1ο Φυλλάδιο Ασκήσεων - Θεωρία Galois

Αναστάσιος Φράγκος: ΑΜ 1112201900239 Διορθώσεις: Τετάρτη, 23 Μαρτίου 2022

Συμβολισμοί - Παρατηρήσεις

1. $[x^k]_f$: Είναι ο συντελεστής του x^k στο πολυώνυμο f. **2.** Έστω '$\sim$' μια σχέση ισοδυναμίας στο R^2 και $r \in R$. Θα συμβολίζουμε με $[{}^r/_\sim]$ την κλάση ισοδυναμίας του r ως προς τη σχέση '$\sim$'. **3.** Ορίζουμε $O(f(x)) := \{g \mid \exists c$ σταθερά με $g \leq cf\}$. Όταν γράφουμε $g(x) = h(x) + O(f(x))$ εννοούμε ότι υπάρχει $\overline{f} \in O(f(x))$ τέτοια ώστε $g(x) = h(x) + \overline{f}(x)$.

Άσκηση 1 Ποιά από τα παρακάτω πολυώνυμα είναι ανάγωγα πάνω από το $\mathbb{Q}$;

i. $x^3 - 7x^2 + 3x + 3$

ii. $x^6 - 6x^2 + 3x + 3$

iii. $x^5 + x^4 - 4x^3 + 2x^2 + 4x + 1$

$\blacksquare$

$\boxed{\text{i.}}$ *Λύση:* Το πολυώνυμο $f(x) = x^3 - 7x^2 + 3x + 3$ δεν είναι ανάγωγο στο $\mathbb{Q}[x]$, αφού το 1 αποτελεί ρίζα του. Ισοδύναμα, το $f(x)$ γράφεται στη μορφή:

$$f(x) = (x-1)g(x), \text{ για κάποιο } g(x) \in \mathbb{Q}[x] \text{ βαθμού } 2$$

$\square$

$\boxed{\text{ii.}}$ *Λύση:* Έστω $f(x) = x^6 - 6x^2 + 3x + 3$. Παρατηρούμε ότι ο πρώτος 3 διαιρεί καθέναν από τους συντελεστές $[x^k]_f$, $0 \leq k \leq 5$ και μάλιστα δεν διαιρεί τον $[x^6]_f$, ούτε το τετράγωνο αυτού διαιρεί τον $[x^0]_f$. Κατ' επέκταση, το *κριτήριο του Eisenstein* εφαρμόζει, από το οποίο εξασφαλίζεται ότι το $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$.

$\square$

$\boxed{\text{iii.}}$ *Λύση:* Θεωρούμε την αναγωγή του εν λόγω πολυωνύμου $f(x) = x^5 + x^4 - 4x^3 + 2x^2 + 4x + 1$ modulo 2, και ισχυριζόμαστε ότι αυτή δεν είναι ανάγωγη στο $\mathbb{Z}_2[x]$.

$$\overline{f}(x) = \left[{}^1/_{\equiv_2}\right] x^5 + \left[{}^1/_{\equiv_2}\right] x^4 + \left[{}^1/_{\equiv_2}\right], \text{ όπου } \equiv_2 \text{ είναι η σχέση ισοδυναμίας modulo 2}$$

Πράγματι, ας υποθέσουμε ότι το $\overline{f}$ δεν είναι ανάγωγο στο $\mathbb{Z}_2[x]$, στην οποία περίπτωση γράφεται ως γινόμενο ενός δευτεροβάθμιου αναγώγου πολυωνύμου με ένα τριτοβάθμιο ανάγωγο (αφού δεν διαθέτει απλές ρίζες στο $\mathbb{Z}_2$). Επειδή το μόνο ανάγωγο δευτεροβάθμιο πολυώνυμο στο $\mathbb{Z}_2[x]$ είναι το:

$$\left[{}^1/_{\equiv_2}\right] x^2 + \left[{}^1/_{\equiv_2}\right] x + \left[{}^1/_{\equiv_2}\right]$$

το $\overline{f}(x)$ θα παίρνει τη μορφή:

$$\begin{aligned}\overline{f}(x) &= \left(\left[{}^1/_{\equiv_2}\right] x^2 + \left[{}^1/_{\equiv_2}\right] x + \left[{}^1/_{\equiv_2}\right] \right) \cdot \left(\left[{}^a/_{\equiv_2}\right] x^3 + \left[{}^b/_{\equiv_2}\right] x^2 + \left[{}^c/_{\equiv_2}\right] x + \left[{}^d/_{\equiv_2}\right] \right) \\ &= \left[{}^a/_{\equiv_2}\right] x^5 + \left[{}^{a+b}/_{\equiv_2}\right] x^4 + \left[{}^{a+b+c}/_{\equiv_2}\right] x^3 + \left[{}^{b+c+d}/_{\equiv_2}\right] x^2 + \left[{}^{c+d}/_{\equiv_2}\right] x + \left[{}^d/_{\equiv_2}\right]\end{aligned}$$

κι άρα:

- $\left[{}^a/_{\equiv_2}\right] = [x^5]_{\overline{f}} = \left[{}^1/_{\equiv_2}\right]$
- $\left[{}^{a+b}/_{\equiv_2}\right] = [x^4]_{\overline{f}} = \left[{}^1/_{\equiv_2}\right] \Rightarrow \left[{}^b/_{\equiv_2}\right] = \left[{}^0/_{\equiv_2}\right]$
- $\left[{}^{a+b+c}/_{\equiv_2}\right] = [x^3]_{\overline{f}} = \left[{}^0/_{\equiv_2}\right] \Rightarrow \left[{}^c/_{\equiv_2}\right] = \left[{}^1/_{\equiv_2}\right]$
- $\left[{}^{b+c+d}/_{\equiv_2}\right] = [x^2]_{\overline{f}} = \left[{}^0/_{\equiv_2}\right] \Rightarrow \left[{}^d/_{\equiv_2}\right] = \left[{}^1/_{\equiv_2}\right]$

Παρατηρούμε με αυτά ότι:

$$\overline{f}(x) = \Big(\left[{}^{1}/_{\equiv_2}\right] x^2 + \left[{}^{1}/_{\equiv_2}\right] x + \left[{}^{1}/_{\equiv_2}\right] \Big) \cdot \Big(\left[{}^{1}/_{\equiv_2}\right] x^3 + \left[{}^{1}/_{\equiv_2}\right] x + \left[{}^{1}/_{\equiv_2}\right] \Big)$$

το οποίο συνηστά μια *ένδειξη* ότι το πολυώνυμο $f(x)$ δεν είναι ανάγωγο στο $\mathbb{Z}[x]$. Μάλιστα, κάθε υποψήφια αναγραφή του σε γινόμενο δευτεροβάθμιου με τριτοβάθμιο πολυώνυμο είναι της μορφής:

$$\big((2k+1)x^2 + (2l+1)x + (m+1)\big) \cdot \big((2n+1)x^3 + 2px^2 + (2q+1)x + (r+1)\big)$$

για κάποια $k, l, m, n, p, q, r \in \mathbb{Z}$. Θέτουμε τώρα $k = 0, l = 1, m = 0, n = 0, p = -1, q = 0, r = 0$ και παρατηρούμε ότι:

$$(x^2 + 3x + 1) \cdot (x^3 - 2x^2 + x + 1) = x^5 + x^4 - 4x^3 + 2x^2 + 4x + 1 = f(x)$$

Το $f(x)$ δεν είναι λοιπόν ανάγωγο στο $\mathbb{Q}[x]$.

□

Άσκηση 2 Βρείτε όλες τις ρητές συναρτήσεις ${}^{f(x)}\big/_{g(x)} \in \mathbb{Q}[x]$ που έχουν την ιδιότητα:

$${}^{f(x)}\Big/_{g(x)} = {}^{f(x+a)}\Big/_{g(x+a)}$$

για κάθε $a \in \mathbb{Q}$. Η λύση εφαρμόζει για κάθε σώμα στη θέση του $\mathbb{Q}$; ■

Λύση: Εάν το $f(x)$ είναι το μηδενικό πολυώνυμο του $\mathbb{Q}[x]$, για κάθε $g(x) \in \mathbb{Q}[x]$ ισχύει η εν λόγω σχέση.

Εάν τα $f(x), g(x) \in \mathbb{Q}[x]$ είναι σταθερά πολυώνυμα, και πάλι ισχύει κάπως τετριμμένα η εν λόγω σχέση.

Έστω $f(x), g(x)$ δύο μη μηδενικά πολυώνυμα του $\mathbb{Q}[x]$ με θετικούς βαθμούς. Υποθέτουμε αρχικά ότι τα $f(x), g(x)$ είναι μονικά και μεταξύ τους σχετικά πρώτα. Η δεδομένη σχέση μας δίνει ότι:

$$f(x) = \frac{g(x)}{g(x+a)} \cdot f(x+a) \textbf{ και } f(x+a) = \frac{g(x+a)}{g(x)} \cdot f(x)$$

Επειδή τα $f(x), g(x)$ υποτέθηκαν σχετικά πρώτα, η πρώτη σχέση δίνει $g(x+a)|g(x)$ και η δεύτερη $g(x)|g(x+a)$, από το οποίο συνεπάγεται η ισότητα των δύο $g(x) = g(x+a)$. Ισοδύναμα:

$$\frac{f(x+a)}{f(x)} = \frac{g(x+a)}{g(x)} = 1$$

Εάν τώρα συμβολίσουμε $n = \deg f$ και $m = \deg g$, φέρνοντας τα πολυώνυμα (με τους απαραίτητους πολλαπλασιασμούς) $f(x+a)$, $g(x+a)$ σε μία μορφή περί του μηδενός, έχουμε ότι:

$$\frac{f(x) + a \cdot n \cdot [x^n]_f \cdot x^{n-1} + O(x^{n-2})}{f(x)} = \frac{g(x) + a \cdot m \cdot [x^m]_g \cdot x^{m-1} + O(x^{m-2})}{g(x)} = 1$$
$$\Rightarrow \frac{a \cdot n \cdot [x^n]_f \cdot x^{n-1} + O(x^{n-2})}{f(x)} = \frac{a \cdot m \cdot [x^m]_g \cdot x^{m-1} + O(x^{m-2})}{g(x)} = 0$$
$$\Rightarrow a \cdot n \cdot [x^n]_f \cdot x^{n-1} + O(x^{n-2}) = a \cdot m \cdot [x^m]_g \cdot x^{m-1} + O(x^{m-2}) = 0$$

κι επειδή η τελευταία ισότητα ισχύει για κάθε $a \in \mathbb{Q}$:

$$[x^n]_f = [x^m]_g = 0 \qquad (*)$$

Αυτό οδηγεί σε αντίφαση, αν κανείς λάβει υπ' όψιν τον ορισμό των n, m. Επομένως, εάν η προς μελέτη σχέση ισχύει για σχετικά πρώτα $f(x), g(x)$, τότε αυτά τα $f(x), g(x)$ είναι κατ' ανάγκη σταθερά.

Εάν μια γενικότερη περίπτωση αληθεύει, εάν δηλαδή τα $f(x), g(x)$ είναι απλώς μη μηδενικά και θετικού βαθμού, θεωρούμε μια ανάγωγη γραφή του πηλίκου:

$$\frac{f(x)}{g(x)} = \sigma \cdot \frac{p(x)}{q(x)}, \text{ όπου τα } p, q \text{ είναι μονικά και σχετικά πρώτα και } \sigma \in \mathbb{Q}$$

και παρατηρούμε ότι το πρόβλημα μπορεί να αναχθεί στην περίπτωση που αναλύσαμε πρωτύτερα. Ειδικότερα, σε αυτήν την περίπτωση, θα πρέπει τα $p(x), q(x)$ να είναι σταθερά πολυώνυμα (άρα ίσα με 1, αφού είναι μονικά) - ισοδύναμα, $f(x) = \sigma g(x)$ για $\sigma \in \mathbb{Q}$.

Συνοψίζοντας, η προς μελέτη σχέση ισχύει μόνο στις περιπτώσεις όπου:

- $f(x) = 0$ και $g(x) \in \mathbb{Q}[x]$,

- Τα $f(x)$ και $g(x)$ είναι σταθερά πολυώνυμα του $\mathbb{Q}[x]$,

- Υπάρχει σταθερά $\sigma \in \mathbb{Q}$ τέτοια ώστε $f(x) = \sigma g(x)$.

ή συνοπτικότερα, μόνον αν $\gcd(f, g) \in \{1\} \cup \mathbb{Q} \cdot g$, όπου $\gcd(f, g) \in \mathbb{Q}[x]$ είναι ο μέγιστος κοινός διαιρέτης των f, g και για κάθε πολυώνυμο P ορίζεται $\mathbb{Q} \cdot P := \{sP(x) \mid s \in \mathbb{Q}\}$. Η απόδειξη *δεν* είναι ανεξάρτηση του $\mathbb{Q}$. Συγκεκριμένα, στη σχέση $(*)$ χρησιμοποιείται ότι $\operatorname{char}\mathbb{Q} = 0$. Μάλιστα, υπάρχουν σώματα θετικής χαρακτηριστικής στα οποία η απόδειξή μας δεν εφαρμόζει - παράδειγμα το $\mathbb{Z}_2$.

$$\frac{f(x)}{g(x)} = \frac{x^2 + x}{x^2 + x + 1}$$

(Προφανώς εδώ οι συντελεστές εννοούνται στο $\mathbb{Z}_2$. Αντίθετα με ό,τι κάναμε στην **Άσκηση 1**, παραλείπουμε για χάρη ευκολίας τις κλάσεις ισοδυναμίας).

Νομίζω ότι κάτι δεν πάει καλά (όσον αφορά την ανεξαρτησία της απόδειξης από την πληρότητα του $\mathbb{Q}$). Εάν δεν σας κάνει κόπο και κάτι τέτοιο είναι εφικτό, γράψτε μου ένα λάθος μου εδώ: afragos@email.com.

$\square$

Άσκηση 3 Έστω p πρώτος της μορφής $p = n^2 + 1,\ n \in \mathbb{Z}$. Θέτουμε $a = \sqrt{p + \sqrt{p}}$,$b = \sqrt{p - \sqrt{p}}$ και $K = \mathbb{Q}(a)$.

i. Βρείτε τα πολυώνυμα $\operatorname{Irr}(a, \mathbb{Q})$ και $\operatorname{Irr}(a, \mathbb{Q}(\sqrt{p}))$, καθώς επίσης και τους βαθμούς $[K : \mathbb{Q}]$ και $[K : \mathbb{Q}(\sqrt{p})]$.

ii. Αληθεύει ότι $b \in \mathbb{Q}(a)$;

iii. Αληθεύει ότι $c \in \mathbb{Q}(a)$, όπου c είναι ρίζα του $5x^3 + 18x^2 - 3x + 12$;

iv. Αληθεύει ότι υπάρχει αυτομορφισμός $\sigma : K \to K$ με $\sigma(a) = b$;

v. Αληθεύει ότι υπάρχει αυτομορφισμός $\sigma : K \to K$ με $\sigma(a) = b$ και $\sigma(\sqrt{p}) = -\sqrt{p}$;

$\blacksquare$

$\boxed{\text{i.}}$ *Λύση:* Επειδή:

$$a = \sqrt{p + \sqrt{p}} \Rightarrow a^2 = p + \sqrt{p} \Rightarrow (a^2 - p)^2 = p$$

το πολυώνυμο $f(x) = (x^2 - p)^2 - p = x^4 - 2px^2 + p^2 + p \in \mathbb{Q}[x]$ έχει ρίζα το a. Επομένως $\operatorname{Irr}(a, \mathbb{Q})(x) \mid x^4 - 2px^2 + p^2 - p$. Επειδή επιπλέον το $x^4 - 2px^2 + p^2 + p$ είναι μονικό, εάν δείξουμε ότι είναι ανάγωγο, θα έχουμε δείξει ότι $\operatorname{Irr}(a, \mathbb{Q})(x) = x^4 - 2px^2 + p^2 - p$. Κατ' επέκταση, $[\mathbb{Q}(a) : \mathbb{Q}] = \deg f = 4$.

Το $x^4 - 2px^2 + p^2 - p$ είναι πράγματι ανάγωγο, κι αυτό προκύπτει μέσω του *κριτηρίου του Eisenstein*: ο πρώτος p διαιρεί τους $[x^2]_f = 2p,\ [x^0]_f = p^2 - p,\ [x^3]_f = [x^1]_f = 0$, δεν διαιρεί τον $[x^4]_f = 1$ και επιπλέον το τετράγωνο αυτού δεν διαιρεί τον $[x^0]_f$.

Όσον αφορά το $\operatorname{Irr}(a, \mathbb{Q}(\sqrt{p}))$, θα δείξουμε ότι $\operatorname{Irr}(a, \mathbb{Q}(\sqrt{p})) = g(x) = x^2 - p - \sqrt{p}$. Πράγματι, το a είναι ρίζα του $g(x)$ αφού:

$$a = \sqrt{p + \sqrt{p}} \Rightarrow a^2 = p + \sqrt{p}$$

Επιπλέον αυτό είναι ανάγωγο στο $\mathbb{Q}(\sqrt{p})$, και για να αποδείξουμε τον εν λόγω ισχυρισμό εργαζόμαστε σε βήματα.

Βήμα 1ο: Το $\mathbb{Q}$ είναι υπόσωμα του $\mathbb{Q}(\sqrt{p})$ κι αυτό με την σειρά του είναι υπόσωμα του $\mathbb{Q}(a)$. Πράγματι, ο εγκλεισμός $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p})$ είναι προφανής. Επειδή $a^2 = p + \sqrt{p}$, το $\sqrt{p}$ ανήκει στο $\mathbb{Q}(a)$, το οποίο με την σειρά του σημαίνει ότι $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(a)$.

$$\begin{tikzcd}
\mathbb{Q}(a) \arrow[dd, dash, "{[\mathbb{Q}(a):\mathbb{Q}]=4}"'] \arrow[dr, dash, "{[\mathbb{Q}(a):\mathbb{Q}(\sqrt{p})]=2}"] & \\
& \mathbb{Q}(\sqrt{p}) \arrow[dl, dash, "{[\mathbb{Q}(\sqrt{p}):\mathbb{Q}]=2}"] \\
\mathbb{Q} &
\end{tikzcd}$$

Βήμα 2ο: Το πολυώνυμο $x^2 - p$ είναι ανάγωγο στο $\mathbb{Q}$ και μηδενίζεται από το $\sqrt{p}$, οπότε $\mathrm{Irr}(\sqrt{p}, \mathbb{Q}) = x^2 - p$. Πράγματι $\sqrt{p}^2 - p = 0$ και από το *κριτήριο του Eisenstein* εξασφαλίζεται ότι $x^2 - p$ είναι ανάγωγο.

Βήμα 3ο: Από το *θεώρημα των Πύργων* έπεται ότι:

$$[\mathbb{Q}(a) : \mathbb{Q}(\sqrt{p})] \cdot [\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 4 \Rightarrow [\mathbb{Q}(a, b) : \mathbb{Q}(b)] = 2$$

το οποίο εξασφαλίζει ότι $\deg \mathrm{Irr}(a, \mathbb{Q}(\sqrt{p})) = 2$. Οπότε, αφού το $g(x)$ είναι μονικό πολυώνυμο βαθμού 2, έχουμε αποδείξει ότι $g(x) = \mathrm{Irr}(a, \mathbb{Q}(\sqrt{p}))$.

$\square$

$\boxed{\text{ii.}}$ Λύση: Παρατηρούμε ότι οι επεκτάσεις $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(a)$ και $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(b)$ είναι επεκτάσεις του $\mathbb{Q}(\sqrt{p})$ με το ίδιο ανάγωγο πολυώνυμο $\mathrm{Irr}(a, \mathbb{Q}(\sqrt{p}))(x) = \mathrm{Irr}(b, \mathbb{Q}(\sqrt{p}))(x) = x^2 - p - \sqrt{p} = (x-a)(x-b) = f(x)$. Κατ' επέκταση:

$$[x^0]_f = ab \in \mathbb{Q}(\sqrt{p}) \Rightarrow ab \in \mathbb{Q}(a) \Rightarrow b \in \mathbb{Q}(a)$$

το οποίο είναι το ζητούμενο. Διαφορετικά θα μπορούσαμε να είχαμε παρατηρήσει ότι

$$ab = \sqrt{p^2 - p} = \sqrt{n^4 + 2n^2 + 1 - n^2 - 1} = \sqrt{n^4 + n^2} = n\sqrt{n^2 + 1} = n\sqrt{p} \in \mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(a)$$

$\square$

$\boxed{\text{iii.}}$ Λύση: Ας υποθέσουμε προς άτοπο ότι $c \in \mathbb{Q}(a)$. Υπό αυτήν την υπόθεση, το $\mathbb{Q}(c)$ μπορεί να θεωρηθεί υπόσωμα του $\mathbb{Q}(a)$ με ανάγωγο πολυώνυμο $\mathrm{Irr}(c, \mathbb{Q})(x) \mid 5x^3 + 18x^2 - 3x + 12 = h(x)$. Το $5x^3 + 18x^2 - 3x + 12$ είναι ανάγωγο στο $\mathbb{Q}(x)$, αφού ο πρώτος 3 διαιρεί τους συντελεστές $[x^k]_h$, $0 \leq k \leq 4$, δεν διαιρεί τον $[x^3]_h$ και το τετράγωνο αυτού δεν διαιρεί τον $[x^0]_h$. Οπότε, το αντίστοιχο μονικό $x^3 + \frac{18}{5}x^2 - \frac{3}{5}x + \frac{12}{5}$ ισούται με το ανάγωγο $\mathrm{Irr}(c, \mathbb{Q}(c))$ και κατ' επέκταση $[\mathbb{Q}(c) : \mathbb{Q}] = 3$.

$$\begin{tikzcd}
\mathbb{Q}(a) \arrow[d, dash, "{[\mathbb{Q}(a):\mathbb{Q}(c)]}"] \arrow[dd, dash, bend right, "{[\mathbb{Q}(a):\mathbb{Q}]=4}"'] \\
\mathbb{Q}(c) \arrow[d, dash, "{[\mathbb{Q}(c):\mathbb{Q}]=3}"] \\
\mathbb{Q}
\end{tikzcd}$$

Αυτό είναι άτοπο, αφού από το *θεώρημα των Πύργων* ο βαθμός $[\mathbb{Q}(a) : \mathbb{Q}(c)]$ της αντίστοιχης επέκτασης δεν θα είναι ακέραιος.

$\square$

$\boxed{\text{iv.}}$ Λύση: Το πολυώνυμο $f(x) = (x^2 - p)^2 - p$ είναι ανάγωγο στο $\mathbb{Q}[x]$, a είναι μία ρίζα του $f(x)$ στην επέκταση $\mathbb{Q}(a)$ του $\mathbb{Q}$ και b είναι μία ρίζα του $f(x)$ στην επέκταση $\mathbb{Q}(b)$ του $\mathbb{Q}$.

$$\begin{tikzcd}
\mathbb{Q}(a) \arrow[r, tail, two heads, "\sigma"] \arrow[d, dash] & \mathbb{Q}(b) \arrow[d, dash] \\
\mathbb{Q} \arrow[r, tail, two heads, "\mathrm{id}"'] & \mathbb{Q}
\end{tikzcd}$$

Το *θεώρημα επέκτασης ισομορφισμών* λοιπόν εφαρμόζει και εξασφαλίζει έναν ισομορφισμό σ μεταξύ των $\mathbb{Q}(a)$ και $\mathbb{Q}(b)$, ο οποίος είναι επέκταση του $\mathrm{id} : \mathbb{Q} \to \mathbb{Q}$ και ικανοποιεί τη σχέση $\sigma(a) = b$.

$\square$

$\boxed{\text{v.}}$ <u>*Λύση:*</u> Στο υποερώτημα **iv.** αποδείξαμε ότι υπάρχει ισομορφισμός σ μεταξύ των $\mathbb{Q}(a)$ και $\mathbb{Q}(b)$, ο οποίος είναι επέκταση του $\mathrm{id} : \mathbb{Q} \to \mathbb{Q}$ και ικανοποιεί τη σχέση $\sigma(a) = b$. Θα αποδείξουμε ότι αυτός ο ισομορφισμός ικανοποιεί αναγκαστικά και τη σχέση $\sigma(p) = -\sqrt{p}$.

Πράγματι:

$$\sigma(a^2) = [\sigma(a)]^2 = b^2 \Rightarrow \sigma(p + \sqrt{p}) = p - \sqrt{p}$$

κι επειδή η σ είναι επέκταση της $\mathrm{id} : \mathbb{Q} \to \mathbb{Q}$:

$$p + \sigma(\sqrt{p}) = p - \sqrt{p} \Rightarrow \sigma(\sqrt{p}) = -\sqrt{p}$$

$\square$

Άσκηση 4 Έστω $a \in \mathbb{C}$ ρίζα του $x^3 - x^2 + x + 1$.

i. Βρείτε όλα τα σώματα E με $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(a)$.

ii. Έστω $b = \dfrac{a}{a-3}$. Να βρεθούν $c_0, c_1, c_2 \in \mathbb{Q}$ με $b = c_0 + c_1 a + c_2 a^2$.

$\boxed{\text{i.}}$ <u>*Λύση:*</u> Έστω $a \in \mathbb{C}$ μια ρίζα του $x^3 - x^2 + x + 1$. Το πολυώνυμο $x^3 - x^2 + x + 1$ είναι πολυώνυμο ρητών συντελεστών και έχει ρίζα το $a \in \mathbb{C}$, επομένως το ανάγωγο πολυώνυμο $\mathrm{Irr}(a, \mathbb{Q})$ διαιρεί το $x^3 - x^2 + x + 1$ κι άρα έχει βαθμό το πολύ 3.

$$\begin{tikzcd} \mathbb{Q}(a) \arrow[d, dash, "{[\mathbb{Q}(a) : E]}"] \arrow[dd, dash, bend right=60, "{[\mathbb{Q}(a) : \mathbb{Q}] = 3}"'] \\ E \arrow[d, dash, "{[E : \mathbb{Q}] \in \{1, 3\}}"] \\ \mathbb{Q} \end{tikzcd}$$

Έστω ένα τυχαίο σώμα E το οποίο είναι επέκταση του $\mathbb{Q}$ και υπόσωμα του $\mathbb{Q}(a)$. Από το *θεώρημα των Πύργων* έπεται ότι:

$$[\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(a) : E] \cdot [E : \mathbb{Q}]$$

κι επειδή το 3 είναι πρώτος:

$$\beta = [E : \mathbb{Q}] \in \{1, 3\}$$

Εάν όμως $\beta = 1$, τότε $\mathbb{Q} = E$ και εάν $\beta = 3$, τότε $\mathbb{Q}(a) = E$. Σε κάθε περίπτωση, γνήσια ενδιάμεσα υποσώματα E δεν υπάρχουν.

$\square$

$\boxed{\text{ii.}}$ <u>*Λύση:*</u> Εφόσον το a αποτελεί ρίζα του $x^3 - x^2 + x + 1$, ο αριθμός $a - 3$ θα αποτελεί ρίζα του πολυωνύμου $(x+3)^3 - (x+3)^2 + (x+3) + 1$. Δηλαδή το πολυώνυμο:

$$(x+3)^3 - (x+3)^2 + (x+3) + 1 = x^3 + 8x^2 + 22x + 22$$

μηδενίζεται όταν $x = a - 3$. Άρα:

$$(a-3)^3 + 8(a-3)^2 + 22(a-3) + 22 = 0 \overset{a \neq 3}{\Longrightarrow} (a-3)^2 + 8(a-3) + 22 + \frac{22}{a-3} = 0$$

$$\Rightarrow \frac{1}{a-3} = -\frac{1}{22}a^2 - \frac{1}{11}a - \frac{7}{22}$$

κι επειδή $\dfrac{a}{a-3} = 1 + \dfrac{3}{a-3}$, έπεται ότι:

$$b = \frac{a}{a-3} = -\frac{3}{22}a^2 - \frac{3}{11}a + \frac{1}{22}$$

Οπότε $c_0 = 1/22$, $c_1 = -3/11$, $c_2 = -3/22$.

$\square$

Άσκηση 5 Έστω $p(x),\ q(x) \in \mathbb{Q}[x]$ ανάγωγα πολυώνυμα, $a \in \mathbb{C}$ ρίζα του $p(x)$, $b \in \mathbb{C}$ ρίζα του $q(x)$, $F = \mathbb{Q}(a)$ και $K = \mathbb{Q}(b)$. Τότε το $p(x)$ είναι ανάγωγο στο $K[x]$ εάν και μόνο αν το $q(x)$ είναι ανάγωγο στο $F[x]$. ■

Λύση: Έστω $p(x),\ q(x) \in \mathbb{Q}[x]$ ανάγωγα πολυώνυμα στο $\mathbb{Q}[x]$, $a \in \mathbb{C}$ ρίζα του $p(x)$ και $b \in \mathbb{C}$ ρίζα του $q(x)$. Θεωρούμε τις *πεπερασμένες* επεκτάσεις $\mathbb{Q}(a),\ \mathbb{Q}(b)$ του $\mathbb{Q}$ καθώς επίσης και την (*πεπερασμένη επέκταση*) $\mathbb{Q}(a,b)$ των $\mathbb{Q}(a),\ \mathbb{Q}(b)$:

$$\begin{tikzcd}
 & \mathbb{Q}(a,b) & \\
\mathbb{Q}(a) \arrow[ur, dash] & & \mathbb{Q}(b) \arrow[ul, dash] \\
 & \mathbb{Q} \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

Υποθέτουμε ότι το q είναι ανάγωγο στο $\mathbb{Q}(a)[x]$. Θα δείξουμε ότι το πολυώνυμο p ισούται με το $[x^{\deg p}]_p \cdot \mathrm{Irr}(a, \mathbb{Q}(b))$, οπότε θα είναι ανάγωγο στο $\mathbb{Q}(b)$.

Το πολυώνυμο p είναι ανάγωγο στο $\mathbb{Q}[x]$. Επειδή επιπλέον έχει ρίζα το a, έπεται:

$$\mathrm{Irr}(a, \mathbb{Q}) \mid p \Rightarrow p = [x^{\deg p}]_p \cdot \mathrm{Irr}(a, \mathbb{Q})$$

Το πολυώνυμο q έχει υποτεθεί ανάγωγο στο $\mathbb{Q}(a)[x]$. Επειδή επιπλέον έχει ρίζα το b, έπεται:

$$\mathrm{Irr}(b, \mathbb{Q}(a)) \mid q \Rightarrow q = [x^{\deg q}]_q \cdot \mathrm{Irr}(b, \mathbb{Q}(a))$$

Εφαρμόζοντας το *Θεώρημα των Πύργων* στις διαδοχικές επεκτάσεις $\mathbb{Q} \subseteq \mathbb{Q}(a) \subseteq \mathbb{Q}(a,b)$, έχουμε ότι:

$$[\mathbb{Q}(a,b) : \mathbb{Q}] = \deg p \cdot \deg q \tag{I}$$

Το πολυώνυμο q είναι ανάγωγο στο $\mathbb{Q}[x]$. Επειδή επιπλέον έχει ρίζα το b, έπεται:

$$\mathrm{Irr}(b, \mathbb{Q}) \mid q \Rightarrow q = [x^{\deg q}]_q \cdot \mathrm{Irr}(b, \mathbb{Q})$$

Το πολυώνυμο p έχει ρίζα το a, οπότε:

$$\mathrm{Irr}(a, \mathbb{Q}(b)) \mid p \Rightarrow \deg \mathrm{Irr}(a, \mathbb{Q}(b)) \leq \deg p$$

Εφαρμόζοντας το *Θεώρημα των Πύργων* στις διαδοχικές επεκτάσεις $\mathbb{Q} \subseteq \mathbb{Q}(b) \subseteq \mathbb{Q}(a,b)$, έχουμε ότι:

$$[\mathbb{Q}(a,b) : \mathbb{Q}] \leq \deg p \cdot \deg q \tag{II}$$

Από τις σχέσεις τώρα (I) και (II) κανείς μπορεί να βγάλει το συμπέρασμα ότι τελικά $\deg \mathrm{Irr}(a, \mathbb{Q}(b)) = \deg p$. Ειδικότερα, επειδή το $\mathrm{Irr}(a, \mathbb{Q}(b))$ διαιρεί το p, το p γράφεται στη μορφή:

$$p = [x^{\deg p}]_p \cdot \mathrm{Irr}(a, \mathbb{Q}(b))$$

Αυτό ουσιαστικά δείχνει ότι το p είναι ανάγωγο πολυώνυμο στο $\mathbb{Q}(b)[x]$ και αποδεικνύει την κατεύθυνση ($\Leftarrow$). Τα επιχειρήματα είναι τελείως συμμετρικά για την περίπτωση του p, οπότε αποδυκνύεται η κατεύθυνση ($\Rightarrow$) και κατ' επέκταση η ισοδυναμία ($\Leftrightarrow$).

$\square$