συνεπώς, και $c = \sum_{i=1}^{n} \sum_{j=1}^{m} \beta_{ij} c_i a_j$. Άρα, το τυχόν στοιχείο $c \in M$ είναι γραμμική έκφραση των $m \times n$ στοιχείων $c_i a_j$ του M, με συντελεστές από το σώμα F. Θα δείξουμε ότι τα στοιχεία αυτά είναι γραμμικά ανεξάρτητα, οπότε θα αποτελούν βάση του M επί το F. Πράγματι, μια σχέση της μορφής $\sum_{i=1}^{n} \sum_{j=1}^{m} \beta_{ij} c_i a_j = 0$ δίδει τις n σχέσεις $\sum_{j=1}^{m} \beta_{ij} c_i = 0$ μια και τα a_j βάση του L. Όμως, και τα Όμως, και τα c_i βάση του M. Άρα, $\forall i, j$, $\beta_{ij} = 0$.

Πόρισμα. Αν $F_n \supset F_{n-1} \supset \ldots F_1 \supset F_0$, τότε και

$$[F_n : F_0] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}] \cdots [F_1 : F_0]$$

Ερχόμαστε, τώρα, στην περίπτωση του $F(a)$, όπου a είναι αλγεβρικός αριθμός επί του σώματος F. Υπάρχει, τότε, πολυώνυμο με συντελεστές από το σώμα F, το οποίον έχει ρίζα τον a, (Βλέπε Ενότητα Πολυωνυμικός Δακτύλιος). Ανάμεσα σε όλα αυτά τα πολυώνυμα που έχουν ρίζα το a, υπάρχει και κάποιο ελαχίστου βαθμού. Το πολυώνυμο αυτό f, καλείται ***ελάχιστο πολυώνυμο*** του a επί το F, και ο βαθμός του, ορίζει τον βαθμό του a επί το F, και συμβολίζεται με το $\deg_K a$. Για παράδειγμα, είναι $\deg_R i = 2$, μια και το i είναι ρίζα του $f = x^2 + 1$, που είναι το ελάχιστο πολυώνυμο του i επί το R.

ΕΦΑΡΜΟΓΗ. Είναι $\deg_Q \sqrt[5]{2} = 5$, μια και το πολυώνυμο $x^5 - 2$ είναι ανάγωγο.

Θεώρημα 2. Στην περίπτωση που το a είναι αλγεβρικό επί το F, $F(a) : F = \deg_F a$.

Απόδειξη. Παρατηρούμε ότι, τα στοιχεία του $F(a)$ είναι όλες οι ρητές εκφράσεις $\frac{p}{q}$ όπου p, $q \neq 0$ πολυώνυμα εν $F[x]$. Επιπλέον, το σώμα $F(a)$ περιέχεται σε κάθε σώμα που περιέχει το F και το στοιχείο a. Υποθέτουμε, τώρα, ότι $\deg_F a = n$. Θα δείξουμε ότι τα στοιχεία 1, a, a^2,…, a^{n-1} (1) αποτελούν βάση για το $F(a)$. Προς τούτο, αρκεί να δείξουμε ότι το στοιχείο $b = \frac{p(a)}{q(a)} \in F(a)$ ισούται με κάποιο $r(a)$, όπου $r(x) \in F[x]$, με βαθμό $0 \leq \deg r(x) \leq n-1$ Έστω, λοιπόν, f το ελάχιστο πολυώνυμο του a. Αν $\deg q \geq 1$, το q δεν είναι δυνατόν να διαιρεί το f. Άρα, $(f,q) = 1$, οπότε και (ταυτότης του Bezout) $sf + tq = 1$. Άρα και, $t(a)q(a) = 1$, και συνεπώς, $\frac{p(a)}{q(a)} = p(a)t(a) = r(a)$. Για τον βαθμό του $r(x) \in F[x]$, παρατηρούμε ότι αν διαιρέσουμε το pt με το f θα λάβουμε $pt = fq' + r$, απ' όπου είναι και $p(a)t(a) = r(a)$, με $0 \leq \deg r(x) \leq n-1$. Το γεγονός ότι τα στοιχεία (1) είναι γραμμικά ανεξάρτητα, έπεται από το ότι δεν είναι δυνατόν κανένα απ' αυτά να είναι ρίζα πολυωνύμου βαθμού $\leq n-1$.

Πόρισμα. Ο a είναι αλγεβρικός αριθμός ανν $F(a)/F =$ τυχών φυσικός αριθμός .

Ορισμός. Έστω ένα πολυώνυμο $f \in F[x]$. ***Σώμα διασπάσεως*** (spliting field) του πολυωνύμου f επί του σώματος F, καλούν το ελάχιστο σώμα E που περιέχει το F και όλες τις ρίζες του f. Ένα σώμα E καλείται ***ριζική επέκταση*** (radical extension) του σώματος F, αν το E είναι απλή αλγεβρική επέκταση του F, $E = F(a)$, $a \notin F$, με $a^n \in F$, για κάποιον $n > 0$.
Λέμε ότι το πολυώνυμο $f \in F[x]$ ***λύεται με ριζικά*** (solvable by radicals) επί του F, ανν υπάρχουν οι διαδοχικές επεκτάσεις $F_n \supset F_{n-1} \supset \ldots F_1 \supset F_0$, $F_0 = F$, έτσι ώστε, το σώμα διασπάσεως E του f, να είναι, $E \subseteq F_n$.

ΠΑΡΑΔΕΙΓΜΑ 1. Έστω το $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Με το σύμβολο $\sqrt{2}$, που το ορίζουμε έτσι ώστε $\left(\sqrt{2}\right)^2 = 2$, επεκτείνουμε το σώμα $\mathbb{Q}$ στο $\mathbb{Q}\left(\sqrt{2}\right)$. Το $\mathbb{Q}\left(\sqrt{2}\right)$ περιέχει και την ρίζα $-\sqrt{2}$. Το σώμα διασπάσεως του $f(x)$ είναι το $\mathbb{Q}\left(\sqrt{2}\right)$, μέσα στο οποίο η παραγοντοποίηση του $f(x)$ είναι η $x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)$. Τα στοιχεία 1, $\sqrt{2}$ αποτελούν βάση της επέκτασης $\mathbb{Q}\left(\sqrt{2}\right)$. Είναι, λοιπόν, $\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q} = 2$

ΠΑΡΑΔΕΙΓΜΑ 2. Έστω το $f(x) = x^2 + x + 2 \in \mathbb{Q}[x]$. Στο "Μιγαδικοί αριθμοί" §3 Αρχικές ρίζες της μονάδος, έχουμε την εξής παραγοντοποίηση του $f(x) = x^2 + x + 2$, την $x^2 + x + 1 = \left(x + \frac{1}{2} - i\frac{\sqrt{3}}{2}\right)\left(x + \frac{1}{2} + i\frac{\sqrt{3}}{2}\right)$. Αν, λοιπόν, θέσουμε $\omega = i\frac{\sqrt{3}}{2}$, και με το στοιχείο αυτό επεκτείνουμε το σώμα $\mathbb{Q}$ στο $\mathbb{Q}(\omega)$, τότε, μέσα στο σώμα αυτό το $f(x)$ έχει την παραγοντοποίηση $\left(x + \frac{1}{2} - \omega\right)\left(x + \frac{1}{2} + \omega\right)$. Το $\mathbb{Q}(\omega)$ είναι το σώμα διασπάσεως

του $f(x)$. Τα στοιχεία 1, ω αποτελούν βάση της επέκτασης. $\mathbb{Q}(\omega)$. Είναι, λοιπόν, $\mathbb{Q}(\omega):\mathbb{Q} = 2$

ΠΑΡΑΔΕΙΓΜΑ 3. Να βρείτε τον βαθμό του σώματος διασπάσεως του πολυωνύμου $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ σαν επέκταση του $\mathbb{Q}$.

Βρίσκουμε πρώτα τις ρίζες του $f(x)$. Αυτές είναι οι: $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$. Το σώμα διασπάσεως του $f(x)$ θα είναι το $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$. Μπορούμε να κατασκευάσουμε το L, κάνοντας δύο απλές επεκτάσεις του $\mathbb{Q}$. Ξεκινάμε με την επέκταση $F_1 = \mathbb{Q}(\omega)$, που είναι μία επέκταση του $\mathbb{Q}$ βαθμού 2, με βάση $\{1, \omega\}$. Το ανάγωγο εν $\mathbb{Q}$ πολυώνυμο $f(x)$ δεν έχει όλες τις ρίζες του εν F_1 (είναι ανάγωγο επί του F_1). Η επέκταση $F_2 = F_1(\sqrt[3]{2})$ του F_1 διασπά το $f(x)$ σε γινόμενο πρωτοβαθμίων παραγόντων. Είναι συνεπώς αυτή που ζητάμε. Μία βάσις της F_2 επί την F_1 είναι η $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$. Φανερά, $F_2 = L$. Για να βρούμε την βάση της L επί του $\mathbb{Q}$, πολλαπλασιάζουμε τα στοιχεία της βάσεως F_1 επί τα στοιχεία της βάσεως F_2. Έχουμε συνεπώς βάση της L την $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \sqrt[3]{2}\omega, \sqrt[3]{4}\omega\}$. Άρα και $L:\mathbb{Q} = 6$.

Ορισμός. Έστω ένα πολυώνυμο $f \in F[x]$. Θα ονομάζουμε το $f(x)$ ***χωρισμένο πολυώνυμο*** (separable polynomial) επί του F αν όλες οι ρίζες του μέσα στο σώμα διασπάσεως του πολυωνύμου, έχουν πολλαπλότητα 1. Αν E επέκτασις του F και $a \in E$ αλγεβρικός αριθμός, θα λέγεται και ο a ***χωρισμένος επί*** του F, ανν το ελάχιστο πολυώνυμό του, είναι χωρισμένο επί του F. Η επέκταση E του F θα καλείται ***χωρισμένη επέκταση***, ανν κάθε στοιχείο της είναι χωρισμένο επί του F. Ένα σώμα F θα ονομάζεται ***τέλειο*** (perfect field) ανν κάθε επέκταση E του F είναι χωρισμένη.

Πρόταση. Έστω το ανάγωγο επί το F πολυώνυμο $f(x)$ και έστω $f'(x)$ η παράγωγός του. Το $f(x)$ είναι τότε χωρισμένο επί του σώματος F, ανν η παράγωγός του $f'(x)$ δεν είναι το μηδενικό πολυώνυμο.

Απόδειξη. Έστω E το σώμα διασπάσεως του $f(x)$ επί του σώματος F. Τότε, ως γνωστόν, κάθε ρίζα του $f(x)$ είναι απλή, ανν δεν υπάρχει ρίζα του παραγώγου πολυωνύμου $f'(x)$ που να είναι και ρίζα του $f(x)$ (βλέπε "Πολυωνυμικός Δακτύλιος" § 4).

α) Έστω ότι $f'(x) = 0$, $\forall x \in F$. Τότε, κάθε ρίζα του $f(x)$ είναι και ρίζα του $f'(x)$, και, συνεπώς, το $f(x)$ δεν είναι χωρισμένο επί του σώματος F.

β). Έστω $f'(x) \neq 0$ και $a \in E$ ρίζα αμφοτέρων των $f(x)$ και $f'(x)$. Τότε, το $x - a$ διαιρεί και τα δύο πολυώνυμα $f(x)$ και $f'(x)$. Όμως, $\deg f(x) < \deg f'(x)$ και άρα το $f(x)$ δεν διαιρεί το $f'(x)$. Από υπόθεση, το $f(x)$ είναι ανάγωγο. Άρα τα πολυώνυμα $f(x)$ και $f'(x)$ είναι πρώτα μεταξύ τους. Ισχύει λοιπόν, η ταυτότης του Bezout (βλέπε "Πολυωνυμικός Δακτύλιος" § 1), $u(x)f(x) + v(x)f'(x) = 1$ και κατά συνέπεια το $x - a$ να πρέπει να διαιρεί την σταθερά 1, πράγμα άτοπον. Δεν υπάρχει, λοιπόν, ρίζα του $f(x)$ που να είναι και ρίζα του $f'(x)$, και άρα, το $f(x)$ είναι χωρισμένο επί του σώματος F.

Πρόταση. Το (αριθμητικό) σώμα F είναι τέλειο.

Απόδειξη. Έστω το πολυώνυμο $f(x) \in F[x]$ ανάγωγο επί του F, βαθμού n. Αν $n = 1$, τότε το $f(x)$ έχει ακριβώς μία απλή ρίζα. Αν $n > 1$, τότε και $\deg f' = n - 1$, οπότε και $f'(x) \neq 0$ και σύμφωνα με την προηγούμενη πρόταση, το $f(x)$ είναι χωρισμένο επί του F.

3. Αυτομορφισμοί σώματος. Μία απεικόνιση $\varphi : F \to F$ του σώματος F επί το F, που είναι ένα προς ένα και διατηρεί τις πράξεις, δηλαδή, $\forall a, b \in F$, $\varphi(a + b) = \varphi(a) + \varphi(b)$, και, $\varphi(ab) = \varphi(a)\varphi(b)$, καλείται ***αυτομορφισμός*** του F (βλέπε και ενότητα "Ομάδες").
Ισχύει ότι, $\varphi(1) = 1$. Πράγματι, είναι, $\varphi(b) = \varphi(1b) = \varphi(1)\varphi(b)$. Το $\varphi(1)$ δρα, συνεπώς, σαν μοναδιαίο στοιχείο. Όμως, εδώ, στο σώμα F, το μοναδιαίο στοιχείο είναι μοναδικό. Άρα είναι, αναγκαστικά, $\varphi(1) = 1$. Όμοια και για την $\varphi(0) = 0$. Για κάθε φυσικό αριθμό n, ισχύει ότι $\varphi(n) = n$, μια και $n = 1 + \ldots + 1$ n-φορές. Άρα και γιά κάθε ρητό αριθμό q, ισχύει ότι $\varphi(q) = q$. Το σώμα $\mathbb{Q}$ παραμένει συνεπώς αναλλοίωτο ως προς την ομάδα των αυτομορφισμών του $F \supseteq \mathbb{Q}$.

ΠΑΡΑΔΕΙΓΜΑ 1. Έστω, ότι ζητάμε να βρούμε όλους τους αυτομορφισμούς του σώματος $F = \mathbb{Q}\left(\sqrt[3]{2}\right)$. Το τυχόν στοιχείο του σώματος αυτού, έχει την μορφή $a + b\left(\sqrt[3]{2}\right) + c\left(\sqrt[3]{2}\right)^2$ με $a, b, c \in \mathbb{Q}$. Αν φ αυτομορφισμός του F, τότε και

$$\varphi\left(a + b\left(\sqrt[3]{2}\right) + c\left(\sqrt[3]{2}\right)^2\right) = a + b\varphi\left(\sqrt[3]{2}\right) + c\varphi\left(\sqrt[3]{2}\right)^2 \qquad (1).$$

Επειδή $\left(\sqrt[3]{2}\right)^3 - 2 = 0$, είναι και $\varphi\left(\sqrt[3]{2}\right)^3 - 2 = 0$, απ' όπου συμπεραίνουμε ότι και το στοιχείο $\varphi\left(\sqrt[3]{2}\right) \in \mathbb{Q}\left(\sqrt[3]{2}\right)$ είναι και αυτό μία κυβική ρίζα του 2. Όμως, εν F, το πολυώνυμο $f(x) = x^3 - 2$, έχει μία και μοναδική ρίζα, την $\sqrt[3]{2}$. Άρα, $\varphi\left(\sqrt[3]{2}\right) = \sqrt[3]{2}$. Ο αυτομορφισμός $\varphi : F \to F$ είναι, λοιπόν, λόγω της (1), ο ταυτοτικός αυτομορφισμός του F

ΠΑΡΑΔΕΙΓΜΑ 2. Το ίδιο πρόβλημα με $F = \mathbb{Q}\left(\sqrt{2}\right)$. Το τυχόν στοιχείο του σώματος F έχει την μορφή $a + b\sqrt{2}$, και είναι, $\varphi\left(a + b\sqrt{2}\right) = a + b\varphi\left(\sqrt{2}\right)$, Το πολυώνυμο $f(x) = x^2 - 2$ έχει τις ρίζες $\pm\sqrt{2}$ εν F, Η σχέση, συνεπώς $\varphi(x)^2 - 2 = 0$ ισχύει για τις περιπτώσεις $\varphi_1(x) = \sqrt{2}$ και $\varphi_2(x) = -\sqrt{2}$, Μπορούμε, λοιπόν, να ορίσουμε δύο αυτομορφισμούς $\varphi_i : F \to F$, $1 \le i \le 2$, τον ταυτοτικό, για τον οποίο είναι $\varphi_1\left(\sqrt{2}\right) = \sqrt{2}$, και τον φ_2, για τον οποίο έχουμε $\varphi_2\left(\sqrt{2}\right) = -\sqrt{2}$, οπότε και, $\varphi\left(a + b\sqrt{2}\right) = a - b\sqrt{2}$.

Παρατηρήσεις. 1) Αν L μία επέκταση του σώματος F, το σύνολο των αυτομορφισμών $\varphi : L \to L$ που έχουν την ιδιότητα να απεικονίζουν τα στοιχεία του σώματος F στον εαυτό τους, αποτελούν, φανερά, υποομάδα της ομάδας αυτομορφισμών του L. Την ομάδα αυτή την συμβολίζουμε με το $G(L/F)$ (ομάδα του ***Galois*** του L επί του F) .

2) Σύμφωνα με το παράδειγμα 1, $o\left(G\left(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}\right)\right) = 1$, ενώ από το παράδειγμα 2 είναι, $o\left(G\left(\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}\right)\right) = 2$.

3) Αν a αλγεβρικός αριθμός επί του σώματος F, τότε ο a είναι ρίζα ενός αναγώγου πολυωνύμου (βλέπε ενότητα "Πολυωνυμικός Δακτύλιος" §10) το οποίον αν είναι monic, είναι και μοναδικό. Έστω a_i οι n ρίζες του. Η επέκταση είναι δυνατόν να περιέχει ή όχι κάποιες απ' τις ρίζες αυτές.

4) Αν $f(x) = c_0 + c_1 x + \ldots + c_n x^n \in F[x]$, τότε και $\varphi(f(x)) = f(\varphi(x))$.

Άρα, το $a \in F$ είναι ρίζα του f, ανν το $\varphi(a)$ είναι ρίζα του f.

5) Επίσης είναι $o(G(F(a)/F)) \le [F(a):F]$.

6) Στο πρώτο παράδειγμα, ολόκληρος ο χώρος $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ παραμένει αναλλοίωτος από τον αυτομορφισμό φ. Στο δεύτερο παράδειγμα, μόνον το σώμα των ρητών $\mathbb{Q}$ παραμένει αναλλοίωτο και από τους δύο αυτομορφισμούς φ_1, φ_2.

7) Ως γνωστόν, (βλέπε "Γραμμικές απεικονίσεις", Θεώρημα §2), μία γραμμική απεικόνισις ορίζεται πλήρως από τις εικόνες των στοιχείων της βάσεως ενός γραμμικού χώρου. Εδώ, η επέκτασις $F(a_1,\ldots,a_n)$ είναι γραμμικός χώρος επί του σώματος F, και ένας αυτομορφισμός $\varphi : A \to A$ όπου $A = \{a_1,\ldots,a_n\}$ επεκτεινόμενος επί της επεκτάσεως $F(a_1,\ldots,a_n)$ θέτοντας $\forall x \in F,\ x \notin a_i,\ \varphi(x) = x$, είναι γραμμική απεικόνιση $\varphi : F(a_1,\ldots,a_n) \to F(a_1,\ldots,a_n)$.

Παρατήρηση. Το σύνολο $K_\varphi = \{a \in L \mid \varphi(a) = a\}$, είναι σώμα. Το σώμα αυτό, καλείται ***σταθερό σώμα*** (fixed field) του αυτομορφισμού φ. Αν G σύνολο αυτομορφισμών του L, η τομή $K = \bigcap_\varphi K_\varphi$, καλείται σταθερό σώμα του F.

Στο παράδειγμα 1 το σταθερό σώμα του $G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ είναι το $\mathbb{Q}(\sqrt[3]{2})$, ενώ, στο παράδειγμα 2, το σταθερό σώμα του $G(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ είναι το $\mathbb{Q}$. Αν K το σταθερό σώμα της ομάδος $G(L/F)$, ισχύει τότε, φανερά, ότι $L \supset K \supset F$

Θεώρημα 3. Έστω η επέκταση $L = F(a)$ του σώματος F, a αλγεβρικός αριθμός επί του F, και $a = a_i, 1 \le i \le n$ ρίζες του $f(x) = c_0 + c_1 x + \ldots + c_n x^n \in F[x]$. Τότε, $\forall \varphi \in G(L/F)$, ισχύει ότι $\varphi(a) = a_i$. Και αντίστροφα, $\forall a_i \in L$, υπάρχει μοναδικός αυτομορφισμός $\varphi \in G(L/F)$, τέτοιος ώστε $\varphi(a_i) = a$. (Βλέπε και προηγούμενη παρατήρηση 7).

Απόδειξη. Η παρατήρηση 4) για $x = a_i$ και $a = \varphi(a_i)$ αποδεικνύει το πρώτο μέρος του θεωρήματος. Για το αντίστροφο: Το θεώρημα 2, μας επιτρέπει να γράφουμε τον τυχόντα $b \in L$ στην μορφή $b = r(c)$ όπου $r(x) \in F[x]$ με $\deg r(x) \le n-1$. Οι ισότητες $\varphi(b) = \varphi(r(c)) = r(\varphi(c))$ προσδιορίζουν μονοσήμαντα τον $\varphi \in G(L/F)$. Υπάρχει συνεπώς το πολύ ένας αυτομορφισμός φ, τέτοιος ώστε $\varphi(a) = a_i$. Για να κατασκευάσουμε αυτόν τον αυτομορφισμό, εργαζόμαστε ως εξής: $\forall b \in L$, γράφουμε την έκφρασή του $b = r(c)$ για το κατάλληλο πολυώνυμο $r(x) \in F[x]$, και μετά ορίζουμε την $\varphi(b) = r(c)$. Ο φ, έτσι όπως ορίσθηκε, απεικονίζει τα στοιχεία του F στον εαυτό τους, και την ρίζα του r, σε ρίζα του r.

ΠΑΡΑΔΕΙΓΜΑ 3. Ας υπολογίσουμε την ομάδα Galois του σώματος διασπάσεως του πολυωνύμου $f(x) = x^3 - 2 \in \mathbb{Q}[x]$.

Λόγω της προηγούμενης προτάσεως, ο οιοσδήποτε αυτομορφισμός φ της ομάδος Galois $G(L/\mathbb{Q})$ προσδιορίζεται από τις εικόνες των στοιχείων της βάσης του L. Εξ' άλλου, επειδή η εικόνα μιάς ρίζας είναι και αυτή ρίζα, έχουμε τις επιλογές:

$$\varphi(\sqrt[3]{2}) = \sqrt[3]{2}\text{, είτε } \varphi(\sqrt[3]{2}) = \sqrt[3]{2}\omega\text{, είτε } \varphi(\sqrt[3]{2}) = \sqrt[3]{2}\omega^2$$

$$\text{είτε } \varphi(\omega) = \omega\text{, είτε } \varphi(\omega) = \omega^2$$