ΘΕΩΡΙΑ ΣΩΜΑΤΩΝ

Σημειώσεις προπτυχιακού μαθήματος [1]

Ν.Γ. Τζανάκης

Τμήμα Μαθηματικών

Πανεπιστήμιο Κρήτης - Ηράκλειο

[1] Εαρινό εξάμηνο 2024

Περιεχόμενα

Κεφάλαιο 1

Επεκτάσεις Σωμάτων

1.1 Βασικες Προτασεις

Έστω ότι K, L είναι σώματα και υπάρχει μονομορφισμός σωμάτων $K \hookrightarrow L$. Τότε λέμε ότι το L είναι *επέκταση* του K και γράφομε L/K. Στην ειδική περίπτωση που το K είναι υπόσωμα του L, το L είναι επέκταση του K διότι η ταυτοτική απεικόνιση του K είναι ένας προφανής μονομορφισμός $K \hookrightarrow L$. Πάντως, σε κάθε περίπτωση, όταν το L είναι επέκταση του K και εργαζόμαστε στο L, τότε «ξεχνούμε» το K και μέσω του μονομορφισμού $K \hookrightarrow L$ ταυτίζομε τα στοιχεία του K με τις εικόνες τους, οπότε είναι σαν να θεωρούμε το K ως υπόσωμα του L.

Ορισμός 1.1.1. *Έστω L/K επέκταση σωμάτων.*

(1) *Το $v \in L$ λέγεται αλγεβρικό πάνω από το K αν είναι ρίζα ενός μη μηδενικού πολυωνύμου με συντελεστές από το K.*

(2) *Η επέκταση L/K χαρακτηρίζεται αλγεβρική αν κάθε στοιχείο της είναι αλγεβρικό πάνω από το K.*

Είναι προφανές ότι κάθε στοιχείο u του K είναι αλγεβρικό πάνω από το K, αφού είναι ρίζα του $X - u \in K[X]$.

Μία πολύ σημαντική παρατήρηση είναι ότι το σώμα L μπορεί να θεωρηθεί ως K-διανυσματικός χώρος (ανεξαρτήτως του αν η επέκταση L/K είναι ή όχι αλγεβρική).

Ορισμός 1.1.2. *Βαθμός της επέκτασης L/K είναι, εξ ορισμού, η διάσταση του K-διανυσματικού χώρου L, η οποία και συμβολίζεται $[L : K]$· αν είναι πεπερασμένος αριθμός, η επέκταση χαρακτηρίζεται πεπερασμένη, διαφορετικά, άπειρη.*

Παραδείγματα. Για τις ανάγκες αυτών των παραδειγμάτων, και μόνο, θεωρούμε γνωστά κάποια βασικά πράγματα από τους πραγματικούς και τους μιγαδικούς αριθμούς, όπως η ύπαρξη στο $\mathbb{R}$ τετραγωνικής ρίζας του 2 και η ύπαρξη στο $\mathbb{C}$ της n-οστής ρίζας του 2 για οποιονδήποτε φυσικό n.

1. Έστω $L = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$. Είναι φανερό ότι το L είναι κλειστό ως πρός την πρόσθεση, την αφαίρεση και τον πολλαπλασιασμό. Ως πρός την ύπαρξη αντιστρόφου, παρατηρούμε ότι ο

αντίστροφος πραγματικός αριθμός του $a+b\sqrt{2}$, είναι ο

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

που προφανώς ανήκει στο L. Άρα, το L είναι υπόσωμα του $\mathbb{R}$ και $L/\mathbb{Q}$ είναι επέκταση σωμάτων, της οποίας ο βαθμός είναι 2. Πράγματι, από τον ορισμό του L προκύπτει ότι τα $1, \sqrt{2}$ παράγουν το L πάνω από το $\mathbb{Q}$. Ακόμη, τα στοιχεία αυτά είναι $\mathbb{Q}$-γραμμικώς ανεξάρτητα διότι, διαφορετικά, θα υπήρχαν $a, b \in \mathbb{Q}$, όχι και τα δύο μηδέν που ικανοποιούν τη σχέση $a+b\sqrt{2}=0$. Αλλά αυτό συνεπάγεται (λύνοντας ως πρός $\sqrt{2}$) ότι $\sqrt{2} \in \mathbb{Q}$, άτοπο, αφού είναι γνωστό από τα αρχαία χρόνια ότι ο $\sqrt{2}$ δεν είναι ρητός αριθμός. Συνεπώς, μία βάση της επέκτασης $L/\mathbb{Q}$ είναι η $\{1, \sqrt{2}\}$, οπότε, ειδικότερα, $[L:\mathbb{Q}]=2$.

2. Η επέκταση $\mathbb{C}/\mathbb{R}$ έχει βάση την $\{1, i\}$, οπότε $[\mathbb{C}:\mathbb{R}]=2$. Η απόδειξη είναι ανάλογη με αυτή του προηγούμενου παραδείγματος.

3. Η μελέτη της επέκτασης $\mathbb{C}/\mathbb{Q}$ είναι αρκετά δυσκολότερη. Στην πραγματικότητα, θα δείξομε ότι η επέκταση αυτή είναι άπειρη. Αρκεί να δείξομε ότι, για οσοδήποτε μεγάλο φυσικό αριθμό n, υπάρχουν n το πλήθος μιγαδικοί αριθμοί, που είναι $\mathbb{Q}$-γραμμικώς ανεξάρτητοι. Προς τούτο, θεωρούμε το πολυώνυμο $f(X)=X^n-2$ και έστω $z \in \mathbb{C}$ μία ρίζα του, π.χ. $z = \sqrt[n]{2}(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n})$. Ισχυριμός: οι μιγαδικοί αριθμοί $1, z, z^2, \ldots, z^{n-1}$ είναι $\mathbb{Q}$-γραμμικώς ανεξάρτητοι. Πραγματικά, σε αντίθετη περίπτωση, θα υπήρχαν ρητοί $c_0, c_1, \ldots, c_{n-1}$, όχι όλοι μηδέν, που ικανοποιούν τη σχέση $c_0 + c_1 z + \cdots + c_{n-1}z^{n-1} = 0$, δηλαδή, $g(z)=0$, όπου $g(X) = c_0 + c_1 X + \cdots + c_{n-1}X^{n-1}$. Συνεπώς, τα μη μηδενικά πολυώνυμα $f(X)$ και $g(X)$ έχουν κοινή ρίζα τη z, άρα από το 2 της πρότασης B'.5 (παράρτημα B'), τα $f(X)$ και $g(X)$ δεν είναι πρώτα μεταξύ τους. Αλλά το $f(X)$ είναι ανάγωγο, καθώς φαίνεται αμέσως από το κριτήριο του Eisenstein , συνεπώς, από το 1 της πρότασης B'.5 (παράρτημα B'), συμπεραίνομε ότι $f(X)|g(X)$, που είναι αδύνατο, διότι το μη μηδενικό πολυώνυμο $g(X)$ έχει βαθμό μικρότερο από τόν βαθμό του $f(X)$.

Έστω τώρα $v \in L$ και $K[v]$ το σύνολο όλων των στοιχείων της μορφής $a_0+a_1v+\ldots+a_nv^n$ · το n μπορεί να είναι οποιοσδήποτε μη αρνητικός ακέραιος και τα a_i ανήκουν στο K. Είναι απλούστατο να διαπιστώσει κανείς ότι το $K[v]$ είναι ακέραια περιοχή, υποδακτύλιος του σώματος L, εν γένει όμως, δεν είναι σώμα. Με $K(v)$ συμβολίζομε το σώμα πηλίκων της ακεραίας περιοχής $K[v]$. Τα στοιχεία δηλαδή του $K(v)$ είναι της μορφής $(a_0+a_1v+\ldots+a_nv^n)/(b_0+b_1v+\ldots+b_mv^m)$ με τά n και m οποιουσδήποτε μη αρνητικούς ακεραίους και τα στοιχεία a_i, b_j από το σώμα K (ο παρονομαστής υποτίθεται $\neq 0$).

Θεώρημα 1.1.3. *Αν το $v \in L$ είναι αλγεβρικό πάνω από το K, τότε ο δακτύλιος $K[v]$ είναι σώμα (υπόσωμα του L)· ειδικότερα, $K[v]=K(v)$*[1]*. Στην περίπτωση αυτή, υπάρχει ένα μοναδικό ανάγωγο, μονικό πολυώνυμο $q(X) \in K[X]$, ώστε $q(v)=0$. Το $K[v]$ είναι πεπερασμένη επέκταση του K, βαθμού $n=\deg q$ και τα στοιχεία $1, v, \ldots, v^{n-1}$ παράγουν τον K-διανυσματικό χώρο $K[v]$.*

[1] Έτσι, στο εξής, όταν π.χ. το v είναι αλγεβρικό πάνω από το K, θα μπορούμε ναχρησιμοποιούμε αδιακρίτως το συμβολισμό $K[v]$ εἴτε $K(v)$.

Απόδειξη. Για την απόδειξη του ότι το $K[v]$ είναι υπόσωμα του L αρκεί να δείξομε ότι κάθε μη μηδενικό στοιχείο-του έχει αντίστροφο. Κάθε τέτοιο στοιχείο είναι της μορφής $g(v)$ για κάποιο μη μηδενικό πολυώνυμο $g(X) \in K[X]$ το οποίο δεν έχει ρίζα το v.

Αφού το v έχει υποτεθεί αλγεβρικό πάνω από το K, υπάρχει μη μηδενικό $f(X) \in K[X]$ το οποίο έχει ρίζα το v. Αναλύοντας το f σε γινόμενο ανάγωγων πολυωνύμων του $K[X]$ βλέπομε ότι ένας τουλάχιστον από αυτούς, ας τον πούμε $q(X)$, έχει ρίζα του το v. Επειδή μπορούμε να διαιρέσομε το $q(X)$ με τον συντελεστή του μεγιστοβάθμιου όρου του, αν αυτός δεν είναι 1, το $q(X)$ μπορεί να υποτεθεί και μονικό. Τώρα θα κάνομε χρήση της Πρότασης B'.5 (Παράρτημα B') για ν' αποδείξομε ότι τα πολυώνυμα g και q είναι πρώτα μεταξύ τους. Πράγματι, σε αντίθετη περίπτωση, επειδή το q είναι ανάγωγο πολυώνυμο, θα έπρεπε να διαιρεί το g· αλλά τότε $g(v) = 0$ (αφού και $q(v) = 0$) και ερχόμαστε σε αντίφαση με την υπόθεσή μας για το $g(v)$. Αφού λοιπόν τα g και q είναι πρώτα μεταξύ τους, υπάρχουν πολυώνυμα h και r στο $K[X]$ ώστε να ισχύει $q(X)r(X) + g(X)h(X) = 1$. Η αντικατάσταση $X \leftarrow v$ δίνει τώρα $g(v)h(v) = 1$, που σημαίνει ότι το στοιχείο $h(v) \in K[v]$ είναι το αντίστροφο του $g(v)$.

Τώρα θα αποδείξομε ότι, εκτός από το q, δεν υπάρχει άλλο ανάγωγο, μονικό πολυώνυμο q_1, που να έχει ρίζα το v. Γιατί, αν αυτό συμβαίνει, αποκλείεται να είναι τα q, q_1 πρώτα μεταξύ τους (αν ήταν, θα εἴχαμε μία σχέση της μορφής $q(X)r(X) + q_1(X)r_1(X) = 1$ και η αντικατάσταση $v \leftarrow X$ θα μας οδηγούσε στην αδύνατη σχέση $0 + 0 = 1$. Έτσι, αφού το q είναι ανάγωγο και όχι πρώτο προς το q_1, πρέπει $q|q_1$. Εντελώς συμμετρικά όμως, αφού και το q_1 είναι ανάγωγο, $q_1|q$. Έτσι, τα q, q_1, είναι μονικά και αλληλοδιαιρούνται, άρα ταυτίζονται.

Έστω τώρα $q(X) = a_0 + a_1X + ... + a_{n-1}X^{n-1} + X^n$. Μένει να δείξομε ότι τα $1, v, ..., v^{n-1}$ αποτελούν βάση του K-διανυσματικού χώρου $K[v]$. Τα n αυτά στοιχεία είναι K-γραμμικώς ανεξάρτητα· διαφορετικά, θα είχαμε μία σχέση της μορφής $b_0 + b_1v + ... + b_{n-1}v^{n-1}$ για κάποια στοιχεία $b_0, b_1, ..., b_{n-1}$, που δεν είναι όλα μηδέν, δηλαδή, θα υπήρχε πολυώνυμο $h(X)$ βαθμού $\leq n-1$ με ρίζα το v. Τα q και h δεν θα ήταν τότε πρώτα μεταξύ τους (αυτό προκύπτει ακριβώς όπως και παραπάνω με τα q και q_1), άρα το q θα διαιρούσε το h, άτοπο, αφού $\deg h < \deg q$. Τέλος, τα $1, v, ..., v^{n-1}$ παράγουν το $K[v]$. Αρκεί να δείξομε ότι κάθε v^m, $m \geq n$ είναι K-γραμμικός συνδυασμός των $1, v, ..., v^{n-1}$: Πράγματι, για $m = n$ αυτό ισχύει, αφού από τη σχέση $q(v) = 0$ έπεται ότι $v^n = -a_0 - a_1v - ... - a_{n-1}v^{n-1}$ $(*)$. Επαγωγικά τώρα, άν $v^r = b_0 + b_1v + ... + b_{n-1}v^{n-1}$, με τα $b_i \in K$, τότε $v^{r+1} = b_0v + b_1v^2 + ... + b_{n-2}v^{n-1} + b_{n-1}v^n$ και αντικαθιστώντας το v^n από την $(*)$ εκφράζομε το v^{r+1} μόνο συναρτήσει των $1, v, ..., v^{n-1}$. □

Το $q(X) \in K[X]$, που περιγράφεται στην εκφώνηση του Θεωρήματος 1.1.3, λέγεται *ελάχιστο πολυώνυμο* του v πάνω από το K και συμβολίζεται $\mathrm{Irr}(v, K)$.

Έστω τώρα ότι $v_1, ..., v_r \in L$. Με $K[v_1, ..., v_r]$ συμβολίζομε το υποσύνολο του L, που αποτελείται από όλα τα πεπερασμένα αθροίσματα στοιχείων του L της μορφής $av_1^{n_1} \cdots v_r^{n_r}$ όπου $a \in K$ και $n_i \geq 0$ για κάθε $i = 1, ..., r$. Το $K[v_1, ..., v_r]$ είναι, προφανώς, δακτύλιος (αντιμεταθετικός).

Θεώρημα 1.1.4. *Έστω ότι L/K και M/L είναι πεπερασμένες επεκτάσεις. Τότε και η M/K είναι πεπερασμένη επέκταση καί, μάλιστα $[M : K] = [M : L] \cdot [L : K]$.*

Απόδειξη. Έστω $[L : K] = l$, $[M : L] = m$, $u_1, \dots, u_l$ μία K-βάση του L και $v_1, \dots, v_m$ μία L-βάση του M. Αρκεί να δείξομε ότι τα $u_i v_j$, $1 \leq i \leq l$, $1 \leq j \leq m$ είναι μία K-βάση του M. Πρώτα δείχνομε ότι τα στοιχεία αυτά παράγουν το M πάνω από το K. Έστω $v \in M$, οπότε

$$v = \sum_{i=1}^{m} a_i v_i \,, \qquad \text{για κάποια} \quad a_i \in L.$$

Αλλά για κάθε $i = 1, \dots, m$,

$$a_i = \sum_{j=1}^{l} b_{ij} u_j \,, \qquad \text{για κάποια} \quad b_{ij} \in K.$$

Αντικαθιστώντας τα a_i από την τελευταία σχέση στην προηγούμενη βλέπομε ότι το v είναι K-γραμμικός συνδυασμός των $v_i u_j$. Όσον αφορά στην K-ανεξαρτησία αυτών των στοιχείων, ας θεωρήσομε τη σχέση

$$\sum_{1 \leq i \leq l \,,\, 1 \leq j \leq m} b_{ij} u_i v_j = 0 \,, \qquad \text{για κάποια} \quad b_{ij} \in K.$$

Αυτή γράφεται

$$\sum_{j=1}^{m} \left(\sum_{i=1}^{l} b_{ij} u_i \right) v_j = 0.$$

Λόγω της L-γραμμικής ανεξαρτησίας των v_j, πρέπει κάθε εσωτερικό άθροισμα στην τελευταία σχέση να είναι μηδέν. Δηλαδή, για κάθε $j = 1, \dots, m$,
$b_{1j} u_1 + \dots + b_{lj} u_l = 0$, και από την K-ανεξαρτησία των u_i, έπεται τώρα ότι όλα τα b_{ij} είναι μηδέν. □

Θεώρημα 1.1.5. *Αν $v_1, \dots, v_r \in L$, το v_1 είναι αλγεβρικό πάνω από το K και για κάθε $i = 2, \dots, r$ το v_i είναι αλγεβρικό πάνω από το $K[v_1, \dots, v_{i-1}]$* [2] *(ειδικότερα, αν όλα τα v_i είναι αλγεβρικά πάνω από το K), ο δακτύλιος $K[v_1, \dots, v_r]$ είναι υπόσωμα του L, πεπερασμένη επέκταση του K.*

Απόδειξη. Σύμφωνα με το Θεώρημα 1.1.3, η $K[v_1]/K$ είναι πεπερασμένη επέκταση. Εύκολα διαπιστώνεται ότι $K[v_1, v_2] = (K[v_1])[v_2]$ και επειδή, εξ υποθέσεως, το v_2 είναι αλγεβρικό πάνω από το $K[v_1]$, το Θεώρημα 1.1.3 συνεπάγεται ότι η επέκταση $K[v_1, v_2]$ είναι, επίσης, σώμα και, μάλιστα, πεπερασμένη επέκταση του $K[v_1]$. Τώρα, έχομε τις διαδοχικές πεπερασμένες επεκτάσεις $K[v_1]/K$ και $K[v_1, v_2]/K[v_1]$, άρα, από το Θεώρημα 1.1.4 συμπεραίνομε ότι η επέκταση $K[v_1, v_2]/K$ είναι πεπερασμένη. Στή συνέχεια προχωρούμε εντελώς ανάλογα, βασιζόμενοι στο ότι $K[v_1, v_2, v_3] = (K[v_1, v_2])[v_3]$ και στην υπόθεση ότι το v_3 είναι αλγεβρικό πάνω από το $K[v_1, v_2]$, κ.ό.κ. μέχρις ότου καταλήξομε στο ότι η $K[v_1, \dots, v_r]/K$ είναι αλγεβρική επέκταση. □

Θεώρημα 1.1.6. *Κάθε πεπερασμένη επέκταση του K είναι αλγεβρική επέκταση του K.*

[2] Πρόκειται περί σώματος, όπως θα φανεί στην απόδειξη.

Απόδειξη. Έστω L/K πεπερασμένη επέκταση και $v \in L$. Επειδή είναι αδύνατον να υπάρχουν άπειρα στοιχεία του L γραμμικώς ανεξάρτητα πάνω από το K, έπεται για κάποιον ακέραιο $n \geq 1$ τα $1, v, \ldots, v^n$ είναι K-γραμμικώς εξηρτημένα. Αυτό σημαίνει ότι υπάρχουν $a_0, \ldots, a_n \in K$, όχι όλα μηδέν, ώστε να ισχύει $a_0 + a_1 v + \ldots + a_n v^n = 0$, δηλαδή το v είναι ρίζα ενός μη μηδενικού πολυωνύμου με συντελεστές από το K· άρα το τυχόν $v \in L$ είναι αλγεβρικό πάνω από το K. □

Θεώρημα 1.1.7. *Αν το K είναι υπόσωμα του σώματος L, τότε το υποσύνολο A του L, το αποτελούμενο από τα στοιχεία του L που είναι αλγεβρικά πάνω από το K, είναι υπόσωμα του L (προφανώς, $K \subseteq A$).*

Απόδειξη. Αρκεί να δειχθεί ότι, αν $a, b \in A$ τότε $a - b, ab \in A$, καθώς και $a^{-1} \in A$ για $a \neq 0$. Από το Θεώρημα 1.1.5 έχομε ότι το $K[a, b]$ είναι σώμα, πεπερασμένη επέκταση του K, άρα και αλγεβρική επέκταση του K, λόγω του Θεωρήματος 1.1.6. Συνεπώς, κάθε στοιχείο του $K[a, b]$ είναι αλγεβρικό πάνω από το K. Αλλά αφού το $K[a, b]$ είναι σώμα, τα $a - b, ab, a^{-1}$ ανήκουν σε αυτό, άρα είναι αλγεβρικά πάνω από το K, δηλαδή ανήκουν στο A. □

Αν θεωρήσομε ως L το $\mathbb{C}$ και ως K το $\mathbb{Q}$, τότε το σύνολο A του Θεωρήματος 1.1.7 συμβολίζομε με $\mathbf{A}$ και το ονομάζομε *σώμα των αλγεβρικών αριθμών* . Δηλαδή:

> Ένας μιγαδικός αριθμός χαρακτηρίζεται *αλγεβρικός* αν είναι ρίζα ενός μη μηδενικού πολυωνύμου με ρητούς συντελεστές· στην αντίθετη περίπτωση χαρακτηρίζεται *υπερβατικός* .

Το σύνολο των υπερβατικών αριθμών είναι μη κενό. Η απλούστερη απόδειξη είναι έμμεση-συνολοθεωρητική και οφείλεται στον Cantor: Αποδεικνύεται πρώτα ότι το $\mathbb{R}$ είναι μη αριθμήσιμο σύνολο και μετά ότι το σύνολο $\mathbf{A}$ είναι αριθμήσιμο, οπότε προκύπτει ότι το $\mathbb{R} \setminus \mathbf{A}$, δηλαδή το σύνολο των πραγματικών υπερβατικών αριθμών, είναι μη κενό. Το μειονέκτημα αυτής της μεθόδου είναι ότι δεν μας παρέχει τρόπο κατασκευής έστω και ενός υπερβατικού αριθμού. Ο Liouville ήταν ο πρώτος που έδωσε (στα 1844) παράδειγμα υπερβατικού αριθμού. Συγκεκριμένα, απέδειξε ότι ο αριθμός $\xi = \sum_{n=1}^{\infty} 10^{-n!}$ είναι υπερβατικός. Στα 1873, ο Hermitte απέδειξε την υπερβατικότητα του e, ενώ η υπερβατικότητα του π αποδείχθηκε από τον Lindemann στα 1882.

Ασκησεις

1. Να βρεθούν βάσεις και οι βαθμοί των εξής επεκτάσεων: $\mathbb{R}(\sqrt{5})/\mathbb{R}$, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $\mathbb{Q}(\sqrt[7]{3})/\mathbb{Q}$, $\mathbb{Q}(\rho)$, όπου ρ είναι ρίζα του $\mathrm{X}^3 + 3\mathrm{X} + 3$, $\mathbb{Q}(\sqrt{5}, \sqrt{7})/\mathbb{Q}$.

2. Αν $[L : K] = 1$, τότε $L = K$.

3. Αν ο βαθμός $[L : K]$ είναι πρώτος, τότε δεν υπάρχει *γνήσια* επέκταση του K, η οποία ναπεριέχεται *γνησίως* στο L.

4. Αν η L/K είναι πεπερασμένη επέκταση και έχομε τις διαδοχικές επεκτάσεις

$$L/K_r/K_{r-1}/\ldots/K_1/K,$$

τότε

$$[L : K] = [L : K_r][K_r : K_{r-1}] \dots [K_2 : K_1][K_1 : K].$$

5. Δείξτε ότι η επέκταση L/K είναι πεπερασμένη αν και μόνο αν υπάρχει ένας φυσικός αριθμός r και $a_1, \dots, a_r \in L$, αλγεβρικά πάνω από το K, έτσι ώστε $L = K(a_1, \dots, a_r)$.

6. Αν $\mathbf{A}$ είναι το σώμα των αλγεβρικών αριθμών, δείξτε ότι η επέκταση $\mathbf{A}/\mathbb{Q}$ δεν είναι πεπερασμένη.

   Υπόδειξη. Χρησιμοποιήστε το κριτήριο Eisenstein προκειμένου να αποδείξετε ότι υπάρχουν ανάγωγα πολυώνυμα πάνω από το $\mathbb{Q}$ οσοδήποτε μεγάλου βαθμού.

7. Έστω $\mathbf{A}$ όπως στην προηγούμενη άσκηση. Θεωρώντας γνωστό ότι κάθε μιγαδικό πολυώνυμο έχει μιγαδική ρίζα («Θεμελιώδες Θεώρημα της Αριθμητικής» του Gauss), αποδείξτε ότι κάθε μη σταθερό πολυώνυμο με συντελεστές από το $\mathbf{A}$ έχει ρίζα στο $\mathbf{A}$. Ως συνέπεια αυτού δείξτε ότι δεν υπάρχει γνήσια αλγεβρική επέκταση του $\mathbf{A}$.

8. Δείξτε ότι $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

9. Βρείτε μία βάση και το βαθμό της επέκτασης $\mathbb{Q}\left(\sqrt{1 + \sqrt{3}}\right)/\mathbb{Q}$.

10. Αν ο βαθμός της επέκτασης L/K είναι πρώτος αριθμός, τότε υπάρχει $u \in L$, ώστε $L = K(u)$ (είναι, δηλαδή, η επέκταση L/K *απλή*, όπως λέμε).

11. Δείξτε ότι το πολυώνυμο $f(X) = X^3 - 3X + 15 \in \mathbb{Q}[X]$ είναι ανάγωγο. Θεωρήστε την επέκταση $\mathbb{Q}(\rho)/\mathbb{Q}$ και εκφράστε το $(3 + \rho)^{-1}$ ως στοιχείο του $\mathbb{Q}[\rho]$ (δηλαδή, ως πολυωνυμική έκφραση του ρ).

    Απάντηση: $2 - \rho + \frac{1}{3}\rho^2$.

12. Πάρετε ως δεδομένο ότι το πολυώνυμο $f(X) = X^4 + 2X^2 - 1 \in \mathbb{Q}[X]$ είναι ανάγωγο. Θεωρήστε την επέκταση $\mathbb{Q}(\rho)/\mathbb{Q}$ και εκφράστε το $(1+\rho)^{-1}$ ως στοιχείο του $\mathbb{Q}[\rho]$ (δηλαδή, ως πολυωνυμική έκφραση του ρ).

    Απάντηση: $\frac{3}{2} - \frac{3}{2}\rho + \frac{1}{2}\rho^2 - \frac{1}{2}\rho^3$.

1.2 Κατασκευες με κανονα και διαβητη

Έστω S_0 ένα σύνολο σημείων του $\mathbb{R}^2$ (επίπεδο). Λέμε ότι ένα σημείο του επιπέδου είναι *άμεσα κατασκευάσιμο* (με κανόνα και διαβήτη) από το S_0 αν είναι σημείο τομής δύο ευθειών, ή μιάς ευθείας και ενός κύκλου, ή δύο κύκλων, που προκύπτουν ως εξής: Η μεν ευθεία διέρχεται από δύο σημεία του S_0, ο δε κύκλος έχει ως κέντρο του ένα σημείο του S_0 και η ακτίνα του ισούται με την απόσταση δύο σημείων του S_0. Λέμε ότι ένα σημείο του επιπέδου *κατασκευάζεται* (με κανόνα και διαβήτη) από το S_0 αν υπάρχει πεπερασμένο πλήθος σημείων $s_1, s_2, \dots, s_n$, έτσι ώστε (1) το s_1 να είναι άμεσα κατασκευάσιμο από το S_0, (2) για κάθε $i = 2, \dots, n$, το s_i να είναι άμεσα κατασκευάσιμο από το $S_0 \cup \{s_1, \dots, s_{i-1}\}$ και (3) $s_n = s$.

Συμβολίζομε τώρα με K_0 το υπόσωμα του $\mathbb{R}$ που παράγεται από τις συντεταγμένες όλων των σημείων του S_0. Είναι δηλαδή το K_0 το ελάχιστο υπόσωμα του $\mathbb{R}$ που περιέχει τις συντεταγμένες όλων των σημείων του S_0.

Θεώρημα 1.2.1. *Αν οι συντεταγμένες όλων των σημείων ενός συνόλου $S \subset \mathbb{R}^2$ περιέχονται σε ένα υπόσωμα K του $\mathbb{R}$ και το σημείο $s = (x, y)$ είναι άμεσα κατασκευάσιμο από το S, τότε τα x, y είναι αλγεβρικά πάνω από το K και η επέκταση $K(x, y)/K$ είναι βαθμού 1 ή 2.*

Απόδειξη. Αν μία ευθεία διέρχεται από δύο σημεία του S, τότε οι συντεταγμένες αυτών των σημείων ανήκουν στο K και, συνεπώς, η εξίσωση της ευθείας που ορίζουν έχει τη μορφή $ax + by + c = 0$ με $a, b, c \in K$. Αυτές τις ευθείες ας τις λέμε σε τούτη την απόδειξη *S-ευθείες*. Επίσης, αν ένας κύκλος έχει κέντρο ένα σημείο $(x_0, y_0) \in S$ και ακτίνα r ίση με την απόσταση δύο σημείων (x_1, y_1), (x_2, y_2) του S, τότε $x_0, x_1, x_2, y_0, y_1, y_2 \in K$ και η εξίσωση του κύκλου είναι $(x - x_0)^2 + (y - y_0)^2 = r^2 = (x_2 - x_1)^2 + (y_2 - y_1)^2$, δηλαδή είναι της μορφής $x^2 + y^2 + ax + by + c = 0$, με $a, b, c \in K$. Αυτούς τους κύκλους ας τους λέμε *S-κύκλους*. Συνεπώς, από αυτά που μόλις είπαμε προκύπτουν τα εξής:

- Το σημείο τομής (x, y) δύο S-ευθειών προκύπτει από την επίλυση ενός συστήματος

$$a_1x + b_1y + c_1 = 0, \quad a_2x + b_2y + c_2 = 0, \quad a_1, b_1, c_1, a_2, b_2, c_2 \in K.$$

Καθώς το σύστημα είναι γραμμικό με συντελεστές στο K, οι αριθμοί x, y που προκύπτουν από την επίλυσή του ανήκουν στο K. Άρα οι συντεταγμένες του σημείου που προκύπτει από την τομή των δύο ευθειών δεν δημιουργούν γνήσια επέκταση του K.

- Τα σημεία τομής (x, y) μιας S-ευθείας και ενός S-κύκλου είναι λύσεις ενός συστήματος

$$a_1x + b_1y + c_1 = 0, \quad x^2 + y^2 + a_2x + b_2y + c_2 = 0, , \quad a_1, b_1, c_1, a_2, b_2, c_2 \in K.$$

Ένας τουλάχιστον από τους συντελεστές a_1, b_1 είναι μη μηδενικός, έστω ο b_1. Λύνοντας την εξίσωση αυτή ως προς y, παίρνομε $y = \lambda x + \mu$, όπου $\lambda, \mu \in K$. Αντικαθιστώντας αυτή την έκφραση του y στη δεύτερη εξίσωση, οδηγούμαστε σε μια δευτεροβάθμια εξίσωση $\alpha x^2 + \beta x + \gamma = 0$, με $\alpha, \beta, \gamma \in K$. Οι x-συντεταγμένες των σημείων τομής δίδονται από τις σχέσεις $x = (-\beta \pm \sqrt{\Delta})/(2\alpha)$, όπου $\Delta = \beta^2 - 4\alpha\gamma \in K$, άρα ανήκουν στην επέκταση $K(\sqrt{\Delta})$ του K. Λόγω

της σχέσης $y = \lambda x + \mu$, είναι, επίσης, $y \in K(\sqrt{\Delta})$. Συνεπώς, οι συντεταγμένες των σημείων τομής της ευθείας και του κύκλου περιέχονται στην επέκταση $K(\sqrt{\Delta})$, της οποίας ο βαθμός είναι $[K(\sqrt{\Delta}) : K] = 1$ ή 2 (ο βαθμός ισούται με 1 αν και μονο αν $\sqrt{\Delta} \in K$, που συμβαίνει όταν, ακριβώς, $\Delta = k^2$ με $k \in K$).

- Τα σημεία τομής (x, y) δύο S-κύκλων είναι λύσεις ενός συστήματος

$$x^2 + y^2 + a_1x + b_1y + c_1 = 0, \quad x^2 + y^2 + a_2x + b_2y + c_2 = 0, \quad a_1, b_1, c_1, a_2, b_2, c_2 \in K.$$

Αντικαθιστώντας την πρώτη εξίσωση από τη διαφορά των δύο εξισώσεων, προκύπτει το ισοδύναμο σύστημα

$$(a_2 - a_1)x + (b_2 - b_1)y + (c_2 - c_1) = 0, \quad x^2 + y^2 + a_2x + b_2y + c_2 = 0,$$

το οποίο είναι της ίδιας μορφής με αυτό της προηγούμενης περίπτωσης (τομή ευθείας και κύκλου). Συνεπώς, οι συντεταγμένες των νέων σημείων τομής ανήκουν, και πάλι, σε μια επέκταση του K, βαθμού 1 ή 2. □

Έστω τώρα ότι το s είναι κατασκευάσιμο από το σύνολο S_0 και τα σημεία $s_1, s_2, \dots, s_n = s$ μας οδηγούν από το S_0 στην κατασκευή του s. Θέτομε $s_i = (a_i, b_i)$ και έστω K_0 το υπόσωμα του $\mathbb{R}$, που ορίσαμε στην αρχή. Έχομε τότε τις εξής διαδοχικές επεκτάσεις: K_1/K_0, όπου $K_1 = K_0(a_1, b_1)$, K_2/K_1, όπου $K_2 = K_1(a_2, b_2)$, κ.λ.π. K_n/K_{n-1}, όπου $K_n = K_{n-1}(a_n, b_n)$. Από την άσκηση 4 της ενότητας 1.1 και το Θεώρημα 1.2.1, έχομε

$$[K_n : K_0] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \dots [K_2 : K_1][K_1 : K_0] = \text{δύναμη του 2.}$$

Αποδείξαμε δηλαδή το εξής

Θεώρημα 1.2.2. *Αν το σημείο s είναι κατασκευάσιμο από το σύνολο σημείων S_0 και K_0 είναι το ελάχιστο σώμα που περιέχει τις συντεταγμένες όλων των σημείων του S_0, τότε υπάρχει πεπερασμένη επέκταση του K_0, που περιέχει τις συντεταγμένες του s και είναι βαθμού ίσου με δύναμη του 2.*

Τώρα έχομε όλα τα απαραίτητα εφόδια για ν' αποδείξομε ότι είναι αδύνατον να δοθεί λύση με κανόνα και διαβήτη στά τρία περίφημα γεωμετρικά προβλήματα της αρχαιότητας: *Διπλασιασμός του κύβου, τριχοτόμηση γωνίας, τετραγωνισμός του κύκλου.*

Θεώρημα 1.2.3. *Ο διπλασιασμός του κύβου με κανόνα και διαβήτη είναι αδύνατος.*

Απόδειξη. Ας υποθέσομε ότι μας δίνεται ο μοναδιαίος κύβος. Για να πετύχομε το διπλασιασμό του, πρέπει να κατασκευάσομε ένα ευθύγραμμο τμήμα (την ακμή του νέου κύβου) με μήκος $\sqrt[3]{2}$. Εδώ, το μόνο μας δεδομένο είναι το μοναδιαίο μήκος (η ακμή του αρχικού κύβου). Άρα, $S_0 = \{(0, 0), (1, 0)\}$, οπότε $K_0 = \mathbb{Q}$. Πρέπει να κατασκευάσομε με κανόνα και διαβήτη το σημείο $s = (x, 0)$, όπου $x = \sqrt[3]{2}$. Αν αυτό γινόταν, θα υπήρχε πεπερασμένη επέκταση K

του $\mathbb{Q}$ με $x \in K$ και $[K : \mathbb{Q}] =$ δύναμη του 2 (Θεώρημα 1.2.2). Επειδή το x είναι ρίζα του αναγώγου πολυωνύμου $X^3 - 2 \in \mathbb{Q}[X]$, είναι $[\mathbb{Q}(x) : \mathbb{Q}] = 3$. Λόγω των διαδοχικών επεκτάσεων $K/\mathbb{Q}(x)/\mathbb{Q}$ και του Θεωρήματος 1.1.4, θα έπρεπε,

$$\text{δύναμη του } 2 \ = [\mathrm{K} : \mathbb{Q}] = [K : \mathbb{Q}(x)][\mathbb{Q}(x) : \mathbb{Q}] = \ \text{πολλαπλάσιο του } 3,$$

άτοπο. □

Θεώρημα 1.2.4. *Η γωνία $\pi/3$ δεν είναι δυνατόν να τριχοτομηθεί με κανόνα και διαβήτη. Συνεπώς, δεν υπάρχει γενική γεωμετρική μέθοδος τριχοτόμησης γωνιών με τη χρήση κανόνα και διαβήτη.*

Απόδειξη. Έχομε στη διάθεσή μας το μοναδιαίο τριγωνομετρικό κύκλο, οπότε, μία γωνία είναι κατασκευάσιμη αν, και μόνο αν, το συνημίτονο της γωνίας (θεωρούμενο ως ευθύγραμμο τμήμα στον άξονα των συνημιτόνων) είναι κατασκευάσιμο. Εδώ, $S_0 = \{(0,0),(1,0)\}, K_0 = \mathbb{Q}$ και ζητούμε να κατασκευάσομε το σημείο $s = (x, 0), x = \cos\frac{\pi}{9}$. Αν αυτό ήταν δυνατόν, θα υπήρχε επέκταση $K/\mathbb{Q}$ με $x \in K$ και $[K : \mathbb{Q}] =$ δύναμη του 2 (Θεώρημα 1.2.2). Όμως, λόγω της σχέσης

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

έχομε, για $\theta = \pi/9$,

$$\frac{1}{2} = 4x^3 - 3x \ \ \text{ή} \ \ 8x^3 - 6x - 1 = 0.$$

Το x είναι, λοιπόν, ρίζα ενός κυβικού αναγώγου (όπως διαπιστώνεται εύκολα) πολυωνύμου του $\mathbb{Q}[X]$. Άρα, $[\mathbb{Q}(x) : \mathbb{Q}] = 3$, και όπως στο Θεώρημα 1.2.3, οδηγούμαστε σε άτοπο. □

Θεώρημα 1.2.5. *Ο τετραγωνισμός του κύκλου είναι αδύνατος με κανόνα και διαβήτη.*

Απόδειξη. Μπορούμε να υποθέσομε ότι μας δίνουν ένα κύκλο μοναδιαίας ακτίνας, οπότε έχομε να κατασκευάσομε ένα τετράγωνο εμβαδού π, άρα να κατασκευάσομε ευθύγραμμο τμήμα (πλευρά του τετραγώνου) μήκους $\sqrt{\pi}$. Ξεκινούμε πάλι από το $S_0 = \{(0,0),(1,0)\}, K_0 = \mathbb{Q}$. Η δυνατότητα κατασκευής ευθυγράμμου τμήματος μήκους $\sqrt{\pi}$ συνεπάγεται (με τη βοήθεια των στοιχειωδών γεωμετρικών κατασκευών της Ευκλείδιας Γεωμετρίας) τη δυνατότητα κατασκευής ευθυγράμμου τμήματος μήκους π. Συνεπώς (Θεώρημα 1.2.2), υπάρχει πεπερασμένη επέκταση του $\mathbb{Q}$, που περιέχει τόν αριθμό $\pi\cdot$ ειδικότερα, λόγω του Θεωρήματος 1.1.6, αυτό συνεπάγεται ότι ο αριθμός π είναι αλγεβρικός. Όμως, όπως αναφέραμε προηγουμένως, έχει αποδειχθεί ότι ο π είναι υπερβατικός και αυτή η αντίφαση ολοκληρώνει την απόδειξη. □

Ασκησεις

1. Αποδείξτε ότι η κατασκευή του κανονικού 9-γώνου με κανόνα και διαβήτη είναι αδύνατη.

2. Αποδείξτε ότι η γωνία θ μπορεί να τριχοτομηθεί με κανόνα και διαβήτη αν και μόνο αν το πολυώνυμο $4X^3 - 3X - \cos\theta \in \mathbb{Q}(\cos\theta)[X]$ είναι σύνθετο (δηλαδή, όχι ανάγωγο) πάνω από το $\mathbb{Q}(\cos\theta)$.

Ένα παράδειγμα. Η γωνία θ με $\cos\theta = (5 - 7\sqrt{2})/16$ (είναι η γωνία με προσεγγιστική τιμή $107,8315^o$) τριχοτομείται, γιατί το πολυώνυμο $4X^3 - 3X - \frac{5-7\sqrt{2}}{16}$ παραγοντοποείται πάνω από το $\mathbb{Q}(\sqrt{2})$: έχει ρίζα το $\frac{-1+\sqrt{2}}{4}$.

3. Με τη βοήθεια της ισότητας $90 - 2 \cdot 18 = 3 \cdot 18$ δείξτε (εφαρμόζοντας στα δύο μέλη τη συνάρτηση cos) ότι $\sin 18^o = (-1 + \sqrt{5})/4$ και συμπεράνετε ότι η γωνία 18^o κατασκευάζεται με κανόνα και διαβήτη. Έχοντας αυτό ως δεδομένο και κάνοντας χρήση του τύπου για το $\cos 5\theta$ δείξτε ότι το κανονικό πεντάγωνο κατασκευάζεται με κανόνα και διαβήτη.

1.3 Κατασκευη πεπερασμενων επεκτασεων δοθεντος σωματος

Ξεκινούμε με ένα παράδειγμα. Θεωρούμε το $f(X) = X^2 + 1 \in \mathbb{Z}_3[X]$. Πρίν προχωρήσομε, τονίζομε ότι τα στοιχεία του $\mathbb{Z}_3$ δεν πρέπει να συγχέονται με τους ακέραιους αριθμούς, παρά το ότι συμβολίζονται όπως οι ακέραιοι. Για παράδειγμα, ας θυμηθούμε ότι στο σώμα $\mathbb{Z}_3$ ισχύει $1 + 2 = 0$, $-1 = 2$ κλπ κάτι, βέβαια, που δεν ισχύει στούς ακεραίους. Με ένα απλό υπολογισμό διαπιστώνομε ότι το $f(X)$ δεν έχει ρίζα στο $\mathbb{Z}_3$. Το ερώτημα, λοιπόν είναι: *Υπάρχει κάποιο σώμα K, που περιέχει το $\mathbb{Z}_3$, εντός του οποίου το $f(X)$ να έχει ρίζα;*

Η απάντηση είναι καταφατική: από το Θεώρημα A'.5 του Παραρτήματος A', ξέρομε ότι υπάρχει επέκταση $L/\mathbb{Z}_3$ και στοιχείο $\rho \in L$ έτσι ώστε $\rho^2+1 = 0$ και $L = \mathbb{Z}_3[\rho]$. Τώρα, σύμφωνα με το Θεώρημα 1.1.3, τα $1, \rho$ αποτελούν βάση της επέκτασης $L/\mathbb{Z}_3$, άρα $L = \{a+b\rho : a, b \in \mathbb{Z}_3\}$. Συνεπώς

$$L = \{0,\ 1,\ 2,\ \rho,\ 1+\rho,\ 2+\rho,\ 2\rho,\ 1+2\rho,\ 2+2\rho\}.$$

Επίσης, δεδομένου ότι το L είναι σώμα, οι πράξεις του L είναι αντιμεταθετικές και ικανοποιούν τις εξής απαιτήσεις (έχοντας πάντα κατά νου ότι τα $0, 1, 2$ είναι στοιχεία του $\mathbb{Z}_3$, ενώ $\rho^2+1 = 0$):

$$(a_1 + b_1\rho) + (a_2 + b_2\rho) = (a_1 + a_2) + (b_1 + b_2)\rho$$

και

$$\begin{aligned}(a_1 + b_1\rho) \cdot (a_2 + b_2\rho) &= a_1a_2 + a_1(b_2\rho) + (b_1\rho)a_2 + (b_1\rho)(b_2\rho)\\ &= a_1a_2 + a_1b_2\rho + b_1a_2\rho + b_1b_2\rho^2\\ &= (a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2)\rho\,.\end{aligned}$$

Με βάση τα παραπάνω, κατασκευάζονται οι πίνακες πρόσθεσης και πολλαπλασιασμού των 9 στοιχείων:

Πίνακας πρόσθεσης

$+$	0	1	2	ρ	$1+\rho$	$2+\rho$	2ρ	$1+2\rho$	$2+2\rho$
0	0	1	2	ρ	$1+\rho$	$2+\rho$	2ρ	$1+2\rho$	$2+2\rho$
1	1	2	0	$1+\rho$	$2+\rho$	ρ	$1+2\rho$	$2+2\rho$	2ρ
2	2	0	1	$2+\rho$	ρ	$1+\rho$	$2+2\rho$	2ρ	$1+2\rho$
ρ	ρ	$1+\rho$	$2+\rho$	2ρ	$1+2\rho$	$2+2\rho$	0	1	2
$1+\rho$	$1+\rho$	$2+\rho$	ρ	$1+2\rho$	$2+2\rho$	2ρ	1	2	0
$2+\rho$	$2+\rho$	ρ	$1+\rho$	$2+2\rho$	2ρ	$1+2\rho$	2	0	1
2ρ	2ρ	$1+2\rho$	$2+2\rho$	0	1	2	ρ	$1+\rho$	$2+\rho$
$1+2\rho$	$1+2\rho$	$2+2\rho$	2ρ	1	2	0	$1+\rho$	$2+\rho$	ρ
$2+2\rho$	$2+2\rho$	2ρ	$1+2\rho$	2	0	1	$2+\rho$	ρ	$1+\rho$

Πίνακας πολλαπλασιασμού

$\cdot$	1	2	ρ	$1+\rho$	$2+\rho$	2ρ	$1+2\rho$	$2+2\rho$
1	1	2	ρ	$1+\rho$	$2+\rho$	2ρ	$1+2\rho$	$2+2\rho$
2	2	1	2ρ	$2+2\rho$	$1+2\rho$	ρ	$2+\rho$	$1+\rho$
ρ	ρ	2ρ	2	$2+\rho$	$2+2\rho$	1	$1+\rho$	$1+2\rho$
$1+\rho$	$1+\rho$	$2+2\rho$	$2+\rho$	2ρ	1	$1+2\rho$	2	ρ
$2+\rho$	$2+\rho$	$1+2\rho$	$2+2\rho$	1	ρ	$1+\rho$	2ρ	2
2ρ	2ρ	ρ	1	$1+2\rho$	$1+\rho$	2	$2+2\rho$	$2+\rho$
$1+2\rho$	$1+2\rho$	$2+\rho$	$1+\rho$	2	2ρ	$2+2\rho$	ρ	1
$2+2\rho$	$2+2\rho$	$1+\rho$	$1+2\rho$	ρ	2	$2+\rho$	1	2ρ

Έστω πεπερασμένο σώμα K. Η χαρακτηριστική του K είναι πρώτος αριθμός (γνωστό από την Άλγεβρα), έστω p. Αν 1_K είναι το μοναδιαίο στοιχείο του K, τότε η απεικόνιση $\mathbb{Z}_p \ni m \mapsto m\cdot 1_K \in K$ είναι μονομορφισμός σωμάτων, επομένως το K είναι επέκταση του $\mathbb{Z}_p$. Αφού το σώμα K είναι πεπερασμένο, η επέκταση $K/\mathbb{Z}_p$ είναι (προφανώς) πεπερασμένη. Έστω $[K:\mathbb{Z}_p]=n$ και $u_1,\dots,u_n \in K$ μια βάση της επέκτασης. Τότε,

$$K=\{a_1u_1+\cdots+a_nu_n : a_1,\dots,a_n\in\mathbb{Z}_p\}.$$

Καθώς τα $u_1,\dots,u_n$ είναι $\mathbb{Z}_p$-γραμμικώς ανεξάρτητα, διαφορετικές (διατεταγμένες) n-άδες $(a_1,\dots,a_n)$ αντιστοιχούν σε διαφορετικά στοιχεία του K και, συνεπώς, το πλήθος των στοιχείων του K είναι όσες και οι n-άδες αυτές, δηλαδή, p^n. Συμπέρασμα:

> Το πλήθος των στοιχείων ενός πεπερασμένου σώματος είναι πάντα ίσο με δύναμη κάποιου πρώτου αριθμού.

Αποδεικνύεται ότι, για κάθε πρώτο p και κάθε θετικό ακέραιο n υπάρχει σώμα του οποίου το πλήθος των στοιχείων είναι, ακριβώς, p^n. Επιπλέον, όλα τα σώματα με τον ίδιο πληθάριθμο p^n είναι ισόμορφα.

Αν μας δοθεί ένα πολυώνυμο $f(X)\in\mathbb{Z}_p[X]$ (p πρώτος) βαθμού $n>1$, ανάγωγο πάνω από το $\mathbb{Z}_p$, τότε, κατ' αναλογία με το παράδειγμα στην αρχή αυτής της ενότητας, θεωρούμε επέκταση $L[\rho]$ του $\mathbb{Z}_p$, στην οποία ισχύει $f(\rho)=0$. Σύμφωνα με το Θεώρημα 1.1.3, τα $1,\rho,\dots,\rho^{n-1}$ αποτελούν βάση της επέκτασης $L/\mathbb{Z}_p$. Συνεπώς, $K=\{a_0+a_1\rho+\cdots+a_{n-1}\rho^{n-1} : a_0,a_1,\dots,a_{n-1}\in\mathbb{Z}_p\}$, άρα ο πληθάριθμος του K είναι p^n.

Ασκησεις

1. Κατασκευάστε σώμα με 8 στοιχεία. Δηλαδή, περιγράψτε την κατασκευή του και φτιάξτε τους πίνακες των πράξεών του.

   Υπόδειξη. Θεωρήστε το πολυώνυμο $p(X)=X^3+X+1\in\mathbb{Z}_2[X]$ και διαπιστώστε ότι είναι ανάγωγο.

Εφαρμόστε το Θεώρημα A'.5 του Παραρτήματος A', και εργασθείτε κατ' αναλογία με το παράδειγμα του σώματος των 9 στοιχείων.

1.4 Σωμα αναλυσης πολυωνυμου

Στην ενότητα 1.3 είδαμε ότι, αν έχομε ένα σώμα K και ένα ανάγωγο $p(X) \in K[X]$, τότε υπάρχει επέκταση L του K, μέσα στην οποία το $p(X)$, θεωρούμενο ως πολυώνυμο του $L[X]$, έχει μία τουλάχιστον ρίζα, έστω $\lambda \in L$ και μάλιστα, $L = K(\lambda)$. Δεν αποκλείεται να περιέχει το L κι άλλες ρίζες του $p(X)$, αλλά αυτό δεν είναι ο κανόνας. Πολύ περισσότερο δεν είναι κανόνας να περιέχονται *όλες* οι ρίζες του $p(X)$ στο L. Τί σημαίνει, όμως, να περιέχονται όλες οι ρίζες του $p(X)$ στο L; Ο παρακάτω ορισμός δίνει μα πρώτη ιδέα για το πώς προσεγγίζεται αυτό το ζήτημα.

Ορισμός 1.4.1. *Έστω σώμα K και μη σταθερό $f \in K[X]$ βαθμού n. Η επέκταση L του K λέγεται σώμα ανάλυσης του f αν υπάρχουν $\rho_1, \dots, \rho_n \in L$ ώστε να ισχύει $f(X) = c(X - \rho_1) \dots (X - \rho_n)$ για κάποιο $c \in K$ (ο συντελεστής του μεγιστοβαθμίου όρου του f) και $L = K(\rho_1, \dots, \rho_n)$.*

Σημείωση: Σημαντικό! Το σώμα ανάλυσης εξαρτάται ουσιωδώς από το σώμα K· δείτε, οπωσδήποτε, την άσκηση 2. Γι' αυτό, ακριβέστερο (και ασφαλέστερο) είναι να λέμε π.χ. ότι το L είναι σώμα ανάλυσης του f *πάνω από το* K, ή, συντομώτερα, ότι το L είναι σώμα ανάλυσης του $f \in K[X]$, υποδηλώνοντας σαφώς ποιός είναι ο βασικός δακτύλιος πολυωνύμων στον οποίο θεωρούμε ότι ανήκει το f.

Θεώρημα 1.4.2. *Κάθε μη σταθερό πολυώνυμο με συντελεστές από ένα σώμα K έχει σώμα ανάλυσης πάνω από το K.*

Απόδειξη. Επαγωγικά επί του βαθμού του πολυωνύμου. Κατ' αρχάς, είναι προφανές ότι όλα τα πολυώνυμα πρώτου βαθμού με συντελεστές από ένα οποιοδήποτε σώμα K έχουν σώμα ανάλυσης τό ίδιο το K. Ας υποθέσομε ότι, για κάποιο $n \geq 2$, όλα τα πολυώνυμα βαθμού $< n$ με συντελεστές από οποιοδήποτε σώμα, έχουν σώμα ανάλυσης. Θεωρούμε τώρα ένα πολυώνυμο f βαθμού n με συντελεστές από κάποιο σώμα K. Έστω p ένας ανάγωγος παράγων του f. Σύμφωνα με το Θεώρημα A'.5 του Παραρτήματος A' υπάρχει επέκταση L/K και $\rho_1 \in L$ ώστε $L = K(\rho_1)$ και το ρ_1 είναι ρίζα του p. Τότε $f(X) = (X - \rho_1)g(X)$, $g \in L[X]$ και ο βαθμός του g είναι $= n - 1$. Λόγω της επαγωγικής υπόθεσης, υπάρχει επέκταση M του L και $\rho_2, \dots, \rho_n \in$ M έτσι ώστε $g(X) = c(X - \rho_2) \dots (X - \rho_n)$, $c \in L$ και $M = L(\rho_2, \dots, \rho_n)$. Τότε όμως, $f(X) = c(X - \rho_1)(X - \rho_2) \dots (X - \rho_n)$ (άρα το c είναι ο συντελεστής του μεγιστοβαθμίου όρου του $f(X)$ και, συνεπώς, είναι στοιχείο του σώματος K) και $M = K(\rho_1, \rho_2, \dots, \rho_n)$. □

Πριν προχωρήσετε στο επόμενο θεώρημα, είναι απαραίτητο να μελετήσετε τη σύντομη ενότητα B'.1 του Παραρτήματος B'.

Θεώρημα 1.4.3. *Έστω ένας ισομορφισμός σωμάτων $\sigma : K \to K'$ και $p(X) = a_0 + a_1X + \dots + a_nX^n \in K[X]$ μη σταθερό ανάγωγο πολυώνυμο. Έστω $p'(X) = \sigma(a_0) + \sigma(a_1)X + \dots + \sigma(a_n)X^n \in K'[X]$ (δηλαδή, με τον συμβολισμό της ενότητας B'.1 του Παραρτήματος B', $p' = \sigma p$). Αν u, v είναι ρίζες των p και p' (σε κάποιες κατάλληλες επεκτάσεις των K και K'),*

αντιστοίχως, τότε ο σ μπορεί να επεκταθεί σε ένα ισομορφισμό $\tilde{\sigma} : K(u) \to K'(v)$ ο οποίος, επιπλέον, ικανοποιεί την $\tilde{\sigma}(u) = v$.

Απόδειξη. Απλουστεύοντας τον συμβολισμό, για κάθε $u \in K$ γράφομε $\sigma(u) = u'$ και αντιστρόφως, τα στοιχεία του K' τα γράφομε με τη μορφή $u' = \sigma(u)$ για κάποιο (ακριβώς ένα) $u \in K$. Από το Θεώρημα B'.1 του Παραρτήματος B', ο σ επεκτείνεται σε ισομορφισμό δακτυλίων $\sigma : K[X] \to K'[X]$. Μεταξύ άλλων, αυτό συνεπάγεται ότι, για κάθε $f' \in K'[X]$ υπάρχει ένα μοναδικό $f \in K[X]$ ώστε $\sigma f = f'$.

Πρώτα παρατηρούμε ότι το p' είναι ανάγωγο. Πράγματι, έστω ότι δεν ήταν ανάγωγο και $p' = f'g'$ με τα $f', g' \in K'[X]$ μη σταθερά. Θεωρούμε τα $f, g \in K[X]$ για τα οποία ισχύει $\sigma f = f'$ και $\sigma g = g'$ (προφανώς τα f, g δεν είναι σταθερά), οπότε, η σχέση $p' = f'g'$ ισοδυναμεί με την $\sigma p = \sigma f \cdot \sigma g = \sigma(fg)$, άρα $p = fg$, άτοπο, αφού το p έχει υποτεθεί ανάγωγο.

Επίσης, επειδή ο πολλαπλασιασμός ενός πολυωνύμου επί μη μηδενική σταθερά δεν επηρεάζει τις ρίζες του, μπορούμε, χωρίς βλάβη της γενικότητος, να υποθέσομε μονικό το p (οπότε και το p' είναι μονικό). Τα πολυώνυμα p, p' έχουν τον ίδιο βαθμό, έστω n, οπότε (Θεώρημα 1.1.3) τα $1, u, \dots, u^{n-1}$ αποτελούν βάση της $K[u]/K$, καθώς και τα $1, v, \dots, v^{n-1}$ είναι βάση της $K'[v]/K'$.

Ορίζομε τώρα την εξής απεικόνιση $\tilde{\sigma} : K[u] \to K'[v]$.

$$K[u] \ni f(u) \xrightarrow{\tilde{\sigma}} f'(v) \in K'[X], \quad f' = \sigma f.$$

Στα επόμενα, όταν γράφομε $f, f', g, g', \dots$ εννοούμε ότι τα $f, g, \dots$ είναι πολυώνυμα του $K[X]$ και $f' = \sigma f, g' = \sigma g, \dots$. Πριν προχωρήσομε, κάνομε την εξής παρατήρηση: Αν $f, g \in K[X]$ και $f' = \sigma f, g' = \sigma g$, τότε το g διαιρεί το f αν και μόνο αν το g' διαιρεί το f'· διότι $g|f$ ισοδυναμεί με την ύπαρξη $h \in K[X]$ ώστε $f = gh$. Εφαρμόζοντας τον ισομορφισμό $\sigma : K[X] \to K'[X]$, βλέπομε ότι η τελευταία σχέση ισοδυναμεί με την $\sigma f = \sigma(gh) = \sigma g \cdot \sigma h$, δηλαδή, με την $f' = g'h'$ που σημαίνει $g'|f'$. Επίσης, υπενθυμίζομε την Πρόταση B'.5 (2) που λέει ότι, *αν δύο πολυώνυμα πάνω από ένα σώμα έχουν κοινή ρίζα σε κάποια επέκταση του σώματος και το ένα από τα δύο είναι ανάγωγο, τότε το ανάγωγο διαιρεί το άλλο πολυώνυμο.*

Τώρα ελέγχομε τα εξής:

- Η απεικόνιση $\tilde{\sigma}$ είναι καλά ορισμένη, δηλαδή, αν $f, g \in K[X]$ και $f(u) = g(u)$, τότε $f'(v) = g'(v)$. Συνοπτική απόδειξη:

$$f(u) = g(u) \Rightarrow (f-g)(u) = 0 \xrightarrow{\text{Πρόταση B'.5 (2)}} p \mid (f-g) \Rightarrow p' \mid (f'-g')$$
$$\Rightarrow (f'-g')(v) = 0 \Rightarrow f'(v) = g'(v)$$

- Η $\tilde{\sigma}$ είναι ομομορφισμός, δηλ. $\tilde{\sigma}(f(u) * g(u)) = \tilde{\sigma}(f(u)) * \tilde{\sigma}(g(u))$, όπου $*$ συμβολίζει την $+$ (πρόσθεση), είτε τον $\cdot$ (πολλαπλασιασμό). Συνοπτική απόδειξη:

$$\tilde{\sigma}(f(u) * g(u)) = \tilde{\sigma}((f*g)(u)) = (f*g)'(v) = (\sigma(f*g))(v)$$
$$= (\sigma f * \sigma g)(v) = (f' * g')(v) = f'(v) * g'(v) = \tilde{\sigma}(f(u)) * \tilde{\sigma}(g(u)).$$

- Η απεικόνιση $\tilde{\sigma}$ είναι 1-1 (ισοδύναμα, $\ker(f) = \{0\}$) και επί. Το «επί» είναι προφανές. Μένει να δείξομε ότι $\ker(f) = \{0\}$, δηλαδή, αν $\tilde{\sigma}(f(u)) = 0$, τότε $f(u) = 0$. Απόδειξη:

$$\tilde{\sigma}(f(u)) = 0 \Rightarrow f'(v) = 0 \xrightarrow{\text{Πρόταση B'.5 (2)}} p' \mid f' \Rightarrow p \mid f \Rightarrow f(u) = 0.$$

□

Το υπόλοιπο αυτής της ενότητας αφιερώνεται, ουσιαστικά, στην απόδειξη της μοναδικότητος του σώματος ανάλυσης ενός πολυωνύμου, η ύπαρξη του οποίου εξασφαλίζεται από το Θεώρημα 1.4.2.

Θεώρημα 1.4.4. *Έστω $\sigma : K \to K'$ ισομορφισμός σωμάτων. Αν τα $f \in K[X]$ και $f' \in K'[X]$ αντιστοιχούν μέσω του σ (βλ. Θεώρημα B'.1) και L/K, L'/K' είναι σώματα ανάλυσης των f και f', αντιστοίχως, τότε ο ισομορφισμός σ μπορεί να επεκταθεί σε ισομορφισμό $L \to L'$.*

Απόδειξη. Με επαγωγή στον βαθμό $[L : K]$, ο οποίος είναι πεπερασμένος λόγω του ορισμού του σώματος ανάλυσης και του Θεωρήματος 1.1.5. Έστω ότι $[L : K] = 1$, οπότε $L = K$. Εξ ορισμού του L, αυτό σημαίνει ότι υπάρχουν $c, u_1, \dots, u_m \in K$ ώστε $f(X) = c(X-u_1)\cdots(X-u_k)$. Έπεται ότι $f'(X) = c'(X-u'_1)\cdots(X-u'_m)$, όπου $c' = \sigma(c) \in K'$ και $u'_i = \sigma(u_i) \in K'$ για $i = 1, \dots, m$. Εξ ορισμού του L', υπάρχουν $k' \in K'$ και $\lambda'_1, \dots, \lambda'_m \in L'$ ώστε να ισχύει $f'(X) = k'(X-\lambda'_1)\cdots(X-\lambda'_m)$ και $L' = K'[\lambda'_1, \dots, \lambda'_m]$. Στον $L'[X]$ ισχύει η μονοσήμαντη ανάλυση σε ανάγωγα πολυώνυμα, άρα η σχέση $c'(X-u'_1)\cdots(X-u'_m) = k'(X-\lambda'_1)\cdots(X-\lambda'_m)$ συνεπάγεται ότι $k = c'$ και τα $\lambda'_1, \dots, \lambda'_m$ είναι μετάθεση των $u'_1, \dots, u'_m$. Συνεπώς, $L' = K'[\lambda'_1, \dots, \lambda'_m] = K'[u'_1, \dots, u'_m] = K'$, οπότε $\sigma : L \to L'$ είναι ο ισομορφισμός $\sigma : K \to K'$.

Έστω τώρα ακέραιος $n > 1$ κι ας υποθέσομε ότι το θεώρημα ισχύει για όλα τα πολυώνυμα, πάνω από οποιοδήποτε σώμα, τα οποία έχουν σώμα ανάλυσης πάνω από αυτό το σώμα, βαθμού $< n$. Στη συνέχεια, θεωρούμε πολυώνυμο $f \in K[X]$, με σώμα ανάλυσης L πάνω από το Kκαι $[L : K] = n$. Λόγω του ότι $n > 1$, υπάρχει ανάγωγος παράγων του f βαθμού > 1 και έστω p ένας οποιοσδήποτε τέτοιος παράγων. Μέσω του ισομορφισμού σ το p αντιστοιχεί σε ένα πολυώνυμο $p'(X) \in K'[X]$. Από τον ορισμό του L έπεται ότι υπάρχει $u \in L$ ώστε $p(u) = 0$ και, εντελώς ανάλογα, υπάρχει $v \in L'$, ώστε $p'(v) = 0$. Από το Θεώρημα 1.4.3 ξέρομε ότι ο σ επεκτείνεται σε έναν ισομορφισμό $\tilde{\sigma} : K[u] \to K'[v]$ [3]. Θέτομε $K_1 = K[u]$ και $K'_1 = K'[v]$ και από την άσκηση 3 ξέρομε ότι, αν δούμε τα f και f' ως πολυώνυμα των $K_1[X]$ και $K'_1[X]$, τα L, L' εξακολουθούν να είναι σώματα ανάλυσης τους, αντιστοίχως. Όμως τώρα, $[L : K_1] =$(Θεώρημα 1.1.4) $[L : K]/[K_1 : K] < [L : K] = n$, οπότε η επαγωγική υπόθεση συνεπάγεται ότι ο $\tilde{\sigma}$ επεκτείνεται σε ισομορφισμό $L \to L'$. Προφανώς, αυτός ο ισομορφισμός, ως επέκταση του $\tilde{\sigma}$, είναι και επέκταση του σ. □

Πόρισμα 1.4.1. *Έστω $f \in K[X]$ μη σταθερό, L σώμα ανάλυσης του f πάνω από το K και $\rho, \rho' \in L$ ρίζες του f. Τότε υπάρχει K-αυτομορφισμός του L που στέλνει τη ρ στη ρ'.*

Απόδειξη. Εφαρμόζοντας το Θεώρημα 1.4.3 με $\sigma = \mathrm{id}_K$ συμπεραίνομε ότι υπάρχει K-ισομορφισμός $\tilde{\sigma} : K(\rho) \to K(\rho')$ που στέλνει τη ρίζα ρ στη ρίζα ρ'. Το $K(\rho)$ είναι επέκταση

[3] Ο $\tilde{\sigma}$ στέλνει το u στο v, αλλά αυτό δεν μας ενδιαφέρει εδώ.

ενδιάμεση μεταξύ K και L, άρα, από την άσκηση 3, το L είναι σώμα ανάλυσης του f πάνω από το $K(\rho)$. Εντελώς ανάλογα, το L είναι σώμα ανάλυσης του f πάνω από το $K(\rho')$. Εφαρμόζοντας το Θεώρημα 1.4.4 με $f' = f$, $\sigma = \tilde{\sigma}$, $K(\rho)$ στη θέση του K, $K(\rho')$ στη θέση του K' και $L' = L$, συμπεραίνομε ότι ο $\tilde{\sigma}$ μπορεί να επεκταθεί σε αυτομορφισμό $\tau : L \to L$, ο οποίος έχει τις ζητούμενες ιδιότητες, καθώς $\tau(\rho) = \tilde{\sigma}(\rho) = \rho'$ και για κάθε $u \in K$ ισχύει $\tau(u) = \tilde{\sigma}(u) = \sigma(u) = u$. □

Θεώρημα 1.4.5. *Κάθε μη σταθερό πολυώνυμο με συντελεστές από ένα σώμα K έχει σώμα ανάλυσης πάνω από το K. Δύο σώματα ανάλυσης του ίδιου πολυωνύμου, πάνω από τόίδιο σώμα K, είναι K-ισόμορφα μεταξύ τους. Υπάρχει δηλαδή ένας ισομορφισμός από το ένα στο άλλο, ο οποίος αφήνει τα στοιχεία του K αναλλοίωτα.*

Απόδειξη. Εφαρμόζοντας το Θεώρημα 1.4.4 με $K' = K$ και σ τον ταυτοτικό αυτομορφισμό, συμπεραίνομε ότι υπάρχει ένας ισομορφισμός μεταξύ δύο οποιωνδήποτε σωμάτων ανάλυσης L και L' του $f \in K[X]$, ο οποίος αφήνει αναλλοίωτα όλα τα στοιχεία του K – είναι, όπως λέμε, *K-ισομορφισμός*. □

Λόγω του Θεωρήματος 1.4.5, όλα τα σώματα ανάλυσης ενός πολυωνύμου $f \in K[X]$ πάνω από το K είναι K-ισόμορφα, γι' αυτό και συνήθως λέμε π.χ. «έστω L το σώμα ανάλυσης του πολυωνύμου $f \in K[X]$» αντί να λέμε «έστω L (ένα ή κάποιο) σώμα ανάλυσης του πολυωνύμου $\in K[X]$».

Ασκήσεις

1. Αν το $f \in \mathbb{Q}[X]$ είναι ανάγωγο, $d \in \mathbb{Q}$ με $\sqrt{d} \notin \mathbb{Q}$ και $a + b\sqrt{d}, a, b \in \mathbb{Q}$ είναι ρίζα του f, δείξτε ότι και $a - b\sqrt{d}$ είναι ρίζα του f.

2. Στην άσκηση αυτή χρησιμοποιείστε ελεύθερα πραγματικούς και μιγαδικούς αριθμούς. Έστω $\sqrt[3]{2}$ η πραγματική κυβική ρίζα του 2 και $\omega = (-1 + i\sqrt{3})/2$. Παρατηρήστε ότι $\omega^2 + \omega + 1 = 0$, άρα $\omega^3 = 1$. Αποδείξτε ότι το $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ είναι σώμα ανάλυσης του $X^3 - 2$ πάνω από το $\mathbb{Q}$, ενώ, πάνω από το $\mathbb{R}$, το ίδιο πολυώνυμο έχει σώμα ανάλυσης το $M = \mathbb{R}(\omega)$.

3. Έστω $f \in K[X]$ και L σώμα ανάλυσης του f πάνω από το K. Έστω M ενδιάμεση επέκταση μεταξύ των K και L (δηλαδή, έχομε τις διαδοχικές επεκτάσεις $L/M/K$). Προφανώς, $f \in M[X]$. Αποδείξτε ότι το L είναι σώμα ανάλυσης του f πάνω από το M.

4. Αποδείξτε ότι το $f = X^2 - 2 \in \mathbb{Z}_5[X]$ είναι ανάγωγο. Από τη θεωρία είναι γνωστό ότι το f έχει σώμα ανάλυσης πάνω από το $\mathbb{Z}_5$· συμβολίστε το με L. Έστω $\theta \in L$ μία ρίζα του f. Αποδείξτε ότι $L = \mathbb{Z}_5(\theta)$ και καταγράψτε όλα τα στοιχεία του L (είναι 25 συνολικά). Εκτελέστε τις εξής πράξεις στο L:

$$(3 + 4\theta) + (2 + 2\theta), \quad (3 + 2\theta)(2 + \theta), \quad (2 + \theta)^3, \quad (1 + 2\theta)^{-1}.$$

Τα αποτελέσματα των πράξεων: $\theta,\ 2\theta,\ 4\theta,\ 2 + \theta$.

5. Έστω $f = X^3 - 3X + 1 \in \mathbb{Q}[X]$ και L το σώμα ανάλυσής-του πάνω από το $\mathbb{Q}$. Έστω $\rho \in L$ μία ρίζα του f. Βρείτε μια βάση της επέκτασης $\mathbb{Q}(\rho)/\mathbb{Q}$ και δείξτε ότι το στοιχείο $-2 + \rho^2$ είναι, επίσης, ρίζα του f· ποιά είναι η τρίτη ρίζα; (Θυμηθείτε τους τύπους του Viète για τις σχέσεις ανάλυσης και συντελεστών.) Συμπεράνατε ότι $L = \mathbb{Q}(\rho)$ και $[L : \mathbb{Q}] = 3$. Εκτελέστε τις εξής πράξεις:

$$(2 - 3\rho + 4\rho^2)(7 + 11\rho + 5\rho^2), \quad (-1 + 2\rho + 3\rho^2)^2, \quad (2 + \rho^2)^{-1}.$$

Τα αποτελέσματα των πράξεων: $-15 + 68\rho + 65\rho^2$, $-11 + 23\rho + 25\rho^2$, $\frac{1}{51}(25 - \rho - 5\rho^2)$.

6. Έστω το $f = X^3 + X + 1 \in \mathbb{Q}[X]$. Αποδείξτε ότι είναι ανάγωγο και έχει ακριβώς μία πραγματική ρίζα. Έστω ότι $\rho_1, \rho_2, \rho_3 \in \mathbb{C}$, $\rho_1 \in \mathbb{R}$ είναι οι ρίζες του f. Δείξτε ότι το $\mathbb{Q}(\rho_1, \rho_2)$ είναι σώμα ανάλυσης του f πάνω από το $\mathbb{Q}$ και $[\mathbb{Q}(\rho_1, \rho_2) : \mathbb{Q}] = 6$. Συμπεράνατε ότι αν L είναι ένα *οποιοδήποτε* σώμα ανάλυσης του f πάνω από το $\mathbb{Q}$, τότε $[L : \mathbb{Q}] = 6$. Βλέπετε την αντίθεση με το παράδειγμα της προηγούμενης άσκησης; Έστω τώρα ότι ρ και θ είναι δύο διαφορετικές ρίζες του f, που ανήκουν στο L. (Ξεχάστε τους μιγαδικούς τώρα!) Βρείτε ένα δευτεροβάθμιο πολυώνυμο του $\mathbb{Q}(\rho)[X]$, το οποίο να έχει ρίζα το θ. Βρείτε μία βάση της επέκτασης $L/\mathbb{Q}$ συναρτήσει των ρ, θ. Εκφράστε το στοιχείο $(-1 + 2\rho + \rho^2 - \theta)^2$ ως $\mathbb{Q}$-γραμμικό συνδυασμό των στοιχείων της βάσης που βρήκατε.
Απάντηση στα δύο τελευταία ερωτήματα: Η απλούστερης μορφής βάση της επέκτασης $L/\mathbb{Q}$ είναι $1, \rho, \rho^2, \theta, \theta\rho, \theta\rho^2$. Ισχύει $(-1 + 2\rho + \rho^2 - \theta)^2 = -4 - 9\rho + 2\theta - 5\theta\rho - 2\theta\rho^2$.

7. Έστω επέκταση L/K και E ενδιάμεση επέκταση ($K < E < L$). Έστω $u \in L$ αλγεβρικό πάνω από το K και $f = \mathrm{Irr}(u, K)$. Δείξτε ότι το u είναι αλγεβρικό πάνω από το E (τετριμμένο) και αν $g = \mathrm{Irr}(u, E)$, τότε, στον δακτύλιο $E[X]$ ισχύει $g \mid f$.
Υπόδειξη. Τα f, g είναι πολυώνυμα του $E[X]$ και έχουν το $u \in L$ κοινή ρίζα. Εφαρμόστε την Πρόταση B'.5 (2).

8. Σ' αυτή την άσκηση χρειαζόμαστε πρώτα τον παρακάτω ορισμό:

   Δύο στοιχεία μιας επέκτασης L του σώματος K, αλγεβρικά πάνω από το K, λέγονται συζυγή πάνω από το K *ή, απλώς,* K-συζυγή, *αν έχουν το ίδιο ελάχιστο πολυώνυμο πάνω από K.*

   Τώρα η άσκηση: Θεωρούμε τις διαδοχικές επεκτάσεις $L/M/K$. Έστω το $\lambda \in L$, αλγεβρικό πάνω από το K με ελάχιστο πολυώνυμο πάνω από το K το q. Τότε, το λ είναι αλγεβρικό και πάνω από το M (τετριμμένο), οπότε έστω p το ελάχιστο πολυώνυμο του λ πάνω από το M. Βλέποντας και το q ως πολυώνυμο του $M[X]$, αποδείξτε ότι το p διαιρεί το q. Δείξτε επίσης ότι, αν το $\mu \in M$ είναι αλγεβρικό συζυγές του λ πάνω από το M, τότε είναι αλγεβρικό συζυγές του λ και πάνω από το K.

9. Έστω ανάγωγο $p \in K[X]$, L σώμα ανάλυσης του p πάνω από το K και $u, v \in L$ οποιεσδήποτε ρίζες του p (με την ορολογία της άσκησης 8, τα u, v είναι K-συζυγή). Δείξτε

ότι υπάρχει ένας K-αυτομορφισμός του L, δηλαδή, ένας αυτομορφισμός του L, ο οποίος αφήνει αναλλοίωτο κάθε στοιχείο του K και στέλνει το u στο v.

10. Έστω K σώμα, ανάγωγο πολυώνυμο $f \in K[X]$ και M σώμα ανάλυσης του f πάνω από το K. Έστω και το πολυώνυμο $g \in K[X]$, το οποίο είναι ανάγωγο πάνω από το M και L σώμα ανάλυσης του g πάνω από το M. Τότε, για κάθε ζεύγος ριζών α, α' του f και κάθε ζεύγος ριζών β, β' του g υπάρχει $\sigma \in \mathcal{G}(L/K)$ με την ιδιότητα $\sigma(\alpha) = \alpha'$ και $\sigma(\beta) = \beta'$.
Υπόδειξη. Το Θεώρημα 1.4.3 μας εξασφαλίζει ότι ο ταυτοτικός ισομορφισμός $K \to K$ επεκτείνεται σε ισομορφισμό $\sigma_1 : K(\alpha) \to K(\alpha')$, με την ιδιότητα $\sigma_1(\alpha) = \alpha'$. Μέσω του σ_1 το f απεικονίζεται στον εαυτό του. Επίσης, το M είναι σώμα ανάλυσης του f πάνω από το $K(\alpha)$, καθώς και πάνω από το $K(\alpha')$ (άσκηση 3). Άρα το Θεώρημα 1.4.4 μας εξασφαλίζει ότι ο σ_1 επεκτείνεται σε αυτομορφισμό $\sigma_2 : M \to M$. Μέσω του σ_2 το g απεικονίζεται στον εαυτό του άρα, από το Θεώρημα 1.4.3, ο σ_2 επεκτείνεται σε ισομορφισμό $\sigma_3 : M(\beta) \to M(\beta')$, με την ιδιότητα $\sigma_3(\beta) = \beta'$. Μέσω του σ_3 το g απεικονίζεται στον εαυτό του, και το L είναι σώμα ανάλυσης του g πάνω από το $M(\beta)$, καθώς και πάνω από το $M(\beta')$ (ξανά η άσκηση 3). Άρα, από το Θεώρημα 1.4.4, ο σ_3 επεκτείνεται σε ισομορφισμό $\sigma : L \to L$, που "κληρονομεί" τις ιδιότητες των $\sigma_3, \sigma_2, \sigma_1$, άρα αφήνει αναλλοίωτο κάθε στοιχείο του K και στέλνει το α στο α' και το β στο β'.

1.5 Σωμα αναλυσης κυβικου πολυωνυμου

Σ' αυτή την ενότητα θα υποθέσομε ότι το σώμα K έχει χαρακτηριστική $\neq 2, 3$, θα θεωρήσομε ένα ανάγωγο $g(X) = X^3 + pX^2 + qX + r \in K[X]$ και θα μελετήσομε το σώμα ανάλυσης του $g(X)$. Στην περίπτωση που $p \neq 0$, θα υποθέσομε ότι η χαρακτηριστική του K είναι $\neq 3$. Αυτό μας επιτρέπει να θεωρήσομε το πολυώνυμο $g(X - p/3)$,[4] οπότε μελετούμε το απλούστερης μορφής πολυώνυμο

$$f(X) = g(X - p/3) = X^3 + aX + b, \qquad a = -3p^2 + q,\ b = 2p^3 - qp + r.$$

Παρατηρήστε ότι ένα στοιχείο ρ (σε κάποια επέκταση του K) είναι ρίζα του f αν και μόνο αν το $\rho - p/3$ είναι ρίζα του g, άρα, πάνω απ' το K, ένα σώμα ανάλυσης του f είναι και σώμα ανάλυσης του g. Παρατηρήστε, επίσης, ότι, αφού το f έχει υποτεθεί ανάγωγο πάνω από το K, το ίδιο ισχύει και για το f. θα εστιάσομε, λοιπόν, τη μελέτη μας στο παραπάνω f.

Ας δούμε πρώτα την περίπτωση που $a = 0$ *και* η χαρακτηριστική του K είναι 3. Τότε, αν L είναι σώμα ανάλυσης του f και $\rho \in L$ είναι μία ρίζα του f, παρατηρούμε ότι $0 = f(\rho) = \rho^3 + b$ άρα $b = -\rho^3$ και $f(X) = X^3 + b = X^3 - \rho^3 = (X - \rho)^3$.[5] Άρα, σ' αυτή την περίπτωση το f έχει μία μόνο ρίζα, έστω ρ, και το σώμα ανάλυσης του f πάνω απ' το K είναι $L = K[\rho]$. Αυτή η περίπτωση, λοιπόν, δεν έχει κάποια δυσκολία ή ουσιαστικό ενδιαφέρον.

> Στο εξής, θα υποθέτομε ότι, η χαρακτηριστική του K είναι $\neq 2$ και, στην περίπτωση που $a = 0$, θα κάνομε και την *επιπλέον* υπόθεση ότι η χαρακτηριστική του K είναι $\neq 3$.

Έστω $L = K(\rho, \rho', \rho'')$ σώμα ανάλυσης του f. Τότε $f(X) = (X - \rho)(X - \rho')(X - \rho'')$. Ας αποδείξομε πρώτα ότι $3\rho^2 + a \neq 0$, κάτι που θα μας χρειαστεί παρακάτω. Πράγματι, αν ήταν $3\rho^2 + a = 0$, αυτό θα σήμαινε ότι το ρ είναι ρίζα του $3X^2 + a$, οπότε, απ' την Πρόταση B'.5 (2), $f(X)|(3X^2 + a)$. Αλλά το f είναι βαθμού 3, άρα η τελευταία σχέση είναι δυνατή μόνο αν το $3X^2 + a$ είναι το μηδενικό πολυώνυμο. Αυτό μπορεί να συμβεί μόνον όταν η χαρακτηριστική του K είναι 3 και το $a = 0$, περίπτωση που ήδη αποκλείσαμε.

Συνεχίζομε δείχνοντας ότι οι ρίζες ρ, ρ', ρ'' είναι διαφορετικές. Πράγματι, έστω ότι $\rho = \rho'$. Τότε, λόγω των τύπων του Viète , $\rho'' = -\rho - \rho' = -2\rho$, άρα $X^3 + aX + b = (X - \rho)(X - \rho')(X - \rho'') = (X - \rho)^2(X + 2\rho)$, απ' όπου παίρνομε $a = -3\rho^2$, άρα $3\rho^2 + a = 0$, σχέση που αποκλείσαμε λίγο παραπάνω.

Θεωρούμε τώρα την ποσότητα

$$\delta = (\rho - \rho')(\rho - \rho'')(\rho' - \rho'') \neq 0, \tag{1.1}$$

καθώς και τις σχέσεις $f(\rho) = 0$ και $f(\rho') = 0$. Αφαιρώντας-τις κατά μέλη και διαιρώντας μετά

[4] Όταν γράφομε, στην Άλγεβρα, $p/3$, όπου p είναι στοιχείο ενός σώματος K, εννοούμε $p \cdot (3 \cdot 1_K)^{-1}$, όπου 1_K είναι το μοναδιαίο στοιχείο του K. Αυτό το στοιχείο έχει νόημα, εφ' όσον το $3 \cdot 1_K$ είναι μη μηδενικό, κάτι που ισχύει όταν η χαρακτηριστική του K δεν είναι 3.

[5] Στην τελευταία ισότητα παίζει ρόλο το ότι η χαρακτηριστική του K είναι 3.

διά $\rho - \rho' \neq 0$, παίρνομε τη σχέση

$$\rho^2 + \rho\rho' + \rho'^2 = -a \ . \tag{1.2}$$

Από την τελευταία και την $-\rho'' = \rho + \rho'$ έχομε:

$$\begin{aligned}
\delta &= (\rho - \rho')(2\rho + \rho')(\rho + 2\rho') \\
&= (\rho - \rho')(2\rho^2 + 5\rho\rho' + 2\rho'^2) = (\rho - \rho')[3\rho\rho' + 2(\rho^2 + \rho\rho' + \rho'^2)] \\
&\overset{(1.2)}{=} (\rho - \rho')(3\rho\rho' - 2a) = -3\rho\rho'^2 + (3\rho^2 + 2a)\rho' - 2a\rho \\
&= 3\rho(-\rho'^2) + (3\rho^2 + 2a)\rho' - 2a\rho \\
&\overset{(1.2)}{=} 3\rho(\rho^2 + \rho\rho' + a) + (3\rho^2 + 2a)\rho' - 2a\rho \\
&= (6\rho^2 + 2a)\rho' + (3\rho^3 + a\rho) = (6\rho^2 + 2a)\rho' + 3(-a\rho - b) + a\rho \\
&= -2a\rho - 3b + (6\rho^2 + 2a)\rho'.
\end{aligned}$$

Ο συντελεστής $2(3\rho^2 + a)$ του ρ' στην τελευταία ισότητα είναι $\neq 0$, επειδή έχομε υποθέσει ότι η χαρακτηριστική του K είναι $\neq 2$ και, επίσης, έχομε αποδείξει ότι $3\rho^2 + a \neq 0$. Συνεπώς,

$$\rho' = \frac{\delta + 2a\rho + 3b}{2a + 6\rho^2} \ ,$$

απ' όπου γίνεται φανερό ότι $\rho', \rho'' \in K(\rho, \delta)$ και, συνεπώς, το σώμα ανάλυσης του f πάνω απ' το K είναι το $K(\rho, \delta)$. Ποιά είναι όμως η χρησιμότητα αυτού του συμπεράσματος; Γιατί να μήν πούμε απλώς ότι το σώμα ανάλυσης είναι το $K(\rho, \rho', \rho'') = K(\rho, \rho')$; Το παραπάνω συμπέρασμά μας δεν θα είχε καμμία σημασία αν, όπως θα δούμε αμέσως παρακάτω, το δ δεν είχε την ωραία ιδιότητα να είναι τεραγωνική ρίζα ενός στοιχείου του K.

Θεώρημα 1.5.1. *Έστω K σώμα χαρακτηριστικής διάφορης του 2 και το ανάγωγο $f(X) = X^3 + aX + b \in K[X]$. Στην περίπτωση που $a = 0$ υποθέτομε ότι η χαρακτηριστική του σώματος K δεν είναι ούτε 3. Συμβολίζομε με L το σώμα ανάλυσης του f πάνω από το K και με $\rho, \rho', \rho'' \in L$ τις ρίζες του f και θέτομε*

$$\delta = (\rho - \rho')(\rho - \rho'')(\rho' - \rho'') \ .$$

Τότε, οι ρίζες ρ, ρ', ρ'' είναι διαφορετικές, $L = K(\rho, \delta)$ και

$$\begin{aligned}
\rho' &= \frac{\delta + 2a\rho + 3b}{2a + 6\rho^2} = \frac{-4a^2 + (9b - \delta)\rho - 6a\rho^2}{2\delta} \\
\rho'' &= \frac{-\delta + 2a\rho + 3b}{2a + 6\rho^2} = \frac{4a^2 - (9b + \delta)\rho + 6a\rho^2}{2\delta} \\
\delta^2 &= -4a^3 - 27b^2 \neq 0 \ .
\end{aligned}$$

Το στοιχείο $\delta^2 = D \in K$ καλείται διακρίνουσα του f.

Απόδειξη. Έχομε ήδη αποδείξει ότι οι ρίζες ρ, ρ', ρ'' είναι διαφορετικές, καθώς και την

έκφραση για το ρ'. Από την έκφραση αυτή του ρ' προκύπτει αμέσως η αντίστοιχη έκφραση του ρ'', αρκεί να εναλλάξομε τα ρ' και ρ'' και να παρατηρήσομε ότι η εναλλαγή αυτή μετατρέπει το δ στο $-\delta$.

Από τις εκφράσεις αυτές των ρ' και ρ'' έχομε (λόγω και της $\rho\rho'\rho'' = -b$),

$$\frac{(2a\rho + 3b)^2 - \delta^2}{(2a + 6\rho^2)^2} = \rho'\rho'' = -\frac{b}{\rho} = \rho^2 + a.$$

Λύνοντας ως πρός δ^2, παίρνομε ύστερα από απλές πράξεις (λαμβάνοντας υπόψη τη σχέση $\rho^3 = -a\rho - b$) την τρίτη από τις αποδεικτέες σχέσεις. Η σχέση $\delta^2 \neq 0$, φυσικά, προκύπτει από το ότι οι ρίζες ρ, ρ', ρ'' είναι διαφορετικές. Για ένα διαφορετικό τρόπο απόδειξης του τύπου $\delta^2 = -4a^3 - 27b^2$ δείτε την άσκηση 5. □

Ασκήσεις

1. Αποδείξτε ότι (με τους συμβολισμούς αυτής της ενότητας) το σώμα ανάλυσης του f όταν το $-4a^3 - 27b^2$ δεν είναι τέλειο τετράγωνο του K, είναι έκτου βαθμού πάνω απ' το K; διαφορετικά, είναι τρίτου βαθμού.
   Υπόδειξη. Έστω $D = -4a^3 - 27b^2$. Δείξτε ότι το $X^3 - D$ είναι ανάγωγο, όχι μόνο πάνω απ' το K, αλλά και πάνω απ' το $K[\rho]$.

2. Έστω το $f(X) = X^3 + aX + b \in K[X]$. Δέν κάνομε καμμία υπόθεση για το αν το f είναι ή όχι ανάγωγο, ούτε θέτομε κανένα περιορισμό στη χαρακτηριστική του K. Παρατηρήστε ότι, και πάλι, οι σχέσεις του Θεωρήματος 1.5.1 ισχύουν. Η ποσότητα $\Delta = -4a^3 - 27b^2$ λέγεται *διακρίνουσα* του f. Αποδείξτε τα εξής: (α) Το f έχει πολλαπλή ρίζα αν και μόνο αν $\Delta = 0$. (β) Αν το K είναι υπόσωμα του $\mathbb{R}$ και $\Delta > 0$, τότε οι τρείς ρίζες του f είναι πραγματικές, ενώ αν $\Delta < 0$, μία ακριβώς ρίζα είναι πραγματική.

3. Αν ρ είναι μία ρίζα του $f(X) = X^3 - 3X + 1 \in \mathbb{Q}[X]$, υπολογίστε, με βάση τα εκτεθέντα στην προηγηθείσα ενότητα, τις δύο άλλες ρίζες του f ως πολυωνυμικές εκφράσεις του ρ (πρβλ. άσκηση 5 της ενότητας 1.4). Όμοιο ζήτημα για το $X^3 - 7X + 7$.

4. Αν ρ είναι μία ρίζα του $X^3 - 6X + 2 \in \mathbb{Q}[X]$, εκφράστε τις άλλες δύο ρίζες ως πολυωνυμικές εκφράσεις του ρ και μιας τετραγωνικής ρίζας ρητού αριθμού. Αν ξέρετε ότι μία προσεγγιστική τιμή για το ρ είναι -2.60167913, υπολογίστε προσεγγιστικές τιμές για τις άλλες δύο ρίζες. Όμοιο ζήτημα για το $X^3 + 3X + 5$, του οποίου μία ρίζα έχει την προσεγγιστική τιμή -1.15417149.

5. *Υπολογισμός της διακρίνουσας κυβικού πολυωνύμου.* Έστω $f(X) = X^3 + aX + b \in K[X]$ (K σώμα) και $f(X) = (X-\rho)(X-\rho')(X-\rho'')$, σε κάποια επέκταση του K (παρατηρήστε ότι δεν γίνεται καμμιά υπόθεση για το αν οι ρίζες ρ, ρ', ρ'', είναι διαφορετικές). Αποδείξτε ότι
   $$D = (\rho - \rho')^2(\rho - \rho'')^2(\rho' - \rho'')^2 = -4a^3 - 27b^2.$$

Υπόδειξη. Χρησιμοποιήστε τους τύπους του Viète $\rho+\rho'+\rho''=0$ και $\rho\rho'\rho''=-b$. Παρατηρήστε ότι $(\rho-\rho')^2=(\rho+\rho')^2-4\rho\rho'=\rho''^2+4b/\rho''=(\rho''^3+4b)/\rho''=(-a\rho''+3b)/\rho''$. Κάνετε το ανάλογο και για τους υπόλοιπους δύο παράγοντες του D, οπότε $D=(3b-a\rho'')(3b-a\rho')(3b-a\rho)/(\rho''\rho'\rho)$. Αν $a=0$, βλέπομε αμέσως ότι $D=-27b^2$. Αν $a\neq 0$, τότε παρατηρήστε ότι $(3b-a\rho'')(3b-a\rho')(3b-a\rho)=a^3(3b/a-\rho'')(3b/a-\rho')(3b/a-\rho)=f(3b/a)$ κλπ.

1.6 Το Θεμελιωδες Θεωρημα της Αλγεβρας

Τό γεγονός ότι, δοθέντος ενός οποιουδήποτε μή σταθερού πολυωνύμου μέ συντελεστές από ένα τυχόν σώμα K, υπάρχει ένα σώμα "πλουσιώτερο" (εν γένει) από τό K, εντός τού οποίου μπορούμε νά μιλούμε γιά τίς ρίζες τού θεωρουμένου πολυωνύμου (βλ. Θεώρημα 1.4.5), παίζει βασικό – άν καί μάλλον αφανή – ρόλο, στήν απόδειξη τού Θεμελιώδους Θεωρήματος τής Άλγεβρας:

Κάθε μή σταθερό πολυώνυμο μέ μιγαδικούς συντελεστές έχει μιγαδική ρίζα.

Ορισμένες προκαταρκτικές γνώσεις (πολύ χρήσιμες καί σέ αρκετές άλλες περιπτώσεις) είναι απαραίτητες πρώτα. Έστω δακτύλιος R. Τό πολυώνυμο (πολλών μεταβλητών) $f(X_1,\dots,X_n)\in R[X_1,\dots,X_n]$ λέγεται *συμμετρικό*, άν κάθε μετάθεση τών $X_1,\dots,X_n$ τό αφήνει αναλλοίωτο. Τά λεγόμενα *στοιχειώδη συμμετρικά πολυώνυμα τών* $X_1,\dots,X_n$ είναι τά πολυώνυμα

$$S_1=\sum_{i=1}^{n}X_i\ ,\ \ S_2=\sum_{1\le i<j\le n}X_iX_j\ ,$$

$$S_3=\sum_{1\le i<j<k\le n}X_iX_jX_k\ ,\ \dots,\ S_n=X_1X_2\cdots X_n\ .$$

Έστω τώρα ότι τά $u_1,\dots,u_n$ είναι στοιχεία κάποιου δακτυλίου, τού οποίου ο R είναι υποδακτύλιος (π.χ. τά u_i θά μπορούσε νά ήταν οι μεταβλητές $X_1,\dots,X_n$). Λέγοντας ότι τό στοιχείο u τού δακτυλίου $R[u_1,\dots,u_n]$ είναι συμμετρική παράσταση τών $u_1,\dots,u_n$, εννοούμε ότι, όταν εκφράσομε τό u ως $f(u_1,\dots,u_n)$, γιά κάποιο κατάλληλο πολυώνυμο $f(X_1,\dots,X_n)\in R[X_1,\dots,X_n]$, τό πολυώνυμο αυτό είναι συμμετρικό. Επίσης, λέγοντας στοιχειώδεις συμμετρικές παραστάσεις τών $u_1,\dots,u_n$, εννοούμε τά στοιχεία $S_1(u_1,\dots,u_n),S_2(u_1,\dots,u_n),\dots,S_n(u_1,\dots,u_n)$. Ένα πολύ σημαντικό θεώρημα, τού οποίου μία κάπως ακριβέστερη μορφή αποδεικνύεται στό Παράρτημα Δ' (βλ. Θεώρημα Δ'.1), είναι τό εξής:

Θεώρημα 1.6.1. *(Θεμελιώδες Θεώρημα τών συμμετρικών πολυωνύμων). Άν τό* $u\in R[u_1,\dots,u_n]$ *είναι συμμετρική παράσταση τών* $u_1,\dots,u_n$*, τότε* $u\in R[v_1,\dots,v_n]$*, όπου* $v_1,\dots,v_n$ *είναι οι στοιχειώδεις συμμετρικές παραστάσεις τών* $u_1,\dots,u_n$*.*

Συχνά, τό θεώρημα αυτό διατυπώνεται καί ως εξής: *Άν τό* $f\in R[X_1,\dots,X_n]$ *είναι συμμετρικό, τότε μπορεί νά εκφραστεί καί ως πολυώνυμο τών* $S_1,\dots,S_n$ *μέ συντελεστές από τό* R*.*

Παράδειγμα στίς δύο μεταβλητές: $f=X_1^2+X_2^2$, προφανώς συμμετρικό. Εδώ $S_1=X_1+X_2, S_2=X_1X_2$ καί $f=S_1^2-2S_2$.

Παράδειγμα στίς τρείς μεταβλητές: $f=X_1^3+X_2^3+X_3^3$. Είναι $S_1=X_1+X_2+X_3, S_2=X_1X_2+X_1X_3+X_2X_3, S_3=X_1X_2X_3$ καί εύκολα βρίσκεται από τήν ανάπτυξη τού $(X_1+X_2+X_3)^3$ ότι $f=S_1^3-3S_1S_2-3S_3$.

Η διαδικασία γιά νά εκφράσει κανείς ένα συμμετρικό πολυώνυμο ως πολυώνυμο τών στοιχειωδών συμμετρικών παραστάσεων τών μεταβλητών του, άν καί αλγοριθμική, είναι, μερικές φορές, κοπιαστική. Άς έλθομε τώρα στό βασικό θέμα αυτής τής ενότητας.

Θεώρημα 1.6.2. *(Θεμελιώδες Θεώρημα τής Άλγεβρας). Κάθε μή σταθερό πολυώνυμο τού* $\mathbb{C}[X]$ *έχει μία, τουλάχιστον, μιγαδική ρίζα.*

Απόδειξη. Έστω μή σταθερό $f(X) \in \mathbb{C}[X]$. Μέ $\overline{f}(X)$ συμβολίζομε τό πολυώνυμο πού προκύπτει άν τούς συντελεστές τού $f(X)$ αντικαταστήσομε από τούς μιγαδικούς συζυγείς τους. Αρκεί νά δείξομε ότι τό $g(X) = f(X)\overline{f}(X)$ έχει ρίζα στό $\mathbb{C}$. Γιατί, άν $g(z) = 0$, τότε ή $f(z) = 0$, οπότε έχομε τελειώσει, ή $\overline{f}(z) = 0$, οπότε, παίρνοντας μιγαδικούς συζυγείς, $f(\overline{z}) = 0$. Μιά δεύτερη παρατήρηση είναι ότι $g(X) \in \mathbb{R}[X]$, όπως φαίνεται ύστερα από απλές πράξεις (άσκηση 1).

Μέ τούς παραπάνω συλλογισμούς βλέπομε, λοιπόν, ότι αρκεί ν" αποδείξομε τήν ύπαρξη μιγαδικής ρίζας γιά κάθε μή σταθερό πολυώνυμο μέ *πραγματικούς συντελεστές*. Έστω μή σταθερό $g(X) \in \mathbb{R}[X]$. Ο βαθμός τού $g(X)$ μπορεί νά γραφεί $\deg g = 2^n m$, όπου m περιττός καί $n \geq 0$. Η απόδειξη θά γίνει επαγωγικά επί τού n. Άν $n = 0$ τό $g(X)$ είναι περιττού βαθμού καί ο στοιχειώδης Απειροστικός Λογισμός μάς λέει ότι τό πολυώνυμό μας έχει ρίζα καί, μάλιστα, πραγματική [6]. Έστω τώρα ότι ο l είναι ακέραιος ≥ 1 καί ο ισχυρισμός μας αληθεύει γιά κάθε πολυώνυμο μέ πραγματικούς συντελεστές, τού οποίου ο βαθμός είναι τής μορφής $2^{l-1} \cdot$ περιττός. Θεωρούμε τώρα $g(X) \in \mathbb{R}[X], \deg g = d = 2^l \cdot$ περιττός καί έστω L τό σώμα ριζών τού $g(X)$ πάνω από τό $\mathbb{C}$. Χωρίς βλάβη τής γενικότητος, άς υποθέσομε τό $g(X)$ μονικό, οπότε $g(X) = (X - u_1) \dots (X - u_d)$, όπου $u_1, \dots, u_d \in L$ οι ρίζες τού $g(X)$ (όχι, κατ" ανάγκη, διαφορετικές). Γιά κάθε πραγματικό αριθμό a σχηματίζομε τά εξής στοιχεία τού L:

$$v_{ij} = u_i + u_j + a u_i u_j \ , \ 1 \leq i, j \leq d \ ,$$

καθώς καί τό πολυώνυμο $h(X) \in \mathbb{L}[X]$, πού τά έχει ως ρίζες,

$$h(X) = \prod_{1 \leq i \leq j \leq d} (X - v_{ij}) \ .$$

Εύκολα διαπιστώνεται ότι $\deg h = d(d+1)/2 = 2^{l-1} \cdot$ περιττός. Θά δείξομε ακόμη ότι τό $h(X)$ έχει πραγματικούς συντελεστές. Πράγματι, κάθε μετάθεση τών $u_1, \dots u_d$ προκαλεί, απλώς, μία μετάθεση στίς ρίζες τού $h(X)$ (βλ. άσκηση 2), άρα αφήνει αναλλοίωτο τό $h(X)$, δηλαδή, τούς συντελεστές του. Όμως, οι συντελεστές τού $h(X)$ είναι, κατά προσέγγιση προσήμου, οι στοιχειώδεις συμμετρικές παραστάσεις τών v_{ij} (τύποι τού Viète , άρα είναι πολυωνυμικές εκφράσεις τών $u_1, \dots, u_d$ καί, μόλις τώρα, είδαμε ότι μένουν αναλλοίωτες από τίς μεταθέσεις τών $u_1, \dots, u_d$. Συνεπώς (Θεώρημα 1.6.1), οι συντελεστές τού $h(X)$ είναι πολυωνυμικές εκφράσεις μέ πραγματικούς συντελεστές τών στοιχειωδών συμμετρικών παραστάσεων τών $u_1, \dots, u_n$. Αυτές οι τελευταίες, όμως, είναι, κατά προσέγγιση προσήμου, ίσες μέ τούς συντελεστές τού $g(X)$ (πάλι οι τύποι τού Viète), άρα είναι πραγματικοί αριθμοί; έπεται ότι καί οι συντελεστές τού $h(X)$ είναι πραγματικοί. Εφαρμόζομε τώρα τήν επαγωγική υπόθεση στό $h(X)$ καί συμπεραίνομε ότι μία από τίς ρίζες του ανήκει στό $\mathbb{C}$; άς τή συμβολίσομε μέ z_a (προφανώς, εξαρτάται από τό a).

Μέχρι στιγμής συμπεράναμε λοιπόν ότι, γιά κάθε $a \in \mathbb{R}$, υπάρχουν δείκτες i_a, j_a μέ $1 \leq$

[6] Εδώ είναι τό μόνο σημείο τής αποδείξεως, στό οποίο χρησιμοποιούμε κάτι από τήν Ανάλυση.

$i_a \leq j_a \leq d$, τέτοιοι ώστε τό στοιχείο $z_a = v_{i_a j_a} = u_{i_a} + u_{j_a} + a u_{i_a} u_{j_a}$ τού L νά ανήκει, επίσης καί στό $\mathbb{C}$. Καθώς τό a μπορεί νά πάρει άπειρες τιμές, ενώ οι δείκτες i_a, j_a μόνο πεπερασμένες, συμπεραίνομε (αρχή τού περιστερώνα) ότι σέ δύο διαφορετικά a, a' αντιστοιχούν οι ἴδιοι δείκτες i, j, δηλαδή

$$u_i + u_j + a u_i u_j \in \mathbb{C}\,,\ u_i + u_j + a' u_i u_j \in \mathbb{C}\,,\ a \neq a'\,.$$

Από εδώ έπεται αμέσως ότι $u_i + u_j \in \mathbb{C}$ καί $u_i u_j \in \mathbb{C}$. Αλλά τότε (άσκηση 4), οι ρίζες u_i, u_j τού $g(X)$ ανήκουν στό $\mathbb{C}$. □

Ασκήσεις

1. Έστω μή σταθερό $f(X) \in \mathbb{C}[X]$ καί $\overline{f}(X)$ τό πολυώνυμο πού προκύπτει άν τούς συντελεστές τού $f(X)$ αντικαταστήσομε από τούς μιγαδικούς συζυγείς τους. Αποδείξτε ότι $f(X)\overline{f}(X) \in \mathbb{R}[X]$.

2. Θεωρήστε τά στοιχεία v_{ij}, όπως ορίσθηκαν στήν απόδειξη τού Θεωρήματος 1.6.2 καί τό σύνολο V εκείνων τών v_{ij}, γιά τά οποία $i \leq j$. Δείξτε ότι κάθε αντιμετάθεση $u_i \leftrightarrow u_j$ προκαλεί μία μετάθεση τών στοιχείων τού V. Συμπεράνατε ότι κάθε μετάθεση τών $u_1, \ldots, u_d$ προκαλεί μετάθεση τών στοιχείων τού V.

3. Εστω ότι τό $g(X)$, πού εμφανίζεται στήν απόδειξη τού Θεωρήματος 1.6.2 είναι τό $X^2 + pX + q$ καί $a = 1$ στόν ορισμό τών v_{ij}. Σύμφωνα μέ τήν απόδειξη (ξανακοιτάξτε την στό σημείο πού μιλάμε γιά τούς συντελεστές τού $h(X)$), τό αντίστοιχο $h(X)$ είναι τρίτου βαθμού καί οι συντελεστές του είναι πολυωνυμικές εκφράσεις τών p, q. Υπολογίστε τους.

4. Έστω L επέκταση τού $\mathbb{C}$ καί καί $\lambda_1, \lambda_2 \in L$, τέτοια ώστε $\lambda_1 + \lambda_2$ καί $\lambda_1 \lambda_2$ είναι στοιχεία τού $\mathbb{C}$. Δείξτε ότι τότε καί $\lambda_1, \lambda_2 \in \mathbb{C}$.

5. Δείξτε ότι κάθε μή σταθερό πολυώνυμο μέ μιγαδικούς συντελεστές έχει *όλες* τίς ρίζες του στό $\mathbb{C}$. Συμπεράνατε ότι τό $\mathbb{C}$ είναι *αλγεβρικά κλειστό*. Ο γενικός ορισμός τού αλγεβρικά κλειστού σώματος είναι ο εξής: *Τό σώμα K χαρακτηρίζεται αλγεβρικά κλειστό, άν δέν υπάρχει γνήσια αλγεβρική επέκταση τού K.*

Κεφάλαιο 2

Θεωρία Galois

2.1 Βασικες εννοιες και Προτασεις

Ορισμός 2.1.1. *Έστω L/K επέκταση σωμάτων. Ο αυτομορφισμός σ του L λέγεται K-αυτομορφισμός του L αν $\sigma(u) = u$ για κάθε $u \in K$.*

Τη σύνθεση $L \xrightarrow{\sigma_2} L \xrightarrow{\sigma_1} L$ των αυτομορφισμών σ_1, σ_2 του L συμβολίζομε με $\sigma_1\sigma_2$.

Θεώρημα - Ορισμός 2.1.2. *Αν L/K είναι επέκταση σωμάτων, τότε το σύνολο των K-αυτομορφισμών του L είναι υποομάδα της ομάδας όλων των αυτομορφισμών του L με πράξη τη σύνθεση αυτομορφισμών. Η υποομάδα αυτή συμβολίζεται με $\mathcal{G}(L/K)$ και λέγεται ομάδα Galois της L/K. Αν η L/K είναι πεπερασμένη επέκταση, τότε και η ομάδα $\mathcal{G}(L/K)$ είναι πεπερασμένη.*

Στην περίπτωση που το L είναι σώμα ανάλυσης κάποιου πολυωνύμου $f \in K[X]$, η ομάδα $\mathcal{G}(L/K)$ λέγεται ομάδα Galois του πολυωνύμου f πάνω από το K. Αν $\deg f = n$ και οι ρίζες του f είναι διαφορετικές, τότε η $\mathcal{G}(L/K)$ ταυτίζεται με μία υποομάδα της συμμετρικής ομάδας $\mathbf{S}_n$.

Απόδειξη. Είναι γνωστό από τη βασική Άλγεβρα ότι το σύνολο των αυτομορφισμών ενός σώματος, με πράξη τη σύνθεση απεικονίσεων, αποτελεί ομάδα. Συνεπώς, αρκεί να δείξομε ότι το $\mathcal{G}(L/K)$ είναι μη κενό, κλειστό ως πρός την πράξη της ομάδος και αν $\sigma \in \mathcal{G}(L/K)$, τότε $\sigma^{-1} \in \mathcal{G}(L/K)$. Πράγματι, είναι μη κενό, διότι ο ταυτοτικός αυτομορφισμός του L είναι, προφανώς, K-αυτομορφισμός, ενώ η κλειστότητα της σύνθεσης είναι εξ ίσου προφανής (αν οι σ_1, σ_2 αφήνουν αναλλοίωτα τα στοιχεία του K, το ίδιο θα συμβαίνει και με τη σύνθεσή τους). Έστω τώρα K-αυτομορφισμός σ και $u \in K$, τυχόν. Πρέπει να δείξομε ότι $\sigma^{-1}(u) = u$. Έστω $\sigma^{-1}(u) = v$, οπότε $\sigma(v) = u$. Όμως, και $\sigma(u) = u$, αφού ο σ είναι K-αυτομορφισμός. Έτσι, $\sigma(v) = \sigma(u)$, οπότε $v = u$.

Πρίν προχωρήσομε στην περίπτωση πεπερασμένης L/K, κάνομε την εξής παρατήρηση, η οποία θα χρησιμοποιείται στο εξής πάρα πολλές φορές: Έστω ότι το $u \in L$ είναι ρίζα κάποιου $g \in K[X]$ και σ είναι ένας K-αυτομορφισμός του L. Τότε το $\sigma(u)$ είναι, επίσης, ρίζα του g. Διότι, αν $g(X) = a_dX^d + \cdots + a_1X + a_0$ και εφαρμόσομε τον σ στά δύο μέλη της σχέσεως

$0 = a_d u^d + \cdots + a_1 u + a_0$ τότε, λόγω του ότι ο σ αφήνει αναλλοίωτα όλα τα a_i, καθώς και το 0, θα πάρομε $0 = a_d \sigma(u)^d + \cdots + a_1 \sigma(u) + a_0$.

Ας υποθέσομε τώρα ότι η L/K είναι πεπερασμένη και $u_1, \dots, u_m$ είναι μία βάση της. Το τυπικό στοιχείο v του L έχει τη μορφή $v = a_1 u_1 + \cdots + a_m u_m$, άρα, αν σ είναι ένας K-αυτομορφισμός του L, τότε $\sigma(v) = a_1 \sigma(u_1) + \cdots + a_m \sigma(u_m)$. Συνεπώς, ο σ καθορίζεται πλήρως από τις τιμές του στά στοιχεία u_i της βάσεως. Όμως, για κάθε i, οι πιθανές τιμές του $\sigma(u_i)$ είναι, το πολύ, όσες και οι ρίζες του ελαχίστου πολυωνύμου του u_i πάνω από το K, σύμφωνα με την παραπάνω παρατήρηση. Αν λοιπόν d_i είναι ο βαθμός αυτού του πολυωνύμου, τότε το πλήθος των πιθανών τιμών της m-άδας $(\sigma(u_1), \dots, \sigma(u_m))$ είναι, το πολύ, $d_1 \cdots d_m$, άρα $|\mathcal{G}(L/K)| \leq d_1 \cdots d_m$.

Έστω τώρα ότι το $f \in K[X]$ είναι ανάγωγο βαθμού n και οι ρίζες του $\rho_k \in L$, $k = 1, \dots, n$ είναι είναι διαφορετικές. Το L είναι σώμα ανάλυσης του f πάνω από το K, συνεπώς $L = K(\rho_1, \dots, \rho_n)$. Έστω $\sigma \in \mathcal{G}(L/K)$. Λόγω της τελευταίας ισότητας, ο σ είναι πλήρως καθορισμένος από τις τιμές $\sigma(\rho_1), \dots, \sigma(\rho_n)$. Όπως είδαμε πριν, κάθε $\sigma(\rho_k)$ είναι ρίζα του f, συνεπώς, για κάθε $k = 1, \dots, n$, έστω $\sigma(\rho_k) = \rho_{k_i}$, όπου $k_i \in \{1, \dots, n\}$. Επειδή ο σ είναι 1-1, οι n το πλήθος υποδείκτες k_i είναι διαφορετικοί. Μ' άλλα λόγια, η διατεταγμένη n-άδα $(\rho_{k_1}, \rho_{k_2}, \dots, \rho_{k_n})$ είναι μετάθεση της $(1, 2, \dots, n)$. Συνεπώς, ο σ είναι πλήρως καθορισμένος από τη μετάθεση $\begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$. Διότι, η πληροφορία ότι ο σ ταυτίζεται με την παραπάνω μετάθεση, ισοδυναμεί με το ότι $\sigma(\rho_1) = \rho_{k_1}, \sigma(\rho_2) = \rho_{k_2}, \dots, \sigma(\rho_n) = \rho_{k_n}$ και αυτές οι σχέσεις αρκούν για να ορίσουν τις τιμές του σ σε κάθε στοιχείο του L. Έτσι, μπορούμε να ταυτίσομε κάθε με μία ακριβώς μετάθεση της συμμετρικής ομάδας $\mathbf{S}_n$.[1] □

Παράδειγμα 1. Έστω η επέκταση $L/\mathbb{Q}$, όπου $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Το πολυώνυμο $X^2 - 2$ είναι ανάγωγο πάνω από το $\mathbb{Q}(\sqrt{3})$ διότι, όπως εύκολα διαπιστώνεται, δεν έχει ρίζα μέσα στο $\mathbb{Q}(\sqrt{3})$ (δεν υπάρχει $a + b\sqrt{3}$ με $a, b \in \mathbb{Q}$, το οποίο να μηδενίζει το $X^2 - 2$). Εφαρμόζοντας το Θεώρημα 1.4.3 με $K = K' = \mathbb{Q}(\sqrt{3})$, τον ταυτοτικό αυτομορφισμό id_K στη θέση του σ, $p(X) = X^2 - 2$, $u = \sqrt{2}$ και $v = -\sqrt{2}$, συνάγομε την ύπαρξη ισομορφισμού $\sigma : L = \mathbb{Q}(\sqrt{3}, \sqrt{2}) \to \mathbb{Q}(\sqrt{3}, -\sqrt{2}) = L$, ο οποίος επεκτείνει τον id_K και στέλνει το $\sqrt{2}$ στο $-\sqrt{2}$. Άρα, για τον $\sigma \in \mathcal{G}(L/\mathbb{Q})$ ισχύει $\sigma(\sqrt{2}) = -\sqrt{2}$ και $\sigma(\sqrt{3}) = \sqrt{3}$. Εντελώς ανάλογα συμπεραίνομε ότι υπάρχει $\tau \in \mathcal{G}(L/\mathbb{Q})$ για τον οποίον ισχύει $\tau(\sqrt{2}) = \sqrt{2}$ και $\tau(\sqrt{3}) = -\sqrt{3}$. Τώρα, $\sigma\tau \in \mathcal{G}(L/\mathbb{Q})$ και $\sigma\tau(\sqrt{2}) = \sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma\tau(\sqrt{3}) = \sigma(-\sqrt{3}) = -\sigma(\sqrt{3}) = -\sqrt{3}$. Έτσι, μέχρι στιγμής έχομε βρεί τα εξής στοιχεία της $\mathcal{G}(L/\mathbb{Q})$: $\mathrm{id}_L, \sigma, \tau, \sigma\tau$, όπου id_L συμβολίζει τον ταυτοτικό αυτομορφισμό του L. Επειδή μία βάση της $L/\mathbb{Q}$ είναι η $1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}$, έπεται ότι κάθε $\sigma \in \mathcal{G}(L/\mathbb{Q})$ καθορίζεται πλήρως από τη δράση του επί των $\sqrt{2}$ και $\sqrt{3}$. Άρα, αν ϕ είναι τυχόν στοιχείο της $\mathcal{G}(L/\mathbb{Q})$, οι μόνες δυνατότητες για το ζεύγος τιμών $(\phi(\sqrt{2}), \phi(\sqrt{3}))$ είναι: $(\sqrt{2}, \sqrt{3}), (-\sqrt{2}, \sqrt{3}), (\sqrt{2}, -\sqrt{3}), (-\sqrt{2}, -\sqrt{3})$. Στην πρώτη περίπτωση ο ϕ ταυτίζεται με τον id_L, στη δεύτερη με τον σ, στην τρίτη με τον τ και στην τέταρτη με τον $\sigma\tau$ (παρατηρήστε ότι $\tau\sigma = \sigma\tau$). Το τελικό συμπέρασμα είναι ότι

$$\mathcal{G}(L/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^2 = \tau^2 = \mathrm{id}_L \ , \ \sigma\tau = \tau\sigma \rangle \ ,$$

[1] Το αντίστροφο, γενικά, δεν ισχύει, δηλαδή: αν πάρομε μια τυχαία μετάθεση της $\mathbf{S}_n$, δεν είναι βέβαιο ότι υπάρχει $\sigma \in \mathcal{G}(L/K)$ ο οποίος ταυτίζεται (υπό την παραπάνω έννοια) με αυτή τη μετάθεση· δείτε την άσκηση....

άρα $\mathcal{G}(L/\mathbb{Q}) \cong \mathbf{V}_4$ «ομάδα των 4 του Klein».

Παράδειγμα 2. Στο παράδειγμα αυτό χρησιμοποιειούνται, οι υποθέσεις, συμβολισμοί και τα συμπεράσματα της ενότητας 1.5.

Έστω K σώμα χαρακτηριστικής διάφορης του 2 και το ανάγωγο πολυώνυμο $f(X) = X^3 + aX + b \in K[X]$. Στην περίπτωση που $a = 0$ υποθέτομε, επιπλέον, ότι η χαρακτηριστική του σώματος K δεν είναι ούτε 3. Έστω L το σώμα ανάλυσης του f πάνω από το K. Από το Θεώρημα 1.5.1, οι ρίζες ρ, ρ', ρ'' του f είναι διαφορετικές και $L = K(\rho, \delta) = K(\rho', \delta)$. Λόγω του Θεωρήματος 1.4.3 υπάρχει ισομορφισμός $\sigma : K(\delta, \rho) \to K(\delta, \rho')$ ο οποίος επεκτείνει τον ταυτοτικό ισομορφισμό $K(\delta) \to K(\delta)$,[2] για τον οποίον ισχύει $\sigma(\rho) = \rho'$ και, φυσικά, $\sigma(\delta) = \delta$.

Θα δούμε τώρα πού απεικονίζονται οι ρίζες ρ και ρ' μέσω του σ. Επειδή $\sigma(\rho) = \rho'$, αποκλείεται η σχέση $\sigma(\rho') = \rho'$, άρα, $\sigma(\rho') = \rho''$ ή ρ. Θα αποκλείσομε το ενδεχόμενο $\sigma(\rho') = \rho$. Πράγματι, αν $\sigma(\rho') = \rho$, τότε, κατ' ανάγκη, $\sigma(\rho'') = \rho''$, διότι ο σ είναι 1-1. Εφαρμόζοντας τον σ στη σχέση (1.1) της ενότητας 1.5, παίρνομε $\sigma(\delta) = (\rho' - \rho)(\rho' - \rho'')(\rho - \rho'') = -\delta$. Αλλά $\sigma(\delta) = \delta$, άρα $-\delta = \delta$, οπότε $2\delta = 0$. Η χαρακτηριστική του K έχει υποτεθεί $\neq 2$, συνεπώς $\delta = 0$, συμπέρασμα που αντιφάσκει στην (1.1) της ενότητας 1.5. Κατ' ανάγκη λοιπόν, $\sigma(\rho') = \rho''$, οπότε (λόγω του ότι ο σ είναι 1-1) $\sigma(\rho'') = \rho$. Άρα, ο σ μπορεί να ταυτισθεί με τη μετάθεση $(\rho\,\rho'\,\rho')$ και, κατά συνέπεια, ο σ^2 ταυτίζεται με τη μετάθεση $(\rho\,\rho''\,\rho')$, καθώς και $\sigma^3 = \mathrm{id}_L$. Διακρίνομε τώρα δύο περιπτώσεις.

Πρώτη περίπτωση: $\delta \in K$, δηλαδή η διακρίνουσα $D = -4a^3 - 27b^2$ (βλ. Θεώρημα 1.5.1) ισούται με το τετράγωνο ενός στοιχείου του K. Τότε, κάθε K-αυτομορφισμός του L αφήνει αναλλοίωτο το δ, άρα, αν είναι διάφορος του ταυτοτικού και στέλνει το ρ στο ρ', τότε, σύμφωνα με ό,τι δείξαμε παραπάνω, θα ταυτίζεται με τον σ, ενώ αν στέλνει το ρ στο ρ'', εντελώς ανάλογα, θα ταυτίζεται με τη μετάθεση $(\rho\,\rho''\,\rho') = \sigma^2$. Συμπέρασμα: Στην περίπτωση αυτή η ομάδα Galois του f πάνω από το K παράγεται απ' τον αυτομορφισμό σ και είναι ισόμορφη με την *εναλλάσουσα* ομάδα $\mathbf{A}_3 = \langle(1\ 2\ 3)\rangle$ (αντιστοιχήστε τους αριθμούς $1, 2, 3$ στίς ρίζες ρ, ρ', ρ'', οπότε ο $\sigma = (\rho\ \rho'\rho'')$ ταυτίζεται με τη μετάθεση $(1\ 2\ 3)$).

Δεύτερη περίπτωση: $\delta \notin K$, δηλαδή η διακρίνουσα $D = -4a^3 - 27b^2$ δεν ισούται με το τετράγωνο ενός στοιχείου του K. Εξετάζομε αν, εκτός από τους σ, σ^2 υπάρχει και άλλος μη ταυτοτικός K-αυτομορφισμός του L. Στην περίπτωση αυτή το $X^2 - D$ είναι ανάγωγο πάνω από το $K(\rho)$ (γιατί, αλλοιώς, η κυβική επέκταση $K(\rho)$ του K θα περιείχε την τετραγωνική επέκταση $K(\delta)$, που αντιβαίνει στο Θεώρημα 1.1.4). Άρα, από το Θεώρημα 1.4.3, ο ταυτοτικός αυτομορφισμός $K(\rho) \to K(\rho)$ επεκτείνεται σε αυτομορφισμό $\tau : K(\rho, \delta) \to K(\rho, \delta)$, τέτοιον ώστε $\tau(\delta) = -\delta$ και, φυσικά, $\tau(\rho) = \rho$. Από τους τύπους του Θεωρήματος 1.5.1 είναι τώρα πολύ εύκολο να διαπιστώσομε ότι $\tau(\rho') = \rho''$, $\tau(\rho'') = \rho'$, άρα μπορούμε να ταυτίσομε τον τ με την αντιμετάθεση $(\rho'\rho'')$ ή, ακόμη και με την αντιμετάθεση $(2\ 3)$. Στην περίπτωση, δηλαδή, που εξετάζομε τώρα, η ομάδα Galois του f παράγεται απ' τους αυτομορφισμούς σ και τ, τους οποίους μπορούμε να ταυτίσομε, αντιστοίχως, με τις μεταθέσεις $(1\ 2\ 3)$ και $(2\ 3)$. Καθώς αυτές οι δύο μεταθέσεις παράγουν τη συμμετρική ομάδα $\mathbf{S}_3$, η ομάδα $\mathcal{G}(L/K)$ περιέχει ως υποομάδα

[2] Παρατηρήστε ότι $K(\delta) = K$ στην περίπτωση που $\delta \in K$. Παρατηρήστε, επίσης, ότι, για την εφαρμογή του Θεωρήματος 1.4.3, πρέπει να βεβαιωθούμε ότι το f είναι ανάγωγο πάνω από το $K(\delta)$· βλ. άσκηση 4.

την $\mathbf{S}_3$, άρα ταυτίζεται με αυτήν διότι, ισχύει και το αντίστροφο, αφού, σύμφωνα με το Θεώρημα 2.1.2, η $\mathcal{G}(L/K)$ ταυτίζεται με μία υποομάδα της $\mathbf{S}_3$.

Συνοψίζοντας όλα τα προηγούμενα καταλήγομε στο εξής συμπέρασμα:

> Αν η διακρίνουσα ενός ανάγωγου κυβικού πολυωνύμου f όπως αυτό του Θεωρήματος 1.5.1 είναι τετράγωνο στοιχείου του K, τότε η ομάδα Galois του f πάνω από το K είναι ισόμορφη με την $\mathbf{A}_3$, διαφορετικά, είναι ισόμορφη με την $\mathbf{S}_3$.

Παράδειγμα 3. Τώρα θεωρούμε το $f(X) = X^4 - 2 \in \mathbb{Q}[X]$ και θέτομε $\rho = \sqrt[4]{2}$. Όλες οι ρίζες του f είναι $\pm\rho, \pm i\rho$ και, συνεπώς, το σώμα ανάλυσης, έστω L, του πολυωνύμου αυτού πάνω από το $\mathbb{Q}$ είναι το $\mathbb{Q}(\rho, i)$. Είναι απλό να δείξει κανείς ότι $[L : \mathbb{Q}] = 8$ (άσκηση 1). Επίσης, με τη βοήθεια του Θεωρήματος 1.4.3 μπορούμε να δείξομε ότι υπάρχουν $\sigma, \tau \in \mathcal{G}(L/\mathbb{Q})$ τέτοια ώστε

$$\sigma(\rho) = i\rho\,,\ \sigma(i) = i \qquad \tau(\rho) = \rho\,,\ \tau(i) = -i\,.$$

(άσκηση 2). Τότε εύκολα κατασκευάζομε τον παρακάτω πίνακα:

αυτομορφισμός	δράση στο ρ	δράση στο i
id_L	ρ	i
σ	$i\rho$	i
σ^2	$-\rho$	i
σ^3	$-i\rho$	i
τ	ρ	$-i$
$\sigma\tau$	$i\rho$	$-i$
$\sigma^2\tau$	$-\rho$	$-i$
$\sigma^3\tau$	$-i\rho$	$-i$

Επειδή κάθε στοιχείο της $\mathcal{G}(L/\mathbb{Q})$, (1) στέλνει το ρ σε ένα από τα $\rho, -\rho, i\rho, -i\rho$ και το i σε ένα από τα $i, -i$ και (2) καθορίζεται πλήρως από τη δράση του στά ρ και i, έπεται ότι οι οκτώ αυτομορφισμοί του παραπάνω πίνακα καλύπτουν ολόκληρη την ομάδα $\mathcal{G}(L/\mathbb{Q})$. Η ομάδα αυτή είναι η *διεδρική* $\mathbf{D}_4$ της οποίας η αφηρημένη περιγραφή είναι

$$\mathbf{D}_4 = \langle \sigma, \tau \,:\, \sigma^4 = 1\,,\ \tau^2 = 1\,,\ \tau\sigma = \sigma^3\tau \rangle\,.$$

Ασκήσεις

1. Με τον συμβολισμό του Παραδείγματος 3, αποδείξτε ότι $[L : \mathbb{Q}] = 8$.

2. Αποδείξτε την ύπαρξη των αυτομορφισμών σ και τ του Παραδείγματος 3.

3. Υπολογίστε την ομάδα Galois του $X^3 - 2 \in \mathbb{Q}[X]$ δίχως να χρησιμοποιήσετε τα συμπεράσματα του Παραδείγματος 2.

   Υπόδειξη. Το σώμα ανάλυσης του $X^3 - 2$ είναι, ως υπόσωμα του $\mathbb{C}$, το $\mathbb{Q}(\rho, \omega)$, όπου $\rho = \sqrt[3]{2} \in \mathbb{R}$ και ω είναι κυβική ρίζα της μονάδας διαφορετική από 1. Δείξτε ότι $\omega^2 + \omega + 1 = 0$.

4. Με τα δεδομένα και τις υποθέσεις του Παραδείγματος 2, αποδείξτε ότι το πολυώνυμο f είναι ανάγωγο πάνω από το σώμα $K(\delta)$.

5. Αναφερόμενοι στο Παράδειγμα 3, αριθμήστε τις ρίζες $\rho, -\rho, i\rho, -i\rho$ του X^4-2 με $1,2,3,4$ αντιστοίχως και δείξτε ότι οι σ και τ ταυτίζονται, με τις μεταθέσεις (γραμμένες ως κύκλοι της $\mathbf{S}_4$) $(1\,3\,2\,4)$ και $(3\,4)$ αντιστοίχως.

6. Έστω $f(X) = X^4 - 2X^2 - 1 \in \mathbb{Q}[X]$. Θεωρήστε δεδομένο ότι το f είναι ανάγωγο πάνω από το $\mathbb{Q}$. Λύνοντας την εξίσωση $x^4 - 2x^2 - 1 = 0$,[3] διαπιστώστε ότι οι ρίζες του f είναι $\pm\alpha \in \mathbb{R}$ και $\pm\beta \in i\mathbb{R}$, όπου

$$\alpha = \sqrt{\sqrt{2}+1}, \quad \beta = i\sqrt{\sqrt{2}-1},$$

όπου με $\sqrt{2}$ εννοούμε τη θετική τετραγωνική ρίζα του 2.

(α') Δείξτε ότι $\beta = i\alpha^{-1}$ και συμπεράνετε ότι το $L = \mathbb{Q}(\alpha, i)$ είναι σώμα ανάλυσης του f πάνω από το $\mathbb{Q}$ και $[L : \mathbb{Q}] = 8$. Δείξτε, επίσης, ότι $\sqrt{2} \in L$.

(β') Αποδείξτε ότι υπάρχουν $\sigma, \tau \in \mathcal{G}(L/\mathbb{Q})$ με τις εξής ιδιότητες:

$$\sigma(\alpha) = \beta,\ \sigma(i) = -i \quad \text{και} \quad \tau(\alpha) = -\alpha,\ \tau(i) = -i.$$

(γ') Ποια μετάθεση προκαλεί ο σ στις ρίζες $\alpha, -\alpha, \beta, -\beta$ και ποια ο τ; Αν αριθμήσομε τις ρίζες αυτές με $1,2,3,4$, αντιστοίχως, με ποιες μεταθέσεις της συμμετρικής ομάδας $\mathbf{S}_4$ μπορούμε να ταυτίσομε τους σ και τ; Βλέποντας ως μεταθέσεις τους σ, τ δείξτε ότι οι τάξεις τους είναι 4 και 2, αντιστοίχως και $\tau\sigma = \sigma^3\tau$. Συμπεράνετε ότι η υποομάδα της $\mathcal{G}(L/\mathbb{Q})$ που παράγουν οι σ, τ είναι η $\mathbf{D}_4$. Τέλος, δείξτε ότι $\mathcal{G}(L/\mathbb{Q}) = \mathbf{D}_4$.

[3] Θέτοντας $x^2 = y$ και λύνοντας πρώτα τη δευτεροβάθμια $y^2 - 2y - 1 = 0$. Δείτε ότι ως άγνωστο της εξίσωσης χρησιμοποιώ το γράμμα x, όχι το X που χρησιμοποιούμε ως μεταβλητή των πολυωνύμων!

2.2 Η αντιστοιχια Galois

Έστω L/K *πεπερασμένη* επέκταση. Κάθε υπόσωμα του L, το οποίο είναι συγχρόνως και επέκταση του K, λέγεται *ενδιάμεση επέκταση* της L/K. Συμβολίζομε με $\mathcal{E}$ το σύνολο των ενδιάμεσων επεκτάσεων της L/K. Έστω $G = \mathcal{G}(L/K)$. Σύμφωνα με το Θεώρημα 2.1.2, η G είναι πεπερασμένη ομάδα και συμβολίζομε με $\mathcal{O}$ το σύνολο όλων των υποομάδων της G.

Πρόταση 2.2.1. *Αν $H \in \mathcal{O}$, τότε το*

$$\mathcal{F}_L(H) \overset{ορσ}{=} \{u \in L : \sigma(u) = u \ \ \forall \sigma \in H\}$$

ανήκει στο $\mathcal{E}$.

Απόδειξη. Πρώτ' απ' όλα, $1 \in \mathcal{F}_L(H)$, αφού το 1 παραμένει αναλλοίωτο από όλους τους αυτομορφισμούς. Ακόμη, αν $u, v \in \mathcal{F}_L(H)$ τότε, για κάθε $\sigma \in H$, $\sigma(uv) = \sigma(u)\sigma(v) = uv$, άρα $uv \in \mathcal{F}_L(H)$. Εντελώς ανάλογα, αν $u \in \mathcal{F}_L(H)$, τότε και $u^{-1} \in \mathcal{F}_L(H)$. □

Ορίζομε τώρα τις εξής απεικονίσεις μεταξύ των $\mathcal{E}$ και $\mathcal{O}$.

$$\mathcal{G}(L/\cdot) : \mathcal{E} \ni E \longrightarrow \mathcal{G}(L/E) \in \mathcal{O}$$

$$\mathcal{F}_L : \mathcal{O} \ni H \longrightarrow \mathcal{F}_L(H) \in \mathcal{E} \ .$$

Εύκολα βλέπει κανείς ότι $\mathcal{G}(L/\mathcal{F}_L(H)) \supseteq H$ για κάθε υποομάδα H της $\mathcal{G}(L/K)$. Πράγματι, έστω $\sigma \in H$. Ο σ ανήκει στην ομάδα $\mathcal{G}(L/\mathcal{F}_L(H))$ αν, και μόνο αν, αφήνει αναλλοίωτα όλα τα στοιχεία του σώματος $\mathcal{F}_L(H)$. Εξ ορισμού όμως, αυτά τα στοιχεία μένουν αναλοίωτα από κάθε αυτομορφισμό που ανήκει στην H, άρα και από το σ. Το αντίστροφο, ότι δηλαδή $\mathcal{G}(L/\mathcal{F}_L(H)) \subseteq H$, έχει μεγάλη απόδειξη, την οποία παραλείπομε. Διατυπώνομε όμως το συμπέρασμά μας ως εξής:

> Έστω L/K πεπερασμένη επέκταση. Για κάθε υποομάδα H της $\mathcal{G}(L/K)$ ισχύει $\mathcal{G}(L/\mathcal{F}_L(H)) = H$.

Κατ' αναλογίαν με την $\mathcal{G}(L/\mathcal{F}_L(H)) \supseteq H$ αποδεικνύεται, το ίδιο εύκολα και η σχέση $\mathcal{F}_L(\mathcal{G}(L/E)) \supseteq E$ για κάθε ενδιάμεση επέκταση E της L/K (δηλαδή, για κάθε $E \in \mathcal{E}$). Αποδεικνύεται ότι η αντίστροφη σχέση, δηλαδή η $\mathcal{F}_L(\mathcal{G}(L/E)) \subseteq E$, δεν ισχύει, παρά μόνο αν η επέκταση L/K είναι, όπως λέμε, *επέκταση Galois*.

Ορισμός 2.2.2. *Μία επέκταση L/K λέγεται Galois αν είναι κανονική και διαχωρίσιμη.*

Παρακάτω, ορίζομε και επεξηγούμε αυτές τις δύο έννοιες.

Ορισμός 2.2.3. *Η επέκταση L/K λέγεται κανονική, αν κάθε ανάγωγο πολυώνυμο του $K[X]$, που έχει ένα πρωτοβάθμιο παράγοντα στο $L[X]$, αναλύεται πλήρως σε πρωτοβάθμιους παράγοντες του $L[X]$.*
Με λιγότερο αυστηρή, αλλά πιο παραστατική διατύπωση: Η επέκταση L/K λέγεται κανονική, αν

κάθε ανάγωγο πολυώνυμο του $K[X]$, που έχει μία ρίζα μέσα στο L έχει και όλες τις υπόλοιπες ρίζες στο L.

Δηλαδή, η επέκταση K/L είναι κανονική αν *κάθε ανάγωγο πολυώνυμο του $K[X]$ ή έχει όλες τις ρίζες του μέσα στο L, ή καμμία ρίζα μέσα στο L.* Όλα ή τίποτα!
Για παράδειγμα, αν $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{d})$, όπου $d \in \mathbb{Q}$ δεν είναι τετράγωνο ρητού, η L/K είναι κανονική. Πράγματι, έστω $f(X) \in \mathbb{Q}[X]$ ανάγωγο, του οποίου μία ρίζα ανήκει στο L. Τότε η ρίζα αυτή έχει τη μορφή $a + b\sqrt{d}$, $a, b \in \mathbb{Q}, b \neq 0$. Αν στη σχέση $f(a + b\sqrt{d}) = 0$ εφαρμοστεί ο $\mathbb{Q}$-αυτομορφισμός που στέλνει το $a + b\sqrt{d}$ στο $a - b\sqrt{d}$, συμπεραίνομε ότι και το $a - b\sqrt{d}$ είναι ρίζα του $f(X)$, συνεπώς $f(X) = (X - (a + b\sqrt{d}))(X - (a - b\sqrt{d}))g(X)$ για κάποιο $g(X) \in L[X]$. Άρα $f(X) = (X^2 - 2aX + (a^2 - db^2))g(X)$, απ' όπου φαίνεται ότι το $g(X)$ έχει ρητούς συντελεστές, ως πηλίκο δύο πολυωνύμων με ρητούς συντελεστές. Όμως το $f(X)$ έχει υποτεθεί ανάγωγο, άρα το $g(X)$ είναι σταθερό πολυώνυμο και, συνεπώς, οι μόνες ρίζες του $f(X)$ είναι οι $a \pm b\sqrt{d}$, που, όπως είδαμε ήδη, ανήκουν στο L. Ευτυχώς, υπάρχει ένα πολύ βολικό κριτήριο για να εξετάζομε αν μία πεπερασμένη επέκταση είναι κανονική.

Θεώρημα 2.2.4. *Η πεπερασμένη επέκταση L/K είναι κανονική αν και μόνο αν το L είναι σώμα ανάλυσης ενός μη σταθερού πολυωνύμου του $K[X]$.*

Απόδειξη. Έστω ότι η L/K είναι πεπερασμένη κανονική επέκταση και $L = K(u_1, \dots, u_n)$ [4]. Για $j = 1, \dots, n$ έστω $f_j \in K[X]$ το ελάχιστο πολυώνυμο του u_j πάνω από το K. Λόγω κανονικότητας της L/K και του ότι $u_j \in L$, συμπεραίνομε ότι το f_j αναλύεται σε πρωτοβάθμιους παράγοντες του $L[X]$, οπότε το σύνολο S_j των ριζών του f_j περιέχεται στο L. Είναι τώρα

$$L = K(u_1, \dots, u_n) \subseteq K(S_1 \cup \cdots \cup S_n).$$

Όμως, $S_j \subset L$ για κάθε $j = 1, \dots, n$, συνεπώς ισχύει και $K(S_1 \cup \cdots \cup S_n) \subseteq L$, άρα $L = K(S_1 \cup \cdots \cup S_n)$. Συνεπώς το L είναι σώμα ανάλυσης πάνω από το K του πολυωνύμου $f_1 \cdots f_n \in K[X]$.

Αντιστρόφως, έστω L σώμα ανάλυσης του μη σταθερού $f \in K[X]$. Έστω $g \in K[X]$ ανάγωγο, το οποίο έχει μια ρίζα του, έστω u_1 μέσα στο L. Πρέπει και αρκεί να αποδειχθεί ότι το g αναλύεται σε πρωτοβάθμιους παράγοντες του $L[X]$. Έστω M σώμα ανάλυσης του πολυωνύμου $f \cdot g$ πάνω από το L. Το M περιέχει τη ρίζα u_1 καθώς και όλες τις υπόλοιπες ρίζες του g. Έστω $u_2 \in M$ μια οποιαδήποτε άλλη ρίζα του g. Πρέπει και αρκεί ν' αποδειχθεί ότι $u_2 \in L$.

Δείχνομε πρώτα ότι $[L(u_2) : L] = [L(u_1) : L]$.
Για $j = 1, 2$ ισχύει $[L(u_j) : L][L : K] = [L(u_j) : K] = [L(u_j) : K(u_j)][K(u_j) : K]$, άρα

$$[L(u_1) : L][L : K] = [L(u_1) : K(u_1)][K(u_1) : K]$$

και

$$[L(u_2) : L][L : K] = [L(u_2) : K(u_2)][K(u_2) : K].$$

[4] Π.χ., αν $[L : K] = n$ και $u_1, \dots, u_n$ είναι βάση της L/K, τότε $L = K(u_1, \dots, u_n)$.

Επειδή u_1, u_2 είναι ρίζες του ίδιου ανάγωγου πολυωνύμου $g \in K[X]$, έπεται, από το Θεώρημα 1.4.3 ότι υπάρχει K-ισομορφισμός $\sigma : K(u_1) \to K(u_2)$, επομένως, $[K(u_2) : K] = [K(u_1) : K]$ $(*)$. Επίσης, επειδή το L είναι σώμα ανάλυσης του f πάνω από το K, έπεται εύκολα (απλή άσκηση) ότι, για $j = 1, 2$, το $L(u_j)$ είναι σώμα ανάλυσης του f πάνω από το $K(u_j)$, άρα, βάσει του Θεωρήματος 1.4.4, ο ισομορφισμός σ επεκτείνεται σε ισομορφισμό $L(u_1) \to L(u_2)$ και συνεπώς $[L(u_2) : K(u_2)] = [L(u_1) : K(u_1)]$ $(**)$. Συνδυάζοντας το παραπάνω ζευγάρι σχέσεων με τις $(*)$ και $(**)$, παίρνομε $[L(u_2) : L] = [L(u_1) : L] = 1$, όπου η τελευταία ισότητα προκύπτει από το ότι $u_1 \in L$. Συνεπώς $L(u_2) : L] = 1$, που σημαίνει ότι $u_2 \in L$. □

Με αυτό το κριτήριο, το συμπέρασμα του παραπάνω παραδείγματος είναι προφανές, διότι $L = \mathbb{Q}(\sqrt{d})$ και, συνεπώς το L είναι το σώμα ανάλυσης πάνω από το $\mathbb{Q}$ του $X^2 - d \in \mathbb{Q}[X]$. Άλλη εφαρμογή του Θεωρήματος 2.2.4 είναι στην επέκταση $L/\mathbb{Q}$ με $L = \mathbb{Q}(\rho)$ και ρ ρίζα του $f(X) = X^3 - 3X + 1$. Σύμφωνα με την άσκηση 1.3.7, το σώμα ανάλυσης του $f(X)$ είναι το $\mathbb{Q}(\rho)$, άρα η επέκταση $L/\mathbb{Q}$ είναι κανονική. Αντιθέτως, η $L/\mathbb{Q}$ με $L = \mathbb{Q}(\rho)$ και ρ ρίζα του $f(X) = X^3 - 2$, δεν είναι κανονική, διότι οι άλλες ρίζες του $f(X)$, πλήν της ρ, δεν είναι πραγματικές και, συνεπώς, δεν ανήκουν στο L. Εδώ, όπως και σε κάθε περίπτωση που θέλομε να δείξομε ότι μία επέκταση L/K δεν είναι κανονική, δεν χρειάζεται να εφαρμόζομε το Θεώρημα 2.2.4; σύμφωνα με τον ορισμό, αρκεί να δείξομε ότι ένα οποιοδήποτε ανάγωγο πολυώνυμο του $K[X]$ έχει κάποια ρίζα του εκτός του L.

Ορισμός 2.2.5. *(α′) Έστω σώμα K και μη μηδενικό $f(X) \in K[X]$. Λέμε ότι το $f(X)$ είναι* διαχωρίσιμο πολυώνυμο *αν όλες οι ρίζες του είναι απλές.*
(β′) Έστω L/K μία επέκταση. Το αλγεβρικό στοιχείο $u \in L$ λέγεται διαχωρίσιμο πάνω από το K, αν το ελάχιστο πολυώνυμό του πάνω από το K είναι διαχωρίσιμο. Η αλγεβρική επέκταση L/K λέγεται διαχωρίσιμη αν κάθε στοιχείο της είναι διαχωρίσιμο πάνω από το K.

Για τη μελέτη των διαχωρισίμων πολυωνύμων είναι χρήσιμη η έννοια της *τυπικής παραγώγου* πολυωνύμου.

Ορισμός 2.2.6. *Έστω σώμα K και $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, τότε ως τυπική παράγωγο, ή απλώς, παράγωγο του $f(X)$ ορίζομε το πολυώνυμο $f'(X) = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + a_1$.*[5].

Με αλγεβρικές πράξεις μόνο αποδεικνύονται οι εξής ιδιότητες:[6] Αν $f, g \in K[X]$, τότε

$$(f+g)' = f' + g' \,,\ (f \cdot g)' = f' \cdot g + f \cdot g' \,,\ (f^m)' = m \cdot f^{m-1} \cdot f' \,. \tag{2.1}$$

Πρόταση 2.2.7. *Έστω σώμα K και $f(X) \in K[X]$. Έστω επέκταση L του K και $\lambda \in L$. Τότε, το λ είναι πολλαπλή ρίζα του $f(X)$ αν και μόνο αν $f'(\lambda) = 0$.*

Απόδειξη Έστω ότι το $f(X)$ έχει ρίζα το λ με πολλαπλότητα r. Τότε $f(X) = (X-\lambda)^r g(X)$, όπου $g(X) \in L[X]$, $r \geq 1$ και $g(\lambda) \neq 0$. Εφαρμόζοντας κατάλληλα τους τύπους (2.1) έχομε

[5] Την ιδέα για να ορίσομε το f' παίρνομε, φυσικά, από τον Απειροστικό Λογισμό.
[6] Όχι Ανάλυση ! Άλλωστε, δεν μπορούμε να «κάνομε Ανάλυση» στο M, αφού αυτό το σώμα είναι τυχαίο και δεν έχει τοπολογία, άρα, σ' αυτό δεν υπάρχει έννοια σύγκλισης.

$f'(X) = r(X-\lambda)^{r-1}g(X) + (X-\lambda)^r g'(X)$.
Αν το λ είναι πολλαπλή ρίζα του $f(X)$, τότε $r \geq 2$, και από την παραπάνω έκφραση του $f'(X)$ βλέπομε ότι $f'(\lambda) = 0$.
Αντιστρόφως, αν $f'(\lambda) = 0$, τότε, $r \geq 2$. Πράγματι, σε αντίθετη περίπτωση, θα ήταν $r = 1$, οπότε η παραπάνω έκφραση του $f'(X)$ θα μας έδινε $f'(X) = g(X) + (X-\lambda)^r g'(X)$ και τότε, $f'(\lambda) = g'(\lambda) \neq 0$; αντίφαση. □

Αμέσως παρακάτω θα δείξομε ότι τα ανάγωγα πολυώνυμα με συντελεστές από δύο σημαντικές κατηγορίες σωμάτων είναι ανάγωγα. Η πρώτη κατηγορία περιλαμβάνει τα σώματα χαρακτηριστικής 0 και η δεύτερη τα πεπερασμένα σώματα. των σωμάτων της δεύτερης κατηγορίας η χαρακτηριστική είναι πρώτος αριθμός και θα αποδείξομε την εξής σημαντική πρόταση.

Πρόταση 2.2.8. *Έστω πεπερασμένο σώμα K χαρακτηριστικής p.*[7] *Τότε η απεικόνιση $\phi : K \to K$, που ορίζεται $\phi(a) = a^p$ για κάθε $a \in K$, είναι αυτομορφισμός του K και ονομάζεται αυτομορφισμός Frobenius . Ειδικώτερα, αφού η ϕ είναι «έπί», για κάθε $a \in K$ υπάρχει $b \in K$, τέτοιο ώστε $a = b^p$.*

Απόδειξη. Για κάθε $a, b \in K$ ισχύει η ταυτότητα (διώνυμο του Newton) $(a+b)^p = a^p + b^p + \sum_{k=1}^{p-1} \begin{pmatrix} p \\ k \end{pmatrix} a^{p-k}b^k$. Σάν άσκηση Θεωρίας Αριθμών μπορεί να δείξει κανείς ότι καθένας από τους διωνυμικούς συντελεστές μέσα στο άθροισμα $\sum_{k=1}^{p-1}(\cdots)$ είναι 0 (παίζει ρόλο το ότι ο p είναι πρώτος) και, επειδή η χαρακτηριστική του K είναι p, όλοι οι όροι αυτού του αθροίσματος μηδενίζονται. Άρα, $(a+b)^p = a^p + b^p$. Προφανώς $(ab)^p = a^p b^p$, οπότε αυτές οι δύο τελευταίες σχέσεις μας λένε ότι η απεικόνιση ϕ είναι ομομορφισμός. Ο πυρήνας του ϕ είναι ο τετριμμένος, διότι, αν $\phi(a) = 0$, τότε $a^p = 0$, άρα[8] $a = 0$. Συνεπώς, ο ϕ είναι μονομορφισμός. Τέλος, αφού η ϕ απεικονίζει πεπερασμένο σύνολο στον εαυτό του και είναι 1-1, υποχρεωτικά είναι και «έπί».
Παρατήρηση. Η ταυτότητα $(a+b)^p = a^p + b^p$ ισχύει σε κάθε μεταθετικό δακτύλιο με μοναδιαίο, του οποίου η χαρακτηριστική είναι p. Η σχέση αυτή γενικεύεται: $(a_1 + a_2 + \cdots + a_k)^p = a_1^p + a_2^p + \cdots + a_k^p$ (απλή επαγωγική απόδειξη). Συνεπώς, αν το σώμα K έχει χαρακτηριστική p, τότε $K[X]$ είναι μεταθετικός δακτύλιος με μοναδιαίο και η χαρακτηριστική του είναι p. Άρα, στην περίπτωση αυτή, ισχύει στον $K[X]$ η ταυτότητα $(f_1(X) + f_2(X) + \cdots + f_k(X))^p = f_1(X)^p + f_2(X)^p + \cdots + f_k(X)^p$.

Θεώρημα 2.2.9. *Έστω σώμα K. Αν η χαρακτηριστική του K είναι 0, είτε το K είναι πεπερασμένο, τότε κάθε ανάγωγο πολυώνυμο του $K[X]$ είναι διαχωρίσιμο. Συνεπώς, κάθε αλγεβρική επέκταση πάνω από ένα τέτοιο σώμα K είναι διαχωρίσιμη.*

Απόδειξη. Έστω ανάγωγο $f(X) = \sum_{k=1}^{n} a_k X^k$, όπου $n \geq$ και $a_n \neq 0$. Ας υποθέσομε ότι το $f(X)$ δεν είναι διαχωρίσιμο και έστω λ μία ρίζα του $f(X)$ σε κάποια επέκταση L/K, της οποίας η πολλαπλότητα είναι > 1. Θα καταλήξομε σε άτοπο.

[7] Ο p είναι, υποχρεωτικά, πρώτος.
[8] Είμαστε σε σώμα, άρα δεν υπάρχουν μηδενοδιαιρέτες.

Έστω, πρώτα, ότι η χαρακτηριστική του K είναι 0. Από την Πρόταση 2.2.7 έχομε ότι $f'(\lambda) = 0$. Από την Πρόταση B'.5(2) του Παραρτήματος B' συμπεραίνομε ότι $f(X)|f'(X)$. Αυτή η σχέση, όμως, είναι αδύνατη διότι, $f'(X) = na_nX^{n-1} + (\textit{όροι βαθμού} < n-1)$ και $na_n \neq 0$ (σ' αυτή την τελευταία σχέση παίζει ρόλο το ότι η χαρακτηριστική είναι 0) , οπότε το $f(X)$ διαιρεί ένα μη μδενικό πολυώνυμο μικροτέρου βαθμού; άτοπο.

Έστω τώρα ότι το K είναι πεπερασμένο και η χαρακτηριστική του είναι p. Όπως και στην περίπτωση της χαρακτηριστικής 0, καταλήγομε στη σχέση $f(X)|f'(X)$. Αν το $f'(X)$ ήταν μη μηδενικό, θα οδηγούμαστε σε άτοπο διότι το $f(X)$ θα διαιρούσε ένα μη μηδενικό πολυώνυμο μικροτέρου βαθμού. Άρα, αναγκαζόμαστε να δεχθούμε ότι το $f'(X)$ είναι μηδενικό πολυώνυμο. Τώρα γράφομε το $f(X)$ ως εξής:

$$f(X) = a_{n_1}X^{n_1} + a_{n_2}X^{n_2} + \cdots + a_{n_k}X^{n_k}, \;\; n_1 > n_2 > \cdots > n_k \geq 0, \; a_{n_1}a_{n_2}\cdots a_{n_k} \neq 0,$$

οπότε

$$f'(X) = n_1a_{n_1}X^{n_1-1} + n_2a_{n_2}X^{n_2-1} + \cdots + n_ka_{n_k}X^{n_k-1}.$$

Επειδή το $f'(X)$ είναι μηδενικό, συμπεραίνομε ότι $n_1a_{n_1} = n_2a_{n_2} = \ldots n_ka_{n_k} = 0$. Όμως, τα $a_{n_1}, a_{n_2}, \ldots, a_{n_k}$ είναι $\neq 0$, άρα όλοι οι ακέραιοι $n_1, n_2, \ldots, n_k$ είναι πολλαπλάσια του p. Θέτομε $n_i = pm_i$ για $i = 1, \ldots, k$. Επίσης, λόγω της Πρότασης 2.2.8, υπάρχουν $b_1, b_2, \ldots, b_k$, τέτοια ώστε $a_{n_i} = b_i^p$. Συνεπώς,

$$f(X) = b_1^p(X^{m_1})^p + b_2^p(X^{m_2})^p + \cdots + b_k^p(X^{m_k})^p = (b_1X^{m_1} + b_2X^{m_2} + \cdots b_kX^{m_k})^p,$$

όπου η τελευταία ισότητα είναι συνέπεια της παρατήρησης αμέσως μετά την Πρόταση 2.2.8. Βλέπομε, δηλαδή, ότι το $f(X)$ είναι p-δύναμη ενός άλλου πολυωνύμου του $K[X]$ και αυτό αντιβαίνει στην υπόθεση ότι το $f(X)$ είναι ανάγωγο πάνω απ' το K. □

Πόρισμα 2.2.10. *Αν το K είναι σώμα χαρακτηριστικής 0, είτε πεπερασμένο σώμα, τότε οι έννοιες «κανονική επέκταση του K» και «Galois επέκταση του K» είναι ισοδύναμες. Άρα, συνδυάζοντας με το Θεώρημα 2.2.4, συμπεραίνομε: Αν το K είναι σώμα χαρακτηριστικής 0, είτε πεπερασμένο σώμα και το L είναι σώμα ανάλυσης πάνω απ' το K μη μηδενικού πολυωνύμου $f(X) \in K[X]$, τότε η επέκταση L/K είναι Galois.*

Ένα παράδειγμα ανάγωγου και μη διαχωρίσιμου πολυωνύμου. Έστω πρώτος p. Θεωρούμε το σώμα $\mathbb{Z}_p$ και, κατόπιν, το σώμα $K = \mathbb{Z}_p(t)$ των «ρητών συναρτήσεων» μεταβλητής t με συντελεστές στο $\mathbb{Z}_p$, το τυπικό στοιχείο του οποίου έχει τη μορφή $f(t)/g(t)$, όπου f, g είναι πολυώνυμα μεταβλητής t με συντελεστές στο $\mathbb{Z}_p$. Έστω L σώμα ανάλυσης του $h(X) = X^p - t \in K[X]$ και $s \in L$ ρίζα του h, οπότε $s^p = t$. Λόγω του ότι το L έχει χαρακτηριστική p, ισχύει $(X-s)^p = X^p - s^p = X^p - t = h(X)$, άρα το h έχει μία μόνο ρίζα και η πολλαπλότητά της είναι p. Θα δείξομε ότι το h είναι ανάγωγο.

Έστω $h(X) = f(X)g(X)$ με $\phi(X), \psi(X) \in K[X]$ μη σταθερά, οπότε $1 \leq \deg f = n < p$. Λόγω της $\phi(X)\psi(X) = h(X) = (X-s)^p$ και της μονοσήμαντης ανάλυσης σε ανάγωγα πολυώνυμα πάνω από ένα σώμα, είναι $\phi(X) = (X-s)^n$. Ο σταθερός όρος του $\phi(X)$ ανήκει

στο K. Αφετέρου, αυτός ο σταθερός όρος είναι $\pm s^n$, άρα $s^n \in K$. Καθώς $1 < n < p$, ο n είναι πρώτος προς τον p, άρα υπάρχουν ακέραιοι a, b ώστε να ισχύει $an + bp = 1$, οπότε $s = (s^n)^a (s^p)^b = (s^n)^a \cdot t^b \in K$. Συνεπώς, $s = f(t)/g(t)$ με $f(t), g(t) \in K[t]$. Λόγω της σχέσης $t = s^p$ έχομε τώρα $f(t)^p = t \cdot g(t)^p$. Αυτή η σχέση, όμως, είναι αδύνατη. Γιατί, αν $\deg f = \mu$ και $\deg g = \nu$, τότε ο βαθμός του πολυωνύμου (ως προς t) στο αριστερό μέλος είναι $p\mu$, ενώ ο βαθμός του πολυωνύμου στο αριστερό μέλος είναι $p\nu + 1$.

Ας επανέλθομε τώρα στο ερώτημα που είχε μείνει αναπάντητο: Πότε ισχύει η ισότητα στη σχέση $\mathcal{F}_L(\mathcal{G}(L/E)) \supseteq E$;

> Έστω L/K πεπερασμένη, κανονική και διαχωρίσιμη επέκταση, δηλαδή, πεπερασμένη επέκταση Galois. Τότε, για κάθε ενδιάμεση επέκταση E ισχύει $\mathcal{F}_L(\mathcal{G}(L/E)) = E$.

Σε αυτές τις σημειώσεις παραλείπομε την απόδειξη. Τα δύο βασικά συμπεράσματα, όσον αφορά στίς συνθέσεις των απεικονίσεων $\mathcal{G}(L/\cdot) \circ \mathcal{F}_L$ και $\mathcal{F}_L \circ \mathcal{G}(L/\cdot)$, στά οποία καταλήξαμε μέχρι τώρα, συνδυαζόμενα μας οδηγούν στο εξής συμπέρασμα:

Θεώρημα 2.2.11. *Έστω L/K πεπερασμένη επέκταση Galois, $\mathcal{E}$ το σύνολο των ενδιάμεσων επεκτάσεων και $\mathcal{O}$ το σύνολο των υποομάδων της $\mathcal{G}(L/K)$. Τότε οι απεικονίσεις*

$$\mathcal{G}(L/\cdot) : \mathcal{E} \ni E \longrightarrow \mathcal{G}(L/E) \in \mathcal{O}$$

$$\mathcal{F}_L : \mathcal{O} \ni H \longrightarrow \mathcal{F}_L(H) \in \mathcal{E} \, .$$

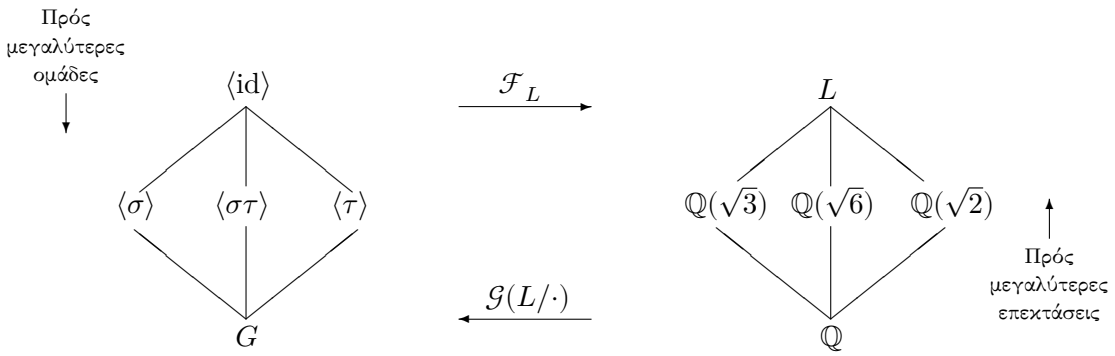
είναι αντίστροφες η μία της άλλης. Ειδικώτερα, κάθε μία από αυτές τις απεικονίσεις είναι αμφιμονοσήμαντη, επί. Αυτή η 1-1 αντιστοιχία μεταξύ ενδιάμεσων επεκτάσεων και υποομάδων της ομάδος Galois ονομάζεται αντιστοιχία Galois.

Ας δούμε τώρα τα τρία παραδείγματα της ενότητας 2.1 υπό το πρίσμα του Θεωρήματος 2.2.11, χρησιμοποιώντας τους συμβολισμούς κλπ καθενός από αυτά.

Παράδειγμα 1. (Βλ. Παράδειγμα 1, σελ. 30.) Η επέκταση $L/\mathbb{Q}$ είναι το σώμα ανάλυσης του πολυωνύμου $(X^2-2)(X^2-3) \in \mathbb{Q}[X]$, άρα είναι κανονική (Θεώρημα 2.2.4). Είναι και διαχωρίσιμη (Θεώρημα 2.2.9), άρα, σύμφωνα με το Θεώρημα 2.2.11, οι υποομάδες της $G \overset{ορσ}{=} \mathcal{G}(L/\mathbb{Q})$ έρχονται σε 1-1 αντιστοιχία με τις ενδιάμεσες επεκτάσεις της $L/\mathbb{Q}$. Οι υποομάδες της G βρίσκονται απλούστατα: Είναι οι $\langle \mathrm{id} \rangle, \langle \sigma \rangle, \langle \tau \rangle, \langle \sigma\tau \rangle, G$. Άρα, υπάρχουν ακριβώς 5 ενδιάμεσες επεκτάσεις. Ας τις δούμε: Προφανώς $\mathcal{F}_L(\langle \mathrm{id} \rangle) = L$, διότι όλα τα στοιχεία του L παραμένουν αναλλοίωτα από τον ταυτοτικό αυτομορφισμό. Ας υπολογίσομε τώρα το $\mathcal{F}_L(\langle \sigma \rangle)$. Το τυπικό στοιχείο της L είναι $u = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}$, $a, b, c, d \in \mathbb{Q}$. Έχομε, εξ ορισμού του σ,

$$\begin{aligned} u \in \mathcal{F}_L(\langle \sigma \rangle) &\Leftrightarrow \sigma(u) = u \\ &\Leftrightarrow a - b\sqrt{2} + c\sqrt{3} - d\sqrt{2}\sqrt{3} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \\ &\Leftrightarrow b = d = 0 \\ &\Leftrightarrow u \in \mathbb{Q}(\sqrt{3}) \, . \end{aligned}$$

Με ανάλογο τρόπο αποδεικνύεται ότι $\mathcal{F}_L(\langle\tau\rangle) = \mathbb{Q}(\sqrt{2})$ και $\mathcal{F}_L(\langle\sigma\tau\rangle) = \mathbb{Q}(\sqrt{6})$ (άσκηση 5). Μία από τις συνέπειες του Θεωρήματος 2.2.11 είναι ότι $\mathcal{F}_L(G) = \mathbb{Q}$. Στο συγκεκριμένο παράδειγμα αυτό αποδεικνύεται και δίχως το Θεώρημα (βλ. άσκηση 5) και, μάλιστα, εύκολα [9]. Η αντιστοιχία μεταξύ των υποομάδων της G και των ενδιάμεσων επεκτάσεων φαίνεται πολύ καθαρά στο παρακάτω διάγραμμα:



Παράδειγμα 2. (Βλ. Παράδειγμα 2, σελ. 31.) Στην περίπτωση που η διακρίνουσα του τριτοβαθμίου πολυωνύμου $f(X)$ είναι τετράγωνο ρητού, το $L = \mathbb{Q}(\rho)$ είναι το σώμα ανάλυσης του $f(X)$ πάνω από το $\mathbb{Q}$, οπότε η $L/\mathbb{Q}$ είναι επέκταση Galois. Η ομάδα $G \overset{o\rho\sigma}{=} \mathcal{G}(L/\mathbb{Q})$ είναι ισόμορφη με την εναλλάσουσα ομάδα $\mathbf{A}_3$, οπότε έχει μόνο τις τετριμμένες υποομάδες. Αυτό σημαίνει ότι δεν υπάρχουν γνήσιες ενδιάμεσες επεκτάσεις.

Ας θεωρήσομε τώρα την περίπτωση που η διακρίνουσα του $f(X)$ δεν είναι τετράγωνο ρητού. Τότε, το σώμα ανάλυσης L του $f(X)$ πάνω από το $\mathbb{Q}$ είδαμε ότι είναι το $\mathbb{Q}(\rho, \delta) = \mathbb{Q}(\rho', \delta) = \mathbb{Q}(\rho'', \delta)$ και η $G \overset{o\rho\sigma}{=} \mathcal{G}(L/\mathbb{Q})$ είναι ισόμορφη με τη συμμετρική ομάδα $\mathbf{S}_3$. Οι υποομάδες της $\mathbf{S}_3$ είναι γνωστές: Εκτός από τις τετριμμένες, έχει και τις $\langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(2\ 3)\rangle, \langle(1\ 2\ 3)\rangle$. Έτσι, αν αριθμήσομε τις ρίζες ρ, ρ', ρ'' με 1, 2, 3, αντιστοίχως, συμπεραίνομε ότι οι υποομάδες της G είναι: $\langle\mathrm{id}\rangle, \langle(\rho\ \rho')\rangle, \langle(\rho\ \rho'')\rangle, \langle(\rho'\ \rho'')\rangle, \langle(\rho\ \rho'\ \rho'')\rangle, G$. Από τον τρόπο που ορίσαμε τους αυτομορφισμούς σ και τ, βλέπομε ότι οι μεταθέσεις $(\rho\ \rho'\ \rho'')$, $(\rho'\ \rho'')$, $(\rho\ \rho')$, $(\rho\ \rho'')$ ταυτίζονται, αντιστοίχως, με τους αυτομορφισμούς $\sigma, \tau, \sigma\tau, \sigma^2\tau$. Από το Θεώρημα 2.2.11 συμπεραίνομε τώρα ότι, εκτός των τετριμμένων ενδιάμεσων επεκτάσεων της $L/\mathbb{Q}$, υπάρχουν άλλες τέσσερις ακόμη. Ας τις δούμε: Ο τ έχομε 'δεί ότι αφήνει αναλλοίωτο το ρ και στέλνει το δ στο $-\delta$. Άρα, αν θεωρήσομε ως βάση της $L/\mathbb{Q}$ την $1, \rho, \rho^2, \delta, \delta\rho, \delta\rho^2$, γράφομε το τυπικό στοιχείο της L ως $u = a_0 + a_1\rho + a_2\rho^2 + b_0\delta + b_1\delta\rho + b_2\delta\rho^2$ και, συνεπώς,

$$\begin{aligned} u \in \mathcal{F}_L(\langle\tau\rangle) &\Leftrightarrow \tau(u) = u \\ &\Leftrightarrow a_0 + a_1\rho + a_2\rho^2 - b_0\delta - b_1\delta\rho - b_2\delta\rho^2 \\ &\quad = a_0 + a_1\rho + a_2\rho^2 + b_0\delta + b_1\delta\rho + b_2\delta\rho^2 \\ &\Leftrightarrow b_0 = b_1 = b_2 = 0 \\ &\Leftrightarrow u \in \mathbb{Q}(\rho). \end{aligned}$$

[9] Ως πρός αυτό, το συγκεκριμένο παράδειγμα αποτελεί μία ευτυχή εξαίρεση.

Συμπέρασμα:

$$\mathcal{F}_L(\langle(\rho'\ \rho')\rangle) = \mathcal{F}_L(\langle\tau\rangle) = \mathbb{Q}(\rho).$$

Επειδή ο ρόλος των ρ, ρ', ρ'' είναι συμμετρικός, ισχύουν ομοίως και οι ισότητες

$$\mathcal{F}_L(\langle(\rho\ \rho')\rangle) = \mathcal{F}_L(\langle\sigma\tau\rangle) = \mathbb{Q}(\rho''), \quad \mathcal{F}_L(\langle(\rho\ \rho'')\rangle) = \mathcal{F}_L(\langle\sigma^2\tau\rangle) = \mathbb{Q}(\rho').$$

Μία απλούστερη απόδειξη με χρήση του Θεμελιώδους Θεωρήματος της Θεωρίας Galois (Θεώρημα 2.2.12), υποδεικνύεται στην άσκηση 6.

Μένει να βρούμε το $\mathcal{F}_L(\langle\sigma\rangle)$. Αυτό μπορεί να γίνει χωρίς κανένα υπολογισμό, χάρη στο Θεώρημα 2.2.11. Πράγματι, το Θεώρημα μας λέει ότι τα στοιχεία του $\mathcal{E}$ είναι τόσα ακριβώς όσα και του $\mathcal{O}$ και, μέχρι στιγμής, τα έχομε βρεί όλα πλήν του $\mathcal{F}_L(\langle\sigma\rangle)$. Αφετέρου, το $\mathbb{Q}(\delta)$ είναι μία ενδιάμεση επέκταση, την οποία δεν έχομε ακόμη αντιστοιχήσει σε καμμία υποομάδα της G, άρα $\mathcal{F}_L(\langle\sigma\rangle) = \mathbb{Q}(\delta)$. Μπορούμε και με άμεσο τρόπο, δίχως χρήση του Θεωρήματος 2.2.11, να καταλήξομε στο ίδιο συμπέρασμα ως εξής: $u \in \mathcal{F}_L(\langle\sigma\rangle) \Leftrightarrow \sigma(u) = u$. Επειδή $\sigma(\rho) = \rho'$ και $\sigma(\delta) = \delta$, η τελευταία σχέση ισοδυναμεί, διαδοχικά, με τις εξής:

$$a_0 + a_1\rho' + a_2\rho'^2 + b_0\delta + b_1\delta\rho' + b_2\delta\rho'^2 = a_0 + a_1\rho + a_2\rho^2 + b_0\delta + b_1\delta\rho + b_2\delta\rho^2,$$

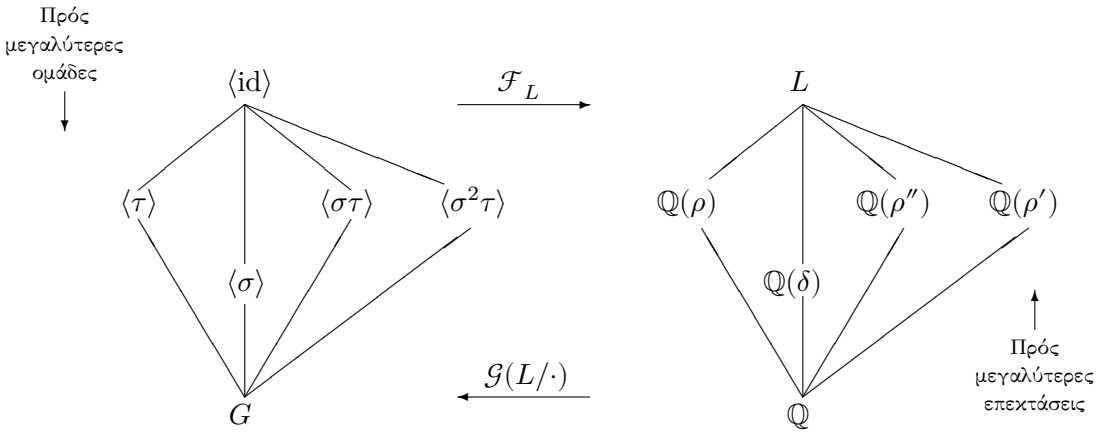
$$a_1(\rho - \rho') + a_2(\rho^2 - \rho'^2) = \delta(b_1(\rho - \rho') + b_2(\rho^2 - \rho'^2)),$$

$$a_1 + a_2(\rho + \rho') = \delta(b_1 + b_2(\rho + \rho')),$$

$$a_1 - a_2\rho'' = \delta(b_1 - b_2\rho'').$$

$$a_1 - a_2\rho'' - \delta b_1 + \delta b_2\rho'' = 0.$$

Εφαρμόζοντας τον σ στην τελευταία παίρνομε $a_1 - a_2\rho - b_1\delta + b_2\delta\rho = 0$. Τα $1, \rho, \delta, \delta\rho$ είναι $\mathbb{Q}$-γραμμικώς ανεξάρτητα, άρα $a_1 = a_2 = b_1 = b_2 = 0$, άρα $u = a_0 + b_0\delta$, δηλαδή $u \in \mathbb{Q}(\delta)$. Τώρα που έχομε την πλήρη αντιστοιχία υποομάδων της G και ενδιάμεσων επεκτάσεων της $L/\mathbb{Q}$, κατασκευάζομε το παρακάτω διάγραμμα:



Παράδειγμα 3. (Βλ. Παράδειγμα 3, σελ. 32.) Είδαμε ότι η ομάδα Galois $\mathcal{G}(L/\mathbb{Q}) \overset{ορσ}{=} G$ είναι

η $\langle \sigma, \tau \rangle$, που είναι ισόμορφη με τη διεδρική ομάδα $\mathbf{D}_4$. Οι υποομάδες της είναι,

Τάξης 1: $\langle \mathrm{id} \rangle$
Τάξης 2: $\langle \sigma^2 \rangle,\ \langle \tau \rangle,\ \langle \sigma\tau \rangle,\ \langle \sigma^2\tau \rangle,\ \langle \sigma^3\tau \rangle$
Τάξης 4: $\langle \sigma \rangle \cong \mathbb{Z}_4,\ \langle \sigma^2, \tau \rangle \cong \mathbf{V}_4,\ \langle \sigma^2, \sigma\tau \rangle \cong \mathbf{V}_4$
Τάξης 8: $G \cong \mathbf{D}_4$

Για να υπολογίσομε τις ενδιάμεσες επεκτάσεις που αντιστοιχούν στίς μη τετριμμένες υποομάδες γράφομε το τυπικό στοιχείο $u \in L$ υπό τη μορφή

$$u = a_0 + a_1\rho + a_2\rho^2 + a_3\rho^3 + b_0 i + b_1 i\rho + b_2 i\rho^2 + b_3 i\rho^3 \ ,$$

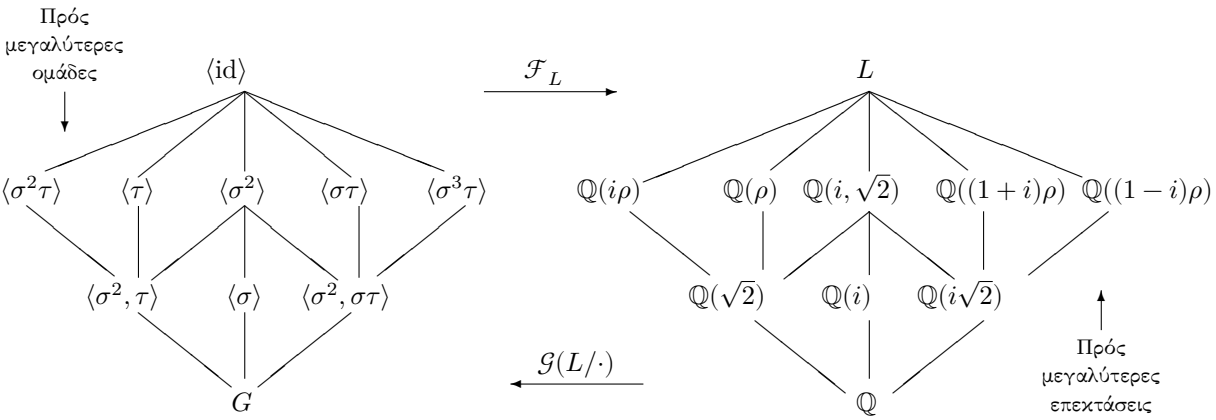
με τους συντελεστές a_i, b_i ρητούς και εξετάζομε, βοηθούμενοι και από τον πίνακα που έχομε φτιάξει, ποιές συνθήκες πρέπει να πληρούν αυτοί οι συντελεστές για να μένει αναλλοίωτο το u από διάφορους αυτομορφισμούς. Για παράδειγμα, η σχέση $\sigma^2(u) = u$ συνεπάγεται, λόγω των $\sigma^2(\rho) = -\rho$ και $\sigma^2(i) = i$, ότι $a_1 = a_3 = b_1 = b_3 = 0$. Αν, επιπλέον, θέλω και $\tau(u) = u$ τότε, λόγω των $\tau(\rho) = \rho, \tau(i) = -i$, είναι $b_0 = b_2 = 0$, οπότε $u = a_0 + a_2\rho^2 = a_0 + a_2\sqrt{2}$; έτσι, $\mathcal{F}_L(\langle \sigma^2, \tau \rangle) = \mathbb{Q}(\sqrt{2})$. Με ανάλογο τρόπο υπολογίζομε (άσκηση 7) ότι $\mathcal{F}_L(\langle \sigma^2, \sigma\tau \rangle) = \mathbb{Q}(i\sqrt{2})$ και $\mathcal{F}_L(\langle \sigma \rangle) = \mathbb{Q}(i)$. Μερικές φορές δεν είναι πολύ εύκολο να υπολογιστεί η ενδιάμεση επέκταση που αντιστοιχεί σε κάποια υποομάδα. Για παράδειγμα, ας υπολογίσομε το $\mathcal{F}_L(\langle \sigma\tau \rangle)$: Η σχέση $u = \sigma\tau(u)$ ισοδυναμεί με την

$$\begin{aligned} &a_0 + a_1\rho + a_2\rho^2 + a_3\rho^3 + b_0 i + b_1 i\rho + b_2 i\rho^2 + b_3 i\rho^3 = \\ &a_0 + a_1 i\rho - a_2\rho^2 - a_3 i\rho^3 - b_0 i + b_1(-i)i\rho - b_2 i(i\rho)^2 - b_3 i(i\rho)^3 = \\ &\quad a_0 + b_1\rho - a_2\rho^2 - b_3\rho^3 - b_0 i + a_1 i\rho + b_2 i\rho^2 - a_3 i\rho^3 \ , \end{aligned}$$

απ' όπου $a_1 = b_1,\ a_2 = -a_2,\ a_3 = -b_3,\ b_0 = -b_0$ και

$$\begin{aligned} u &= a_0 + a_1(1+i)\rho + b_2 i\rho^2 + a_3(1-i)\rho^3 \\ &= a_0 + a_1\{(1+i)\rho\} + \frac{b_2}{2}\{(1+i)\rho\}^2 - \frac{a_3}{2}\{(1+i)\rho\}^3 \ . \end{aligned}$$

Άρα $\mathcal{F}_L(\langle \sigma\tau \rangle) = \mathbb{Q}((1+i)\rho)$. Κάποια δυσκολία υπάρχει στο να υποψιαστούμε ότι $i\rho^2 = \{(1+i)\rho\}^2/2$ και $(1-i)\rho^3 = -\{(1+i)\rho\}^3/2$. Μπορούμε να διαπιστώσομε με ανάλογο τρόπο ότι $\mathcal{F}_L(\langle \sigma^3\tau \rangle) = \mathbb{Q}((1-i)\rho)$ (άσκηση 7). Απλούστερο είναι να διαπιστώσομε ότι $\mathcal{F}_L(\langle \sigma^2 \rangle) = \mathbb{Q}(i, \sqrt{2}),\ \mathcal{F}_L(\langle \sigma^2\tau \rangle) = \mathbb{Q}(i\rho)$ και $\mathcal{F}_L(\langle \tau \rangle) = \mathbb{Q}(\rho)$ (άσκηση 7). Τέλος, $\mathcal{F}_L(\langle \mathrm{id} \rangle) = G$, ενώ λόγω του Θεωρήματος 2.2.11, $\mathcal{F}_L(G) = \mathbb{Q}$. Όπως και στα προηγούμενα παραδείγματα, κατασκευάζομε το παραστατικό διάγραμμα ενδιάμεσων επεκτάσεων και υποομάδων.



Θεμελιώδες Θεώρημα της Θεωρίας Galois 2.2.12. *Έστω L/K πεπερασμένη επέκταση Galois, $\mathcal{E}$ το σύνολο των ενδιάμεσων επεκτάσεών της και $\mathcal{O}$ το σύνολο των υποομάδων της $G \overset{ορσ}{=} \mathcal{G}(L/K)$. Τότε*

1. *Υπάρχει αμφιμονοσήμαντη αντιστοιχία μεταξύ των $\mathcal{E}$ και $\mathcal{O}$, όπως περιγράφεται στο Θεώρημα 2.2.11 (αντιστοιχία Galois).*

2. *Η τάξη της G ισούται με το βαθμό της L/K : $|G| = [L : K]$.*

3. *Για κάθε ενδιάμεση επέκταση E, η επέκταση L/E είναι επέκταση Galois,*

$$[L : E] = |\mathcal{G}(L/E)| \qquad \text{και} \qquad [E : K] = \frac{|G|}{|\mathcal{G}(L/E)|} .$$

4. *Αν $E_1 < E_2$ είναι ενδιάμεσες επεκτάσεις της L/K και H_1, H_2 είναι οι αντίστοιχες (μέσω της αντιστοιχίας Galois) υποομάδες, τότε $H_1 < H_2$ και*

$$[E_2 : E_1] = [H_1 : H_2],$$

   όπου το δεξιό μέλος είναι ο δείκτης της H_2 στην H_1.

5. *Για κάθε ενδιάμεση επέκταση E, η E/K είναι Galois αν και μόνο αν η υποομάδα $\mathcal{G}(L/E)$ της G είναι κανονική. Στην περίπτωση αυτή,*

$$\mathcal{G}(E/K) \cong G/\mathcal{G}(L/E).$$

□

Ας δούμε κάποιες εφαρμογές αυτού του Θεωρήματος στά προηγούμενα παραδείγματα.

Στο παράδειγμα 2, όταν $\delta \notin \mathbb{Q}$, θα μπορούσαμε να βρούμε χωρίς κανένα υπολογισμό την επέκταση $\mathcal{F}_L(\langle\sigma\rangle)$ ως εξής: Επειδή η εναλλάσουσα ομάδα $\langle\sigma\rangle \cong \mathbf{A}_3$ είναι η μοναδική υποομάδα της συμμετρικής ομάδας $G \cong \mathbf{S}_3$ τάξης 3, έπεται από τα (1) και (3) του Θεωρήματος ότι η

ενδιάμεση επέκταση $\mathcal{F}_L(\langle\sigma\rangle)/\mathbb{Q}$ είναι η μοναδική τάξης $6:3=2$. Όμως, μία προφανής ενδιάμεση επέκταση τάξης 2 είναι η $\mathbb{Q}(\delta)/\mathbb{Q}$, άρα $\mathcal{F}_L(\langle\sigma\rangle)=\mathbb{Q}(\delta)$.

Ας δούμε πώς επαληθεύεται το Θεώρημα στο παράδειγμα 3. Οι υποομάδες $\langle\sigma^2,\tau\rangle$, $\langle\sigma\rangle$ και $\langle\sigma^2,\sigma\tau\rangle$ είναι τάξης 4, άρα έχουν δείκτη $8:4=2$ στη G. άρα, από γνωστή άσκηση της Θεωρίας Ομάδων έπεται ότι είναι κανονικές υποομάδες της G. Συνεπώς, από το (4) του Θεωρήματος, οι αντίστοιχες σε αυτές τις υποομάδες επεκτάσεις (βλ. και το σχετικό παραστατικό διάγραμμα) είναι Galois. Πράγματι, διότι είναι σώματα ανάλυσης, αντιστοίχως, των πολυωνύμων X^2-2, X^2+1 και X^2+2. Αντιθέτως, η επέκταση $\mathbb{Q}(\rho)/\mathbb{Q}$ δεν είναι κανονική (άρα, ούτε Galois) διότι, ενώ περιέχει τη ρίζα ρ του X^4-2, δεν περέχει τη ρίζα του $i\rho$. Σύμφωνα λοιπόν με το (4) του Θεωρήματος, η υποομάδα $\langle\tau\rangle$, που αντιστοιχεί στην επέκταση αυτή, δεν είναι κανονική υποομάδα της G, κάτι που διαπιστώνεται και με άμεσο τρόπο: $\sigma\langle\tau\rangle=\{\sigma,\sigma\tau\}\neq\{\sigma,\tau\sigma\}=\langle\tau\rangle\sigma$, αφού $\tau\sigma=\sigma^3\tau$. Επίσης, δεν είναι προφανές αν οι επεκτάσεις $\mathbb{Q}((1+i)\rho)$ και $\mathbb{Q}((1-i)\rho)$ είναι ή όχι κανονικές [10]. Πολύ ευκολώτερο είναι να εξετάσομε αν οι αντίστοιχες υποομάδες της G είναι ή όχι κανονικές: $\langle\sigma\tau\rangle\tau=\{\tau,(\sigma\tau)\tau\}=\{\tau,\sigma\}$ και $\tau\langle\sigma\tau\rangle=\{\tau,\tau(\sigma\tau)\}=\{\tau,(\tau\sigma)\tau\}=\{\tau,(\sigma^3\tau)\tau\}=\{\tau,\sigma^3\}$. Άρα η $\langle\sigma\tau\rangle$ δεν είναι κανονική υποομάδα της G, οπότε η επέκταση $\mathbb{Q}((1+i)\rho)$ δεν είναι κανονική; ομοίως και για την $\mathbb{Q}((1-i)\rho)$.

Όσον αφορά στην $E/\mathbb{Q}$, όπου $E=\mathbb{Q}(i,\sqrt{2})$, αυτή είναι, προφανώς, Galois ως σώμα ανάλυσης του $(X^2-2)(X^2+1)\in\mathbb{Q}[X]$. Σύμφωνα λοιπόν με το (4) του Θεωρήματος, η υποομάδα $\langle\sigma^2\rangle$ της G είναι κανονική και $\mathcal{G}(E/\mathbb{Q})\cong G/\langle\sigma^2\rangle\cong\mathbf{D}_4/\mathbb{Z}_2$. Η τελευταία ομάδα, είναι τάξης 4, αλλά όχι κυκλική, όπως διαπιστώνεται εύκολα, οπότε είναι ισόμορφη με την ομάδα του Klein $\mathbf{V}_4$. Αυτό σημαίνει ότι η $\mathcal{G}(E/\mathbb{Q})$ παράγεται από δύο αυτομορφισμούς, έστω ϕ και ψ, τέτοιους ώστε $\phi^2=\psi^2=\mathrm{id}$. Αν σκεφτούμε λίγο, λαμβάνοντας υπ' όψιν το Θεώρημα 1.4.3, βλέπομε ότι μπορούμε να πάρομε ως ϕ τον αυτομορφισμό που στέλνει την $\sqrt{2}$ στην $-\sqrt{2}$ και αφήνει αναλλοίωτο το i και ως ψ τον αυτομορφισμό που στέλνει το i στο $-i$ και αφήνει αναλλοίωτη την $\sqrt{2}$.

Ασκήσεις

1. Αν $E_1,E_2\in\mathcal{E}$ και $E_1\subseteq E_2$, τότε $\mathcal{G}(L/E_1)\supseteq\mathcal{G}(L/E_2)$. Επίσης, αν $H_1,H_2\in\mathcal{O}$ και $H_1\subseteq H_2$, τότε $\mathcal{F}_L(H_1)\supseteq\mathcal{F}_L(H_2)$.

2. Έστω σώμα K.
   (α') Αν $f(X),g(X)$ είναι *μονώνυμα* του $K[X]$ δείξτε ότι $(f+g)'=f'+g'$ και $(f\cdot g)'=f'\cdot g+g'\cdot f$.
   (β') Έστω τώρα $f(X),g(X)$ οποιαδήποτε πολυώνυμα του $K[X]$. Γράψτε το καθένα ως άθροισμα μονωνύμων (π.χ., αν $f(X)=a_nX^n+\cdots+a_1X+a_0$, τότε $f=f_n+\cdots+f_1+f_0$, όπου $f_n=a_nX^n,\ldots,f_1=a_1X$, $f_0=a_0$) και εφαρμόστε το (α') για ν' αποδείξετε ότι $(f+g)'=f'+g'$ και $(f\cdot g)'=f'\cdot g+g'\cdot f$.
   (γ') Βασιζόμενοι στο (β'), αποδείξτε επαγωγικά, ότι, για κάθε $f\in K[X]$ και κάθε ακέραιο $m\geq 2$ ισχύει $(f^m)'=m\cdot f^{m-1}\cdot f'$.

[10] Παρατηρήστε ότι, αφού κάθε αλγεβρική επέκταση του $\mathbb{Q}$ είναι διαχωρίσιμη, λόγω του Θεωρήματος 2.2.9, οι έννοιες *διαχωρίσιμη* και *κανονική* συμπίπτουν.

3. Έστω πεπερασμένη επέκταση L/K και E ενδιάμεση επέκταση. Αποδείξτε τα εξής:

   (α') Αν η L/K είναι κανονική, τότε και η L/E είναι κανονική.

   Υπόδειξη. Χρησιμοποιείστε το Θεώρημα 2.2.4.

   (β') Αν η L/K είναι διαχωρίσιμη, τότε και η L/E είναι διαχωρίσιμη.

   Υπόδειξη. Έστω οποιοδήποτε $u \in L$. Η διαχωρισιμότητα της L/K εξασφαλίζει (εξ ορισμού) ότι $\mathrm{Irr}(u, K)$ δεν έχει πολλαπλές ρίζες. Πρέπει και αρκεί να δείξετε ότι το $\mathrm{Irr}(u, E)$ δεν έχει πολλαπλές ρίζες. Χρησιμοποιείστε την άσκηση 7 της ενότητας 1.4.

   (γ') Αν η L/K είναι Galois, τότε και η L/E είναι Galois.

   Σχόλιο: Άμεση συνέπεια των (α') και (β'). Με τον τρόπο αυτό αποδεικνύεται ο πρώτος ισχυρισμός του Θεωρήματος 2.2.12 (3).

4. Αποδείξτε την πρόταση 4 του Θεωρήματος 2.2.12, βασισμένοι στην πρόταση 3 του ίδιου θεωρήματος.

5. Αναφερόμενοι στο παράδειγμα 1, αποδείξτε, δίχως να χρησιμοποιήσετε το Θεώρημα 2.2.12, ότι
$$\mathcal{F}_L(\langle\tau\rangle) = \mathbb{Q}(\sqrt{2}), \quad \mathcal{F}_L(\langle\sigma\tau\rangle) = \mathbb{Q}(\sqrt{6}), \quad \mathcal{F}_L(G) = \mathbb{Q}.$$

6. Αναφερόμενοι στο παράδειγμα 2, αποδείξτε ότι $\mathcal{F}_L(\langle\sigma\tau\rangle) = \mathbb{Q}(\rho'')$ ως εξής: Παρατηρήστε ότι η σχέση αυτή ισοδυναμεί με την $\mathcal{G}(L/\mathbb{Q}(\rho'')) = \langle\sigma\tau\rangle$, οπότε αρκεί να δείξετε αυτή την τελευταία, κάτι αρκετά απλό, αν κάνετε χρήση του θεωρήματος 2.2.12. Ανάλογα, δείξτε ότι $\mathcal{F}_L(\langle\sigma^2\tau\rangle) = \mathbb{Q}(\rho')$.

7. Αναφερόμενοι στο παράδειγμα 3, αποδείξτε ότι
$$\begin{aligned} \mathcal{F}_L(\langle\sigma^3\tau\rangle) &= \mathbb{Q}((1-i)\rho) \\ \mathcal{F}_L(\langle\sigma^2\rangle) &= \mathbb{Q}(i, \sqrt{2}) \\ \mathcal{F}_L(\langle\sigma^2\tau\rangle) &= \mathbb{Q}(i\rho) \\ \mathcal{F}_L(\langle\tau\rangle) &= \mathbb{Q}(\rho). \end{aligned}$$
   Αποδείξτε, επίσης, ότι τα $(1+i)\rho$ και $(1-i)\rho$ είναι ρίζες του X^4+8, το οποίο είναι ανάγωγο πάνω από το $\mathbb{Q}$.

8. Αποδείξτε ότι οι ρίζες του $f(X) = X^4 - X^2 + 1 \in \mathbb{Q}[X]$ είναι οι διάφορες των $\pm i$ έκτες ρίζες του -1. Θεωρήστε δεδομένο ότι το f είναι ανάγωγο πάνω από το $\mathbb{Q}$ και υπολογίστε το σώμα ανάλυσης L και την ομάδα Galois G του f. Τέλος, αντιστοιχήστε τις υποομάδες της G με τις ενδιάμεσες επεκτάσεις της $L/\mathbb{Q}$.

   Υπόδειξη-μερική απάντηση: Οι έκτες ρίζες του -1 είναι, προφανώς, όλες οι ρίζες του X^6+1. Παραγοντοποιήστε αυτό το πολυώνυμο χρησιμοποιώντας την παραγοντοποίηση του X^3+1. Δείξτε ότι, αν ρ είναι μια ρίζα του f (δεν χρειάζεται να την υπολογίσετε), τότε οι υπόλοιπες τρεις ρίζες του f εκφράζονται πολύ απλά συναρτήσει της ρ, οπότε $L = \mathbb{Q}(\rho)$.

Όσον αφορά στη G: Είναι ισόμορφη με την V_4 (ομάδα Klein). Αυτό σημαίνει ότι θα βρείτε δύο $\mathbb{Q}$-αυτομορφισμούς σ και τ του L που έχουν την ιδιότητα $\sigma^2 = \mathrm{id} = \tau^2$ και $\sigma\tau = \tau\sigma$.

9. Έστω $\rho = \sqrt[3]{\dfrac{1+\sqrt{5}}{2}}$. Αποδείξτε ότι το ρ είναι ρίζα του $f(X) = X^6 - X^3 - 1 \in \mathbb{Q}[X]$. Θεωρήστε δεδομένο ότι το $f(X)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$ και αποδείξτε τα παρακάτω:

(α') Όλες οι ρίζες του $f(X)$ είναι $\rho, \omega\rho, \omega^2\rho, -1/\rho, -\omega/\rho, -\omega^2/\rho$, όπου ω είναι κυβική ρίζα της μονάδας, $\omega \neq 1$ (άρα $\omega^2 + \omega + 1 = 0$). Συμπεράνατε ότι $L = \mathbb{Q}(\rho, \omega)$ είναι σώμα ανάλυσης του $f(X)$ πάνω από το $\mathbb{Q}$ και συμβολίστε $G = \mathcal{G}(L/\mathbb{Q})$.

(β') Δείξτε ότι υπάρχουν αυτομορφισμοί $\sigma, \tau \in \mathcal{G}(L/\mathbb{Q})$ που δρουν ως εξής: $\sigma(\rho) = -\omega/\rho, \sigma(\omega) = \omega^2$, $\tau(\rho) = \rho, \tau(\omega) = \omega^2$. Μετά, αποδείξτε ότι οι τάξεις των σ, τ είναι 6 και 2, αντιστοίχως, και $\tau\sigma = \sigma^5\tau$, άρα, $G \cong D_6$. Υπενθυμίζεται ότι τα στοιχεία της D_6 είναι $\{\mathrm{id}, \sigma, \dots, \sigma^5, \tau, \sigma\tau, \dots, \sigma^5\tau\}$. Για τις πράξεις στην ομάδα D_6, χρήσιμη είναι η σχέση (αποδείξτε την, είναι απλή) $\tau\sigma^k = \sigma^{6-k}\tau = \sigma^{-k}\tau$. Επίσης, συμπληρώστε ένα πίνακα που θα δείχνει τη δράση καθενός απ' τους 12 αυτομορφισμούς της G στα ρ και ω.

(γ') Στον πίνακα 2.1 φαίνονται όλες οι ενδιάμεσες επεκτάσεις E της $L/\mathbb{Q}$, με $E \neq \mathbb{Q}, L$. Ένας ή δύο γεννήτορες δίδονται για κάθε επέκταση E και ζητούνται τα εξής:
(i) Για κάθε E αποδείξτε ότι $\mathcal{G}(L/E)$ είναι η υποομάδα της G που εμφανίζεται στην ίδια γραμμή με την E. Επίσης, αποδείξτε ότι η $\mathcal{G}(L/E)$ είναι κανονική υποομάδα της G αν δίπλα στην $\mathcal{G}(L/E)$ υπάρχει η ένδειξη «ναί», ενώ δεν είναι κανονική υποομάδα αν υπάρχει η ένδειξη «όχι».
(ii) Βρείτε τον βαθμό $[E : \mathbb{Q}]$ για κάθε E. Για τις τρεις πρώτες E, ο βαθμός είναι προφανής, αλλά για όλες τις επόμενες, να τον υπολογίσετε χωρίς να χρησιμοποιήσετε την πληροφορία της στήλης «ελάχιστα πολυώνυμα γεννητόρων». Αυτό θα το πετύχετε εύκολα υπολογίζοντας την $|\mathcal{G}(L/E)|$ και κάνοντας χρήση του *Θεμελιώδους Θεωρήματος της Θεωρίας Galois*.
(iii) Στις (πέντε) περιπτώσεις, που $\mathcal{G}(L/E) \lhd G$, υπολογίστε τα στοιχεία (αριστερές κλάσεις) της ομάδας-πηλίκο $\mathcal{G}(L/\mathbb{Q})/\mathcal{G}(L/E)$. Αποδείξτε ότι, στις τρεις πρώτες περιπτώσεις, αυτή η ομάδα είναι ισόμορφη με την $\mathbb{Z}_2$, ενώ στην τέταρτη και πέμπτη περίπτωση (από τις προαναφερθείσες πέντε περιπτώσεις, δηλαδή, στις E της $7^{\eta\varsigma}$ και $8^{\eta\varsigma}$ γραμμής) οι ομάδες-πηλίκα είναι ισόμορφες με τις V_4 (*ομάδα των τεσσάρων του Klein*, η οποία είναι ισόμορφη με την $\mathbb{Z}_2 \times \mathbb{Z}_2$) και D_3, αντιστοίχως. Τί συμπεράσματα βγάζετε για την ομάδα Galois $\mathcal{G}(E/\mathbb{Q})$ κάθε μιας από τις πέντε επεκτάσεις $E/\mathbb{Q}$; Προσοχή! Μέχρι λίγο πρίν κάναμε λόγο για ομάδες $\mathcal{G}(L/E)$, άρα για υποομάδες αυτομορφισμών του L, ενώ τώρα αναφερόμαστε σε ομάδες $\mathcal{G}(E/\mathbb{Q})$, άρα σε υποομάδες αυτομορφισμών του E.
Υπόδειξη: Από το Θεμελιώδες Θεώρημα, $\mathcal{G}(E/\mathbb{Q}) \cong G/\mathcal{G}(L/E)$. Άρα, αν, για παράδειγμα, $\mathcal{G}(L/E) \lhd G$ και $G/\mathcal{G}(L/E) \cong \mathbb{Z}_2$, η απάντησή σας πρέπει να είναι ότι, οι μόνοι $\mathbb{Q}$-αυτομορφισμοί του σώματος E είναι ο ταυτοτικός και άλλος ένας, έστω ϕ, τέτοιος ώστε $\phi^2 = \mathrm{id}_E$.

Πίνακας 2.1: Όλες οι ενδιάμεσες επεκτάσεις $\mathbb{Q} \subsetneqq E \subsetneqq L$.

Γεννήτορες της E	ελάχιστα πολυώνυμα γεννητόρων	$\mathcal{G}(L/E)$	$\mathcal{G}(L/E) \lhd G$;
$\sqrt{-15} = (2\rho^3 - 1)(2\omega + 1)$	$X^2 + 15$	$\langle \sigma \rangle$	Ναί
$\sqrt{5} = 2\rho^3 - 1$	$X^2 - 5$	$\langle \sigma^2, \tau \rangle$	Ναί
ω	$X^2 + X + 1$	$\langle \sigma^2, \sigma\tau \rangle$	Ναί
$\theta_1 = 1 - \rho^2 + \omega(-\rho - \rho^2 + \rho^4)$	$X^3 - 3X^2 - 1$	$\langle \sigma^3, \sigma\tau \rangle$	Όχι
$\theta_2 = 1 + \rho - \rho^4 + \omega(\rho + \rho^2 - \rho^4)$	$X^3 - 3X^2 - 1$	$\langle \sigma^3, \sigma^2\tau \rangle$	Όχι
$\theta_3 = 1 - \rho + \rho^2 + \rho^4$	$X^3 - 3X^2 - 1$	$\langle \sigma^3, \sigma^3\tau \rangle$	Όχι
$\xi = 3 + \rho^3 + 6\omega$	$X^4 - 2X^3 + 53X^2 - 52X + 811$	$\langle \sigma^2 \rangle$	Ναί
$\sqrt{-15},\ \theta_1$		$\langle \sigma^3 \rangle$	Ναί
$\sqrt{5},\ \theta_1$		$\langle \sigma^4\tau \rangle$	Όχι
$\omega,\ \theta_1$		$\langle \sigma\tau \rangle$	Όχι
$\sqrt{5},\ \theta_2$		$\langle \sigma^2\tau \rangle$	Όχι
$\omega,\ \theta_2$		$\langle \sigma^5\tau \rangle$	Όχι
$\sqrt{5},\ \theta_3$		$\langle \tau \rangle$	Όχι
$\omega,\ \theta_3$		$\langle \sigma^3\tau \rangle$	Όχι

2.3 Τρεις εφαρμογές

Οι τρεις εφαρμογές αυτής της ενότητας είναι τα Θεωρήματα 2.3.2, 2.3.3 και 2.3.4. Μια σημαντική πρόταση που θα χρησιμοποιήσομε είναι η επόμενη.

Πρόταση 2.3.1. *Για κάθε πεπερασμένη επέκταση L/K υπάρχει πεπερασμένη επέκταση N του L με την N/K κανονική.*

Απόδειξη. Υπάρχει πεπερασμένο πλήθος στοιχείων $\alpha, \beta, \gamma, ...$ της L ώστε $L = K(\alpha, \beta, \gamma, ...)$ (π.χ. πάρετε για $\alpha, \beta, \gamma, ...$ μια βάση της L/K). Έστω ότι τα ελάχιστα πολυώνυμα αυτών των στοιχείων πάνω από το K είναι $f_\alpha, f_\beta, f_\gamma, ...$, αντιστοίχως και f το γινόμενό τους. Έστω N το σώμα ανάλυσης του f πάνω από το L. Τότε $N = L(A \cup B \cup C \cup ...)$, όπου $A, B, C, ...$ είναι τα σύνολα ριζών των $f_\alpha, f_\beta, f_\gamma, ...$ αντιστοίχως. Προφανώς $\alpha \in A$, $\beta \in B$, $\gamma \in C$, κλπ, άρα $N = K(\alpha, \beta, \gamma, ...)(A \cup B \cup C \cup ...) = K(A \cup B \cup C \cup ...)$. Αυτή η σχέση μας λέει ότι το N είναι σώμα ανάλυσης του f πάνω από το K, άρα η επέκταση N/K είναι κανονική βάσει του Θεωρήματος 2.2.4. □

Θεώρημα 2.3.2. *Αν το K είναι σώμα χαρακτηριστικής 0, τότε κάθε πεπερασμένη επέκταση L/K είναι απλή, δηλαδή, υπάρχει $u \in L$ ώστε $L = K(u)$.*

Απόδειξη. Το K είναι άπειρο σώμα διότι η χαρακτηριστική του είναι 0 0[11] και L πεπερασμένη επέκταση του K. Έστω N/L πεπερασμένη επέκταση του L με την N/K κανονική, της οποίας η ύπαρξη εξασφαλίζεται από την Πρόταση 2.3.1. Από το Θεώρημα 2.2.9, η επέκταση N/K είναι διαχωρίσιμη, άρα η N/K είναι Galois (Ορισμός 2.2.2).

Από το Θεώρημα 2.2.12 ξέρομε ότι $|\mathcal{G}(N/K)| = [N : K]$, άρα η ομάδα $\mathcal{G}(N/K)$ είναι πεπερασμένη. Έπεται ότι το πλήθος των υποομάδων της είναι πεπερασμένο άρα, από το (1) του ίδιου Θεωρήματος, και το πλήθος των ενδιαμέσων επεκτάσεων της N/K είναι πεπερασμένο. Αλλά τότε, το ίδιο συμβαίνει και με τη μικρότερη επέκταση L/K. Χρησιμοποιήσαμε τη βοηθητική επέκταση N για ν' αποδείξομε ότι το πλήθος των ενδιαμέσων επεκτάσεων της L/K είναι πεπερασμένο και, στο εξής, ξεχνάμε την N.

Θεωρούμε το σύνολο $\mathcal{S}$ των απλών ενδιάμεσων επεκτάσεων της L/K· πρόκειται για μη κενό σύνολο (η τετριμμένη επέκταση K/K είναι απλή, αφού $K = K(1)$) το οποίο, επιπλέον, είναι και πεπερασμένο, βάσει του συμπεράσματος της αμέσως προηγούμενης παραγράφου. Έστω, λοιπόν, ένα maximal στοιχείο αυτού του συνόλου, δηλαδή, μία απλή ενδιάμεση επέκταση $K(u)$, η οποία δεν περιέχεται *γνησίως* σε καμμία ενδιάμεση απλή επέκταση της L/K. Για κάθε $(a, v) \in K \times L$ είναι $K(au + v) \in \mathcal{S}$. Θα δείξομε τώρα ότι κάθε $v \in L$ ανήκει στο $K(u)$, συμπεραίνοντας έτσι ότι $L = K(u)$. Πράγματι, έστω τυχόν $v \in L$. Αφού το K περιέχει άπειρα στοιχεία, το

[11] Τα $n \cdot 1_K$, $n = 1, 2, 3, ...$ είναι άπειρα στοιχεία του K.

σύνολο $\{au+v \,:\, a \in K\}$ είναι άπειρο. Από την άλλη, το πλήθος των απλών ενδιαμέσων επεκτάσεων $K(au+v)$ είναι πεπερασμένο, άρα υπάρχουν $a, b \in K$, $a \neq b$, ώστε $K(au+v) = K(bu+v)$ (αρχή του περιστερώνα). Ειδικότερα, αυτό συνεπάγεται ότι $bu+v \in K(au+v)$, οπότε $(bu+v)-(au+v) \in K(au+v)$, άρα $(b-a)u \in K(au+v)$ και, τελικά, $u \in K(au+v)$. Συνεπώς, $K(u) \subseteq K(au+v)$ και τότε η maximal ιδιότητα του $K(u)$ συνεπάγεται ότι $K(u) = K(au+v)$, άρα $au+v \in K(u)$. Όμως $au \in K(u)$, άρα $v \in K(u)$. □

Θεώρημα 2.3.3. *Έστω p περιττός πρώτος. Το κανονικό p-γωνο κατασκευάζεται με κανόνα και διαβήτη αν, και μόνο αν, ο p είναι πρώτος του Fermat, δηλαδή της μορφής $2^{2^n}+1$.*

Απόδειξη. Μία πρώτη παρατήρηση είναι ότι αν ο $p = 2^k+1$ είναι πρώτος, τότε ο k είναι δύναμη του 2. Γιατί, στην αντίθετη περίπτωση, ο k έχει κάποιο περιττό διαιρέτη d οπότε, θέτοντας $k = dm$ έχομε $p = (2^m)^d+1 = (2^m+1)(2^{m(d-1)} - 2^{m(d-2)} + \cdots - 2^m + 1)$; αντίφαση με το ότι ο p είναι πρώτος. Συνεπώς, αρκεί να αποδείξομε ότι το κανονικό p-γωνο κατασκευάζεται αν, και μόνο αν, ο p είναι της μορφής 2^k+1.

Πρίν προχωρήσομε στην κυρίως απόδειξη θέτομε

$$\theta = \frac{2\pi}{p}\,,\ \zeta = \cos\theta + i\sin\theta\,,\ L = \mathbb{Q}(\zeta)\,,\ E = \mathbb{Q}(\cos\theta).$$

Το ζ είναι p-τάξεως ρίζα της μονάδος και, από την πρόταση Γ'.6 (παράρτημα Γ'), έχει ελάχιστο πολυώνυμο το *κυκλοτομικό πολυώνυμο*

$$f_p(X) = \frac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + \cdots + X + 1,$$

του οποίου οι ρίζες είναι: $\zeta, \zeta^2, \ldots, \zeta^{p-1}$. Έπεται, ειδικότερα, ότι

$$[L : \mathbb{Q}] = p-1$$

Είναι $\cos\theta = \frac{1}{2}(\zeta + \zeta^{-1})$, άρα $\zeta^2 - (2\cos\theta)\zeta - 1 = 0$, συνεπώς ζ, ζ^{-1} είναι οι ρίζες του $X^2 - (2\cos\theta)X - 1 \in E[X]$ και είναι μη πραγματικές, συνεπώς δεν ανήκουν στο $E \subset \mathbb{R}$. Αυτό συνεπάγεται ότι αυτό το δευτεροβάθμιο πολυώνυμο είναι ανάγωγο πάνω από το E, συνεπώς

$$[L : E] = 2,\ \text{άρα}\ [E : \mathbb{Q}] = \tfrac{1}{2}(p-1).$$

Έστω, πρώτα, ότι το κανονικό p-γωνο κατασκευάζεται. Τότε ο αριθμός $\cos\theta$ κατασκευάζεται άρα, από το Θεώρημα 1.2.2, $[E : \mathbb{Q}] = 2^n$ για κάποιο μη αρνητικό ακέραιο n. Τότε, από τις παραπάνω σχέσεις, $\frac{1}{2}(p-1) = 2^n$, άρα $p = 2^{n+1}+1$.

Αντιστρόφως, έστω $p = 2^k+1$. Θα δείξομε ότι ο αριθμός $\cos\theta$ κατασκευάζεται με κανόνα και διαβήτη. Από τη στοιχειώδη Ευκλείδειο Γεωμετρία ξέρομε να κατασκευάζομε με κανόνα και διαβήτη τις ρίζες οποιασδήποτε δευτεροβάθμιας εξίσωσης, της οποίας οι συντελεστές είναι κατασκευάσιμα μήκη. Αν λοιπόν καταφέρομε να δείξομε ότι υπάρχει μία πεπερασμένη αλυσσίδα

διαδοχικών επεκτάσεων

$$\mathbb{Q} = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_l = E\ , \tag{2.2}$$

έτσι ώστε κάθε $[E_{j+1} : E_j] = 2$, τότε θα έχομε την εξής κατάσταση: Τα στοιχεία του E_1 θα είναι κατασκευάσιμα, ως ρίζες δευτεροβαθμίων πολυωνύμων με συντελεστές από το $\mathbb{Q}$. Μετά, τα στοιχεία του E_2 είναι κατασκευάσιμα, ως ρίζες δευτεροβαθμίων πολυωνύμων με συντελεστές από το E_1 κ.ο.κ., μέχρις ότου καταλήξομε στην κατασκευασιμότητα των στοιχείων του E_l, άρα και του $\cos\theta$. Μένει λοιπόν να αποδείξομε την ύπαρξη μιας αλυσσίδος επεκτάσεων (2.2) με τις προαναφερθείσες ιδιότητες.

Το L είναι σώμα ανάλυσης του f_p πάνω απ' το $\mathbb{Q}$, άρα η επέκταση $L/\mathbb{Q}$ είναι Galois. Η ομάδα Galois $\mathcal{G}(L/\mathbb{Q})$ είναι ισόμορφη με την $\mathbb{Z}_p^*$ (πολλαπλασιαστική ομάδα των μη μηδενικών κλάσεων υπολοίπων mod p)· βλ. πρόταση (α') στην ενότητα 2.4.1. Ειδικότερα, η $\mathcal{G}(L/\mathbb{Q})$ είναι κυκλική, τάξεως $p-1 = 2^k$, άρα η $\mathcal{G}(L/E)$, είναι κανονική υποομάδα της. Τότε, το (4) του Θεωρήματος 2.2.12, εφαρμοζόμενο στην ενδιάμεση επέκταση E της $L/\mathbb{Q}$ μας δίνει ότι η επέκταση $E/\mathbb{Q}$ είναι Galois, άρα, από το (1) του ίδιου θεωρήματος (εφαρμοζόμενο στην επέκταση $E/\mathbb{Q}$), $|\mathcal{G}(E/\mathbb{Q})| = [E : \mathbb{Q}] = \frac{1}{2}(p-1) = 2^{k-1} = 2^l$, όπου θέσαμε $l = k-1$ για απλούστευση του συμβολισμού. Από το (4) του Θεωρήματος 2.2.12, η ομάδα $\mathcal{G}(E/\mathbb{Q})$ είναι ισόμορφη με μία ομάδα-πηλίκο της κυκλικής ομάδας $\mathcal{G}(L/\mathbb{Q})$, άρα είναι κυκλική, τάξεως 2^l. Από το (γ') της ενότητας 2.4.1, συμπεραίνομε τότε ότι υπάρχει μία αλυσσίδα υποομάδων

$$G_l = \langle \mathrm{id} \rangle \lhd G_{l-1} \lhd G_{l-2} \lhd \cdots \lhd G_0 = G,$$

με $|G_j| = 2^{l-j}$ για κάθε $j = 0, 1, \ldots, l$.

Αφετέρου, το Θεώρημα 2.2.12, λέει ότι σε αυτή την αλυσσίδα υποομάδων αντιστοιχεί η αλυσσίδα των ενδιαμέσων επεκτάσεων

$$E = E_l \supseteq E_{l-1} \supseteq E_{l-2} \supseteq \cdots \supseteq E_0 = \mathbb{Q},$$

όπου, βεβαίως, $\mathcal{G}(E/E_j) = G_j$ για κάθε $j = 0, 1, \ldots, l$. Θα δείξομε ότι, για κάθε $j = 0, 1, \ldots, l-1$, ισχύει $[E_{j+1} : E_j] = 2$. Εφαρμόζομε το Θεώρημα 2.2.12 στην επέκταση $E/\mathbb{Q}$.

$$\begin{array}{lcl}
E = E_l & E \longleftrightarrow G_l & G_l = \langle \mathrm{id} \rangle \\
 & \vdots \quad\quad \vdots & \\
 & E_{j+1} \longleftrightarrow G_{j+1} & |G_{j+1}| = 2^{l-(j+1)} \\
 & \vdots \quad\quad \vdots & \\
 & E_j \longleftrightarrow G_j & |G_j| = 2^{l-j} \\
 & \vdots \quad\quad \vdots & \\
\mathbb{Q} = E_0 & \mathbb{Q} \longleftrightarrow G_0 & G_0 = \mathcal{G}(E/\mathbb{Q})
\end{array}$$

Από το (3) του Θεωρήματος 2.2.12 συμπεραίνομε ότι $[E : E_j] = |\mathcal{G}(E/E_j)| = |G_j| = 2^{l-j}$ και, ομοίως, $[E : E_{j+1}] = 2^{l-(j+1)}$. Άρα, $[E_{j+1} : E_j] = [E : E_j]/[E : E_{j+1}] = 2$. □

Ως τρίτη εφαρμογή της Θεωρίας Galois θα αποδείξομε το θεώρημα που, κατά παράδοση, ονομάζεται *Θεμελιώδες Θεώρημα της Άλγεβρας*.

Θεμελιώδες Θεώρημα της Άλγεβρας 2.3.4. *Κάθε μη σταθερό πολυώνυμο με μιγαδικούς συντελεστές έχει ρίζα στο* $\mathbb{C}$*, συνεπώς αναλύεται σε πρωτοβάθμιους παράγοντες του* $\mathbb{C}[X]$.

Για την απόδειξη αυτού του θεωρήματος (γίνεται στη σελίδα 52) θα χρησιμοποιήσομε τρεις προτάσεις και ένα κλασσικό θεώρημα της Θεωρίας Ομάδων (αναπόδεικτο σ' αυτές τις σημειώσεις).

Πρόταση 2.3.5. *Κάθε δευτεροβάθμιο πολυώνυμο του* $\mathbb{C}[X]$ *έχει τις ρίζες του στο* $\mathbb{C}$*. Επομένως, δεν υπάρχει επέκταση του* $\mathbb{C}$ *βαθμού* 2.

Απόδειξη. Αρκεί να αποδείξομε ότι κάθε μιγαδικός αριθμός $a+bi$, $a, b \in \mathbb{R}$ έχει τετραγωνικές ρίζες μέσα στο $\mathbb{C}$, δηλαδή, υπάρχουν $x, y \in \mathbb{R}$ που επαληθεύουν τη σχέση $(x+yi)^2 = a+bi$. Αυτή η σχέση ισοδυναμεί με το σύστημα

$$x^2 - y^2 = a, \quad 2xy = b,$$

το οποίο πρέπει ν' αποδείξομε ότι έχει πραγματική λύση (x, y). Όταν $b = 0$, η λύση είναι $(x, y) = (\sqrt{a}, 0)$ αν $a \geq 0$ και $(x, y) = (0, \sqrt{a})$ αν $a < 0$, οπότε υποθέτομε ότι $b \neq 0$. Θέτομε $y = rx$ και αντικαθιστούμε στις παραπάνω δύο εξισώσεις, οπότε παίρνομε

$$x^2(1 - r^2) = a, \quad 2rx^2 = b. \tag{2.3}$$

Διαιρώντας κατά μέλη: $(1-r^2)/(2r) = a/b$, άρα $br^2+2ar-b = 0$. Λύνοντας ως προς r, παίρνομε $r = (-a \pm \sqrt{a^2+b^2})/b$. Για να είναι ο x πραγματικός αριθμός στη δεύτερη σχέση (2.3) πρέπει και αρκεί οι r, b να είναι ομόσημοι. Επομένως στην τελευταία έκφραση του r επιλέγομε το πρόσημο $+$ και τότε

$$x = \sqrt{\frac{b^2}{2(-a + \sqrt{a^2+b^2})}} \in \mathbb{R}$$

οπότε και $y = rx \in \mathbb{R}$. □

Στις επόμενες δύο προτάσεις θα γίνει χρήση ενός σημαντικού θεωρήματος της Θεωρίας Ομάδων. Πρόκειται για το *Πρώτο Θεώρημα του Sylow*, το οποίο θα χρησιμοποιήσομε υπό την εξής μορφή:

Θεώρημα (Πρώτο Θεώρημα Sylow)**.** *Αν η πεπερασμένη ομάδα* G *έχει τάξη* $p^n m$*, όπου ο* p *είναι πρώτος,* $n \geq 1$ *και* $p \nmid m$*, τότε, για κάθε* $k = 1, \ldots, n$ *υπάρχει υποομάδα της* G *τάξεως* p^k.

Πρόταση 2.3.6. *Δεν υπάρχει γνήσια πεπερασμένη επέκταση του* $\mathbb{R}$ *περιττού βαθμού.*

Απόδειξη. Έστω πεπερασμένη επέκταση K/R με $[K:\mathbb{R}] = n > 1$ περιττό. Από το Θεώρημα 2.3.2 είναι $K = \mathbb{R}(u)$ για κατάλληλο $u \in K$. Αν $f = \mathrm{Irr}(u, K)$, τότε $n = [K:\mathbb{R}] = \deg f$, άρα το f είναι πολυώνυμο περιττού βαθμού, οπότε, από το *Θεώρημα Ενδιάμεσης Τιμής* του Απειροστικού Λογισμού, έχει πραγματική ρίζα. Αυτό, όμως, συνεπάγεται ότι το f δεν είναι ανάγωγο· άτοπο. □

Πρόταση 2.3.7. *Κάθε πεπερασμένη γνήσια επέκταση του* $\mathbb{R}$ *έχει βαθμό δύναμη του* 2.

Απόδειξη. Έστω πεπερασμένη $L/\mathbb{R}$. Από την Πρόταση 2.3.1 υπάρχει πεπερασμένη επέκταση N/L με την $N/\mathbb{R}$ κανονική και επειδή αυτή η επέκταση είναι και διαχωρίσιμη (αφού η χαρακτηριστική του $\mathbb{R}$ είναι 0), η N/R είναι Galois. Επομένως, δίχως βλάβη της γενικότητας μπορούμε να υποθέσομε ότι η $L/\mathbb{R}$ είναι Galois. Έστω $[L:\mathbb{R}] = 2^n m$, όπου $m \geq 1$ περιττός και $n \geq 1$ λόγω της Πρότασης 2.3.6. Έστω $G = \mathcal{G}(L/\mathbb{R})$. Από το Θεώρημα 2.2.12 είναι $|G| = [L:\mathbb{R}] = 2^n m$ και από το Θεώρημα του Sylow υπάρχει $H < G$ τάξεως 2^n. Έστω E η ενδιάμεση επέκταση της $L/\mathbb{R}$ που αντιστοιχεί στην H μέσω της αντιστοιχίας Galois ($E = \mathcal{F}_L(H)$ και $\mathcal{G}(L/E) = H$). Από το Θεώρημα 2.2.12 (3) είναι $[E:\mathbb{R}] = |G|/|H| = m$. Επειδή ο m είναι περιττός, πρέπει υποχρεωτικά να είναι ίσος με 1 λόγω της Πρότασης 2.3.6, άρα $[L:\mathbb{R}] = 2^n$. □

Απόδειξη του Θεωρήματος 2.3.4. Έστω ότι υπάρχει πολυώνυμο με μιγαδικούς συντελεστές που δεν έχει όλες τις ρίζες του στο $\mathbb{C}$. Αυτό σημαίνει ότι υπάρχει ανάγωγο $f \in \mathbb{C}[X]$ με $\deg f > 1$, οπότε υπάρχει επέκταση του $L/\mathbb{C}$ με $[L:\mathbb{C}] = \deg f > 1$ (Θεώρημα 1.1.3). Η $L/\mathbb{R}$ είναι προφανώς πεπερασμένη και, όπως στην απόδειξη της Πρότασης 2.3.7, μπορούμε να θεωρήσομε ότι είναι Galois, οπότε και η $L/\mathbb{C}$ είναι Galois. Είναι $\mathbb{C} = \mathbb{R}(i)$ και το i είναι ρίζα του ανάγωγου $X^2 + 1 \in \mathbb{R}[X]$, άρα $[L:\mathbb{R}] = 2[L:\mathbb{C}]$ και τότε, από την Πρόταση 2.3.7 έπεται ότι $[L:\mathbb{C}]$ είναι δύναμη του 2, έστω $[L:\mathbb{C}] = 2^n$. Επιπλέον, $n > 1$ λόγω της Πρότασης 2.3.5. Έστω $G = \mathcal{G}(L/\mathbb{C})$. Από το Θεώρημα 2.2.12 είναι $|G| = [L:\mathbb{C}] = 2^n$ και το Θεώρημα Sylow μας εξασφαλίζει την ύπαρξη $H < G$ τάξεως 2^{n-1}. Έστω E η ενδιάμεση επέκταση της $L/\mathbb{C}$ που αντιστοιχεί στην H μέσω της αντιστοιχίας Galois ($E = \mathcal{F}_L(H)$ και $\mathcal{G}(L/E) = H$). Από το Θεώρημα 2.2.12 (3) είναι $[E:\mathbb{C}] = |G|/|H| = 2^n/2^{n-1} = 2$, συμπέρασμα που αντιφάσκει στην Πρόταση 2.3.5. □

Ασκήσεις

1. *Ορισμός. Ένα σώμα χαρακτηρίζεται αλγεβρικά κλειστό, αν δεν έχει γνήσια αλγεβρική επέκταση.*

   (α') Αποδείξτε ότι το $\mathbb{C}$ είναι αλγεβρικά κλειστό σώμα.

   (β') Αποδείξτε ότι το υπόσωμα $\mathbb{A}$ του $\mathbb{C}$ που αποτελείται από όλους τους αλγεβρικούς (μιγαδικούς) αριθμούς είναι αλγεβρικά κλειστό.

2. Αν $a, b \in \mathbb{R}$ και $b \neq 0$, δείξτε ότι $\mathbb{R}(a + bi) = \mathbb{C}$.

   Υπόδειξη. Δείξτε πρώτα ότι $a - bi \in \mathbb{R}(a + bi)$. Ύστερα, $\mathbb{R}(i) \subseteq \mathbb{R}(a + bi)$. Τέλος, εφαρμόστε την άσκηση 1 (α').

3. Αποδείξτε ότι κάθε γνήσια αλγεβρική επέκταση του $\mathbb{R}$ (δεν υποθέτομε ότι είναι πεπερασμένη) είναι ισόμορφη με το $\mathbb{C}$.

   Υπόδειξη. Έστω $K/\mathbb{R}$ γνήσια αλγεβρική επέκταση, $u \in K \setminus \mathbb{R}$ και $f = \mathrm{Irr}(u, \mathbb{R})$. Από το Θεώρημα 2.3.4, το f έχει ρίζα, έστω $z \in \mathbb{C}$. Με τη βοήθεια του Θεωρήματος 1.4.3 δείξτε ότι $\mathbb{R}(u) \cong \mathbb{R}(z)$. Χρησιμοποιείστε μετά τις ασκήσεις 2 και 1 (α').

2.4 Επιλυση πολυωνυμικων εξισωσεων με ριζικα

Έστω $f(X) \in \mathbb{Q}[X]$. Θέλομε να βρούμε αναγκαίες συνθήκες για να εκφράζονται οι λύσεις της $f(x) = 0$ με ριζικά, ή, όπως θα λέμε για συντομία, να είναι το $f(X)$ *επιλύσιμο με ριζικά*.[12] Αυτό σημαίνει ότι όλες οι ρίζες του $f(X)$ θα μοιάζουν, για παράδειγμα, με κάτι σάν την παρακάτω έκφραση:

$$\sqrt[3]{q}\sqrt[5]{\frac{r+\sqrt{s}}{t}} + \sqrt[4]{u+\sqrt[3]{v}}\,,$$

όπου $q, r, s, t, u, v \in \mathbb{Q}$. Γενικά, όταν το $f(X)$ είναι επιλύσιμο με ριζικά, εμφανίζονται πεπερασμένα το πλήθος ριζικά, των οποίων οι τάξεις μπορεί να υποτεθούν, χωρίς βλάβη της γενικότητος, πρώτοι αριθμοί $p_1, p_2, p_3, \ldots p_\nu$, λόγω της σχέσης $\sqrt[l]{\sqrt[m]{a}} = \sqrt[l]{\sqrt[m]{a}}$. Για να διατυπώσομε σε πιο αυστηρή τυπική γλώσσα αυτή την έννοια επιλυσιμότητας, χρειαζόμαστε δύο ορισμούς:

Ορισμός 2.4.1. *Μία πεπερασμένη επέκταση L/K λέγεται ριζική, αν υπάρχει αλυσίδα επεκτάσεων*

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_{j-1} \subseteq K_j \subseteq \ldots \subseteq K_n = L$$

που ικανοποιεί την εξής συνθήκη: Για κάθε $j = 1, \ldots, n$ υπάρχει $\alpha_j \in K_j$ και πρώτος p_j, τέτοιοι ώστε $a_j^{p_j} \in K_{j-1}$.

Αν, στον παραπάνω ορισμό, θέσομε $a_j^{p_j} = b_{j-1} \in K_{j-1}$ $(j = 1, \ldots, n)$, τότε, η σχέση $a_j^{p_j} \in K_{j-1}$ διατυπώνεται, παραστατικώτερα: $a_j = \sqrt[p_j]{b_{j-1}}$, άρα, η αλυσίδα, που εμφανίζεται στον ορισμό, γράφεται

$$K = K_0 \subseteq K_0(\sqrt[p_1]{b_0}) = K_1 \subseteq \ldots \subseteq K_{j-1}(\sqrt[p_j]{b_{j-1}}) = K_j \subseteq \ldots \subseteq K_{n-1}(\sqrt[p_n]{b_{n-1}}) = K_n.$$

Προσοχή όμως! Αυτή η διατύπωση του ορισμού είναι μέν πιο παραστατική, αλλά έχει το σοβαρό μειονέκτημα του συμβολισμού $\sqrt[p]{b}$. Διότι, όταν εμφανίζεται σ' ένα τύπο το σύμβολο $\sqrt[p]{b}$, δεν είναι σαφές ποια απ' όλες τις p το πλήθος p-τάξεως ρίζες του b εννοείται. Για τον λόγο αυτό, προτιμώτερη είναι η διατύπωση του ορισμού 2.4.1.

Την επιλυσιμότητα με ριζικά ενός πολυωνύμου $f(X)$ μπορούμε να διατυπώσομε τώρα σε πιο τυπική γλώσσα ως εξής:

Ορισμός 2.4.2. *Το μη σταθερό πολυώνυμο $f(X) \in \mathbb{Q}[X]$ λέμε ότι είναι επιλύσιμο με ριζικά ή, ισοδύναμα, ότι η εξίσωση $f(x) = 0$ επιλύεται (είναι επιλύσιμη) με ριζικά, αν υπάρχει μία πεπερασμένη ριζική επέκταση του $\mathbb{Q}$, η οποία περιέχει όλες τις ρίζες του $f(X)$.*[13]

Στόχος αυτής της ενότητας είναι η απόδειξη του παρακάτω θεωρήματος.

Θεώρημα 2.4.3. *Για κάθε πρώτο $p \geq 5$ υπάρχουν πολυώνυμα βαθμού p, με ρητούς συντελεστές, τα οποία δεν είναι επιλύσιμα με ριζικά.*

[12] Παρατηρείστε τη διαφορά του x από το X. Είναι σοβαρό «ορθογραφικό» λάθος να γράφομε $f(X) = 0$, διότι αυτό σημαίνει ότι το *πολυώνυμο* $f(X)$ είναι μηδενικό και, άρα, όλοι οι συντελεστές του είναι 0.

[13] Θεωρούμε ότι εργαζόμαστε μέσα στο $\mathbb{C}$.

Η απόδειξη του θεωρήματος αυτού θα δοθεί στη σελίδα 60 και θα προκύψει ως συνέπεια μιας σειράς προτάσεων, οι οποίες ακολουθούν αμέσως παρακάτω.

Λήμμα 2.4.4. *Αν το μη σταθερό $f(X) \in \mathbb{Q}[X]$ είναι επιλύσιμο με ριζικά, τότε υπάρχουν:*

(1) Επέκταση $K_0 = \mathbb{Q}(\zeta_1, \dots, \zeta_n)$, όπου, για κάθε $j = 1, \dots, n$, είναι ζ_j πρωταρχική p_j-τάξεως ρίζα της μονάδας για κάποιον πρώτο p_j.

(2) Αλυσίδα επεκτάσεων

$$K_0 \subset K_1 \subset \dots \subset K_{j-1} \subset K_j \subset \dots \subset K_m,$$

στην οποία κάθε επέκταση K_j/K_{j-1} είναι Galois, ο βαθμός της είναι πρώτος ($j = 1, \dots, m$) και όλες οι ρίζες του $f(X)$ ανήκουν στο K_m.

Απόδειξη Σύμφωνα με τον Ορισμό 2.4.2, υπάρχει αλυσίδα επεκτάσεων

$$\mathbb{Q} = K'_0 \subseteq K'_1 \subseteq \dots \subseteq K'_{j-1} \subseteq K'_j \subseteq \dots \subseteq K'_n,$$

με τις εξής ιδιότητες: (1) Το K'_n περιέχει όλες τις ρίζες του $f(X)$, και (2) για κάθε $j = 1, \dots, n$ υπάρχει πρώτος p_j και $\alpha_j \in K'_j$, έτσι ώστε $K'_j = K'_{j-1}(\alpha_j)$ και $\alpha_j^{p_j} \in K'_{j-1}$.

Έστω ότι, για $j = 1, \dots, n$, είναι ζ_j πρωταρχική p_j-ρίζα της μονάδος. Θέτομε $K_0 = K'_0(\zeta_1, \dots, \zeta_n) = \mathbb{Q}(\zeta_1, \dots, \zeta_n)$ και $K_j = K'_j(\zeta_1, \dots, \zeta_n)$ για $j = 1, \dots, n$. Έτσι, παίρνομε την αλυσίδα

$$K_0 = \mathbb{Q}_0 \subseteq K_1 \subseteq \dots \subseteq K_{j-1} \subseteq K_j \subseteq \dots \subseteq K_n. \tag{2.4}$$

Προφανώς, το K_n περιέχει όλες τις ρίζες του $f(X)$. Επίσης, $K_j = K_{j-1}(\alpha_j)$ για κάθε $j = 1, \dots, n$. Πράγματι,

$$K_{j-1}(\alpha_j) = K'_{j-1}(\zeta_1, \dots, \zeta_n, \alpha_j) = K'_{j-1}(\alpha_j)(\zeta_1, \dots, \zeta_n) = K'_j(\zeta_1, \dots, \zeta_n) = K_j.$$

Έστω ότι για κάποιο j είναι $K_j \neq K_{j-1}$. Αυτό ισοδυναμεί με το ότι $\alpha_j \notin K_{j-1}$. Σ' αυτή την περίπτωση θα αποδείξομε ότι η επέκταση K_j/K_{j-1} είναι Galois και ο βαθμός της είναι p_j.

Απόδειξη του ισχυρισμού αυτού: Για απλοποίηση του συμβολισμού, ας θέσομε $\alpha_j = \alpha, p_j = p, \zeta = \zeta_j$. Παρατηρήστε ότι $\zeta \in K_{j-1} \subset K_j$. Εξ υποθέσεως, $\alpha^p = b$ για κάποιο $b \in K_{j-1}$, δηλαδή το α είναι ρίζα του $g(X) = X^p - b \in K_{j-1}[X]$. Οι ρίζες αυτού του πολυωνύμου είναι οι $\alpha, \alpha\zeta, \dots, \alpha\zeta^{p-1}$ και όλες ανήκουν στο K_j. Είναι φανερό τώρα ότι το K_j είναι σώμα ανάλυσης του $g(X)$ πάνω από το K_{j-1}, άρα η επέκταση K_j/K_{j-1} είναι Galois. Για να δείξομε ότι ο βαθμός της είναι p, αρκεί να δείξομε ότι το $g(X)$ είναι ανάγωγο στο $K_{j-1}[X]$. Αν δεν ήταν, θα είχε ένα ανάγωγο παράγοντα $h(X) \in K_{j-1}[X]$, του οποίου οι ρίζες θα ήταν κάποια, *αλλά όχι όλα*, εκ των $\alpha\zeta^k$. Δηλαδή, $h(X) = (X - \alpha\zeta^{k_1}) \dots (X - \alpha\zeta^{k_m})$ όπου $1 \leq m < p$. Ειδικώτερα, ο σταθερός όρος του $h(X)$ ανήκει στο K_{j-1}. Άρα, $(-1)^m \alpha^m \zeta^k \in K_{j-1}$, όπου $k = k_1 + \dots + k_m$. Όμως $\zeta \in K_{j-1}$, άρα $\alpha^m \in K_{j-1}$. Επειδή $(m, p) = 1$, υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $mx + py = 1$, οπότε $\alpha = (\alpha^m)^x (\alpha^p)^y$. Αλλά $\alpha^m, \alpha^p \in K_{j-1}$, άρα $\alpha \in K_{j-1}$, που αντίκειται στην υπόθεση ότι

$K_{j-1} \neq K_j$. Αυτό ολοκληρώνει την απόδειξη του ισχυρισμού.

Σύμφωνα με ό,τι μόλις αποδείξαμε, αν στην αλυσίδα (2.4) διαγράψομε τυχόν επαναλήψεις –δηλαδή, αν για κάποιο j είναι $K_j = K_{j-1}$, τότε διαγράφομε το ένα εκ των K_j, K_{j-1}– τότε καταλήγομε σε μιά αλυσίδα

$$K_0 \subseteq K_1 \subseteq ... \subseteq K_{j-1} \subseteq K_j \subseteq ... \subseteq K_m,$$

$(m \leq n)$, για την οποία ισχύει ότι η επέκταση K_j/K_{j-1} είναι Galois και ο βαθμός της είναι πρώτος για κάθε $j = 1, ..., m$. □

Λήμμα 2.4.5. *Αν K_0 είναι το σώμα, που αναφέρεται στην εκφώνηση του Λήμματος 2.4.4, τότε υπάρχει μία αλυσίδα επεκτάσεων*

$$\mathbb{Q} = M_0 \subset M_1 \subset \cdots \subset M_r = K_0,$$

τέτοια ώστε κάθε επέκταση M_i/M_{i-1} είναι Galois και ο βαθμός είναι πρώτος.

Απόδειξη. Έχομε την εξής αλυσίδα επεκτάσεων:

$$\mathbb{Q} \subset \mathbb{Q}(\zeta_1) \subset \mathbb{Q}(\zeta_1, \zeta_2) \subset \mathbb{Q}(\zeta_1, \zeta_2, \zeta_3) \subset \cdots \subset \mathbb{Q}(\zeta_1, \zeta_2, ..., \zeta_\nu) = K\ .$$

Τώρα, η βοηθητική πρόταση δ' του υπο-εδαφίου 2.4.1 (βλ. παρακάτω, στη σελίδα 60 ((Βοηθητικές προτάσεις, που χρησιμοποιήθηκαν))) εφαρμοζόμενο σε κάθε μία από τις επεκτάσεις

$$\mathbb{Q}(\zeta_1)/\mathbb{Q}, \quad \mathbb{Q}(\zeta_1, \zeta_2)/\mathbb{Q}(\zeta_1), \quad \mathbb{Q}(\zeta_1, \zeta_2, \zeta_3)/\mathbb{Q}(\zeta_1, \zeta_2), ...$$

αποδεικνύει τον ισχυρισμό μας. □

Πρόταση 2.4.6. *Αν το μη σταθερό $f(X) \in \mathbb{Q}[X]$ είναι επιλύσιμο με ριζικά, τότε υπάρχει μία αλυσίδα επεκτάσεων*

$$\mathbb{Q} = E_0 \subset E_1 \subset ... \subset E_{j-1} \subset E_j ... \subset E_s,$$

τέτοια ώστε, κάθε επέκταση E_j/E_{j-1} είναι Galois βαθμού πρώτου και το E_s περιέχει όλες τις ρίζες του $f(X) \in \mathbb{Q}[X]$.

Απόδειξη. Έστω η αλυσίδα επεκτάσεων $K_0 \subset K_1 \subset ... \subset K_m$, που μας εξασφαλίζει το Λήμμα 2.4.4 και $\mathbb{Q} = M_0 \subset M_1 \subset \cdots \subset M_r = K_0$ η αλυσίδα επεκτάσεων του Λήμματος 2.4.5. Τότε οι διαδοχικές επεκτάσεις

$$\mathbb{Q} \subset M_1 \subset \cdots \subset M_r = K_0 \subset K_1 \subset ... \subset K_m$$

αποτελούν μία αλυσίδα, που ικανοποιεί τις απαιτήσεις της εκφώνησης (με $s = r + m$ και $E_s = K_m$). □

Πρόταση 2.4.7. *Αν το μη σταθερό $f(X) \in \mathbb{Q}[X]$ είναι επιλύσιμο με ριζικά και L είναι το σώμα ανάλυσης του $f(X)$ πάνω από το $\mathbb{Q}$, τότε υπάρχει μία αλυσίδα επεκτάσεων*

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_t = L,$$

τέτοια ώστε κάθε επέκταση L_i/L_{i-1} είναι Galois, της οποίας ο βαθμός είναι πρώτος.

Απόδειξη. Θεωρούμε την αλυσίδα της Πρότασης 2.4.6 και θέτομε $L_i = E_i \cap L$, οπότε έχομε την αλυσίδα

$$\mathbb{Q} = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_s = L.$$

Διαγράφοντας τυχόν επαναλήψεις στην παραπάνω αλυσίδα, παίρνομε μία αλυσίδα (μικροτέρου μήκους ενδεχομένως)

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_t = L\ ,$$

$t \leq s$ όπου $L_{i-1} \neq L_i$ για όλα τα i. Λόγω του Θεωρήματος 2.3.2, για κάθε i υπάρχει $\lambda_i \in L_i$ τέτοιο ώστε $L_i = L_{i-1}(\lambda_i)$. Θα δείξομε ότι $E_i = E_{i-1}(\lambda_i)$. Έχομε τις διαδοχικές επεκτάσεις $E_{i-1} \subseteq E_{i-1}(\lambda_i) \subseteq E_i$. Επειδή ο βαθμός $[E_i : E_{i-1}]$ είναι πρώτος, θα πρέπει $E_{i-1}(\lambda_i) = E_i$ είτε E_{i-1}. Στη δεύτερη περίπτωση, $\lambda_i \in E_{i-1}$. Όμως $\lambda_i \in L$, άρα $\lambda_i \in L \cap E_{i-1} = L_{i-1}$ και $L_i = L_{i-1}$, άτοπο; έτσι, μένει η περίπτωση $E_i = E_{i-1}(\lambda_i)$. Ύστερα από αυτό μπορούμε να δείξομε ότι η επέκταση L_i/L_{i-1} είναι Galois και ο βαθμός της είναι πρώτος. Πράγματι, έστω $h(X) \in E_{i-1}[X]$ το ελάχιστο πολυώνυμο του λ_i πάνω από το E_{i-1}. Επειδή η E_i/E_{i-1} είναι Galois, όλες οι ρίζες του $h(X)$ ανήκουν στο E_i. Επειδή η $L/\mathbb{Q}$ είναι Galois (ως σώμα ανάλυσης του $f(X) \in \mathbb{Q}[X]$), η L/E_{i-1} είναι επίσης Galois, άρα (αφού $\lambda_i \in L$) όλες οι ρίζες του $h(X)$ ανήκουν και στο L; έπεται ότι όλες οι ρίζες του $h(X)$ ανήκουν στο $L \cap E_i = L_i$. Ειδικώτερα, οι συντελεστές του $h(X)$ ανήκουν στο L, άρα και στο $L \cap E_{i-1} = L_{i-1}$. Αλλά το $h(X)$ είναι ανάγωγο πάνω από το E_{i-1}, άρα, κατά μείζονα λόγο, είναι ανάγωγο και πάνω από το L_{i-1}. Έτσι, το ελάχιστο πολυώνυμο του λ_i πάνω από το E_{i-1} και πάνω από το L_{i-1} είναι, και στίς δύο περιπτώσεις, το $h(X)$ και, όπως είδαμε, οι ρίζες του $h(X)$ ανήκουν όλες στο L_i. Συνεπώς, το L_i είναι σώμα ανάλυσης του $h(X) \in L_{i-1}[X]$, που σημαίνει ότι η L_i/L_{i-1} είναι Galois. Επίσης, $[L_i : L_{i-1}] = \deg h = [E_i : E_{i-1}] =$ πρώτος. □

Πρόταση 2.4.8. *Υπάρχει μία αλυσίδα υποομάδων της $G = \mathcal{G}(L/\mathbb{Q})$*

$$G = G_0 \rhd G_1 \rhd G_2 \cdots \rhd G_t = \langle \mathrm{id} \rangle$$

($A \rhd B$ σημαίνει B κανονική υποομάδα της A), στην οποία η τάξη της ομάδας πηλίκο G_{j-1}/G_j είναι πρώτος αριθμός για κάθε $j = 1, \ldots, t$.

Απόδειξη. Επειδή η επέκταση $L/\mathbb{Q}$ είναι Galois, στην αλυσίδα ενδιαμέσων επεκτάσεων

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_t = L,$$

που μας εξασφαλίζει η Πρόταση 2.4.7, αντιστοιχεί μέσω της αντιστοιχίας Galois μία αλυσίδα

υποομάδων

$$G = \mathcal{G}(L/\mathbb{Q}) = G_0 > G_1 > \cdots > G_{j-1} > G_j > \ldots > G_{t-1} > G_t = \langle \mathrm{id} \rangle,$$

όπου $G_j = \mathcal{G}(L/L_j)$. Έστω ένα οποιοδήποτε $j \in \{1, \ldots, t\}$. Είναι $\mathbb{Q} < L_{j-1} < L_j < L$ οπότε το Θεώρημα 2.2.12 (4) συνεπάγεται ότι $[G_{j-1} : G_j] = [L_j : L_{j-1}] =$ πρώτος αριθμός, σύμφωνα με την Πρόταση 2.4.7. Αλλά, η τάξη της ομάδας-πηλίκο G_{j-1}/G_j ισούται με τον δείκτη $[G_{j-1} : G_j]$ και έτσι προκύπτει το αποδεικτέο. □

Ορισμός 2.4.9. *Η πεπερασμένη ομάδα G λέγεται επιλύσιμη αν υπάρχει αλυσσίδα υποομάδων*

$$G = G_0 \rhd G_1 \rhd G_2 \cdots \rhd G_t = \langle \mathrm{id} \rangle,$$

στην οποία η ομάδα-πηλίκο G_{j-1}/G_j είναι αβελιανή για κάθε $j = 1, \ldots, t$.

Άμεση συνέπεια της Πρότασης 2.4.8 είναι το εξής:

Θεώρημα 2.4.10. *Αν το μη σταθερό $f \in \mathbb{Q}[X]$ είναι επιλύσιμο με ριζικά, τότε η ομάδα Galois του f είναι επιλύσιμη υπό την έννοιαν του Ορισμού 2.4.9.*

Απόδειξη. Έστω L το σώμα ανάλυσης πάνω από το $\mathbb{Q}$ του επιλύσιμου με ριζικά πολυωνύμου $f \in \mathbb{Q}[X]$. Η ομάδα Galois του f είναι, εξ ορισμού, η $\mathcal{G}(L/\mathbb{Q})$ (βλ. Θεώρημα-Ορισμός 2.1.2). Θεωρούμε την αλυσίδα επεκτάσεων, που μας εξασφαλίζει η Πρόταση 2.4.8. Για κάθε $j = 1, \ldots, t$, η τάξη της ομάδας G_{j-1}/G_j είναι πρώτος άριθμός, οπότε αυτή η ομάδα είναι κυκλική[14], άρα και αβελιανή. □

Στο υπόλοιπο αυτής της ενότητας θα δείξομε ότι υπάρχουν πολυώνυμα με ρητούς συντελεστές, βαθμού ≥ 5, των οποίων η ομάδα Galois δεν είναι επιλύσιμη. Συνεπώς, βάσει του Θεωρήματος 2.4.10, θα οδηγηθούμε στο συμπέρασμα ότι τα πολυ?ωνυμα αυτά δεν είναι επιλύσιμα με ριζικά.

Θεώρημα 2.4.11. *Έστω πρώτος $p \geq 5$. Αν το $f \in \mathbb{Q}[X]$ είναι ανάγωγο, βαθμού p και έχει ακριβώς $p-2$ πραγματικές ρίζες, τότε η ομάδα Galois του f είναι η συμμετρική ομάδα $\mathbf{S}_p$.*

Απόδειξη. Έστω $\rho_1, \rho_2 = \bar{\rho}_1$ οι μοναδικές μη πραγματικές ρίζες και $\rho_3, \ldots, \rho_p$ οι υπόλοιπες $p-2$ ρίζες (οι οποίες είναι πραγματικές) του f, L το σώμα ανάλυσης του f πάνω από το $\mathbb{Q}$ και $G = \mathcal{G}(L/\mathbb{Q})$ η ομάδα Galois του f, την οποία βλέπομε ως υποομάδα της $\mathbb{S}_p$. Αν δείξομε ότι κάθε αντιμετάθεση $(\rho_i\ \rho_j) \in \mathbb{S}_p$, αυτό σημαίνει ότι η G ταυτίζεται με την $\mathbf{S}_p$.

Παρατηρούμε πρώτα ότι $(\rho_1\ \rho_2) \in G$. Πράγματι, ο περιορισμός στο L του αυτομορφισμού $z \to \bar{z}$ του $\mathbb{C}$ είναι $\mathbb{Q}$-αυτομορφισμός του L, δηλαδή, στοιχείο της G, στέλνει τη ρ_1 στη ρ_2 και αντιστρόφως, και αφήνει αναλλοίωτες τις υπόλοιπες ρίζες· συνεπώς ταυτίζεται με την αντιμετάθεση $(\rho_1\ \rho_2)$. Στο σύνολο $P = \{1, 2, \ldots, p\}$ ορίζομε τώρα την εξής σχέση:

$$i \sim j \Leftrightarrow i = j \ \text{ είτε } \ (\rho_i\ \rho_j) \in G.$$

[14] Απλή άσκηση ομάδων: Αν μιας ομάδας η τάξη είναι πρώτος αριθμός, τότε η ομάδα αυτή είναι κυκλική.

Παρατηρήστε ότι η τελευταία συνθήκη $(\rho_i\ \rho_j) \in G$ είναι συντομογραφία της συνθήκης:

$$\exists\, \sigma \in G\ :\ \sigma(\rho_i) = \rho_j\ \&\ \sigma(\rho_j) = \rho_i\ \&\ \sigma(\rho_k) = \rho_k\ \forall\, k \in P,\, k \neq i, j\,.$$

Η σχέση αυτή είναι, προφανώς, αυτοπαθής και συμμετρική. Είναι και μεταβατική, λόγω της σχέσης $(\rho_i\ \rho_k) = (\rho_i\ \rho_j)(\rho_j\ \rho_k)(\rho_i\ \rho_j)$, η οποία συνεπάγεται ότι, αν $i \sim j$ και $j \sim k$ τότε $i \sim k$. Έτσι, η σχέση $\sim$ είναι ισοδυναμία στο P. Στο τέλος θα δείξομε ότι όλες οι κλάσεις ισοδυναμίας είναι ισοπληθείς. Με δεδομένο αυτό, συμπεραίνομε ότι ο κοινός πληθάριθμος των κλάσεων ισοδυναμίας διαιρεί το p, άρα είναι ή 1 ή p. Το πρώτο ενδεχόμενο αποκλείεται, γιατί η κλάση του 1 περιέχει, εκτός από το 1, και το 2 (λόγω του ότι $(\rho_1\ \rho_2) \in G$). Άρα μένει το δεύτερο ενδεχόμενο, που σημαίνει ότι υπάρχει μόνο μία κλάση, δηλαδή, για κάθε ζεύγος i, j στοιχείων του P, $(\rho_i\ \rho_j) \in G$. Μένει να δείξομε ότι όλες οι κλάσεις ισοδυναμίας είναι ισοπληθείς. Έστω $\hat{i}, \hat{j}$ δύο κλάσεις, όπου $i, j \in P$. Θα δείξομε ότι υπάρχει αμφιμονοσήμαντη αντιστοιχία $\hat{i} \to \hat{j}$. Πρώτ' απ' όλα, λόγω του Θεωρήματος 1.4.3, υπάρχει $\mathbb{Q}$-ισομορφισμός $\mathbb{Q}(\rho_i) \to \mathbb{Q}(\rho_j)$, ο οποίος στέλνει τη ρ_i στη ρ_j. Αυτός, λόγω του Θεωρήματος 1.4.4, επεκτείνεται σε αυτομορφισμό του L. Άρα, υπάρχει αυτομορφισμός $\sigma \in G$, ώστε $\sigma(\rho_i) = \rho_j$. Έστω τώρα $m \in \hat{i}$ και $\sigma(\rho_m) = \rho_{m'}$. Είναι $m' \in \hat{j}$. Πράγματι, η σχέση $m \in i$ λέει ότι υπάρχει $\tau \in G$ ώστε $\tau(\rho_i) = \rho_m\ \ \&\ \ \tau(\rho_m) = \rho_i\ \ \&\ \tau(\rho_l) = \rho_l\ \forall l \in P,\, l \neq i, m$. Τότε, είναι απλό να δούμε ότι $\sigma\tau\sigma^{-1}(\rho_j) = \rho_{m'}$ και $\sigma\tau\sigma^{-1}(\rho_{m'}) = \rho_j$. Ακόμη, για $k \in P,\, k \neq j, m'$ είναι $\sigma\tau\sigma^{-1}(\rho_k) = \sigma\tau(\rho_l)$ (για κάποιο $l \in P,\, l \neq i, m$) $= \sigma(\rho_l) = \rho_k$. Συνεπώς, η αντιμετάθεση $(\rho_j, \rho_{m'})$ ταυτίζεται με τον αυτομορφισμό $\sigma\tau\sigma^{-1} \in G$, δηλαδή $m' \in \hat{j}$. Στο $m \in \hat{i}$ αντιστοιχούμε το $m' \in \hat{j}$ και, λόγω της $\sigma(\rho_m) = \rho_{m'}$, διαφορετικά m αντιστοιχούν σε διαφορετικά m'. Άρα ορίζεται αμφιμονοσήμαντη απεικόνιση $\hat{i} \to \hat{j}$. Εντελώς ανάλογα όμως, υπάρχει και αμφιμονοσήμαντη απεικόνιση $\hat{j} \to \hat{i}$, άρα οι κλάσεις $\hat{i}$ και $\hat{j}$ είναι ισοπληθείς. □

Θεώρημα 2.4.12. *Για $n \geq 5$, η συμμετρική ομάδα $\mathbf{S}_n$ δεν είναι επιλύσιμη.*

Απόδειξη. Έστω ότι για κάποιο $n \geq 5$ η $\mathbf{S}_n$ είναι επιλύσιμη. Αυτό σημαίνει ότι υπάρχει μία αλυσίδα υποομάδων της $\mathbf{S}_n$

$$S_n = G_0 \rhd G_1 \rhd G_2 \cdots \rhd G_t = \langle \mathrm{id} \rangle$$

στην οποία η ομάδα-πηλίκο G_i/G_{i-1} είναι αβελιανή ομάδα για κάθε $i = 1, \ldots, t$. Θα δείξομε ότι κάθε $G_i,\ i = 0, 1, \ldots, m$ περιέχει όλους τους κύκλους μήκους 3 της $\mathbf{S}_n$, κάτι προφανώς άτοπο για $i = t$. Για $i = 0$ ο ισχυρισμός είναι τετριμμένος. Έστω τώρα ότι για κάποιο $\nu \geq 0$ ($\nu \leq t-1$) η G_ν περιέχει όλους τους κύκλους μήκους 3. Θα δείξομε ότι, για οποιουσδήποτε διαφορετικούς δείκτες i, j, k μεταξύ 1 και n, ο κύκλος $(i\ j\ k)$ ανήκει στην $G_{\nu+1}$. Για το σκοπό αυτό επιλέγομε δύο δείκτες l, m μεταξύ 1 και n διαφορετικούς μεταξύ τους, αλλά και διαφορετικούς από τους i, j, k (αυτό είναι δυνατόν, διότι $n \geq 5$). Εξ υποθέσεως, $(j\ k\ m), (i\ l\ j), (m\ k\ j), (j\ l\ i) \in G_\nu$, άρα η ομάδα $G_\nu/G_{\nu+1}$ περιέχει τα $(j\ k\ m)G_{\nu+1}, (i\ l\ j)G_{\nu+1}, (m\ k\ j)G_{\nu+1}, (j\ l\ i)G_{\nu+1}$. Επειδή

η ομάδα αυτή είναι αβελιανή,

$$(j\ k\ m)G_{\nu+1}\cdot(i\ l\ j)G_{\nu+1}\cdot(m\ k\ j)\cdot G_{\nu+1}\cdot(j\ l\ i)G_{\nu+1}=$$
$$(j\ k\ m)G_{\nu+1}\cdot(m\ k\ j)G_{\nu+1}\cdot(i\ l\ j)\cdot G_{\nu+1}\cdot(j\ l\ i)G_{\nu+1}\ .$$

Όμως $(j\ k\ m)(m\ k\ j)$ και $(i\ l\ j)(j\ l\ i)$ είναι οι ταυτοτικές μεταθέσεις, οπότε το δεξιό μέλος ισούται με $G_{\nu+1}$, ενώ το αριστερό, εξ ορισμού της πράξης στην $G_\nu/G_{\nu+1}$, ισούται με $(j\ k\ m)(i\ l\ j)(m\ k\ j)(j\ l\ i)G_{\nu+1}=(i\ j\ k)G_{\nu+1}$. Έτσι, $(i\ j\ k)G_{\nu+1}=G_{\nu+1}$, που σημαίνει ότι $(i\ j\ k)\in G_{\nu+1}$. □

Απόδειξη του Θεωρήματος 2.4.3. Έστω πρώτος $p\geq 5$ και πολυώνυμο $f\in\mathbb{Q}[X]$ βαθμού p, ανάγωγο πάνω από το $\mathbb{Q}$, το οποίο έχει ακριβώς $p-2$ πραγματικές ρίζες. Από το Θεώρημα 2.4.11, η ομάδα Galois του f είναι η $\mathbb{S}_p$, η οποία δεν είναι επιλύσιμη, σύμφωνα με το Θεώρημα 2.4.12, άρα, βάσει του Θεωρήματος 2.4.10, το f δεν είναι απιλύσιμο με ριζικά. □

Ένα παράδειγμα τέτοιου πολυωνύμου για $p=5$ είναι το $X^5-17X-17$. Είναι ανάγωγο, όπως προκύπτει από το κριτήριο του Eisenstein, και το ότι έχει τρείς ακριβώς πραγματικές ρίζες είναι απλή άσκηση Απειροστικού Λογισμού.

2.4.1 Βοηθητικές προτάσεις που χρησιμοποιήθηκαν

(α') Αν ο p είναι πρώτος και $\zeta\neq 1$ είναι p-ρίζα της μονάδας, τότε $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})\cong\mathbb{Z}_p^*$. Ειδικότερα η $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ είναι κυκλική ομάδα[15].

(β') Αν ο p είναι πρώτος, $\zeta\neq 1$ είναι p-ρίζα της μονάδας και M οποιοδήποτε υπόσωμα του $\mathbb{C}$, τότε η ομάδα $\mathcal{G}(M(\zeta)/M)$ είναι κυκλική.

(γ') Για κάθε κυκλική πεπερασμένη ομάδα G (την πράξη της συμβολίζομε πολλαπλασιαστικά και το ουδέτερο στοιχείο με e) υπάρχει αλυσίδα υποομάδων της

$$\langle e\rangle=G_k\lhd G_{k-1}\lhd G_{k-2}\cdots\lhd G_0=G,$$

στην οποία ο δείκτης $[G_{j-1}:G_j]$ είναι πρώτος για κάθε $j=1,\dots,k$. Στην ειδική περίπτωση που η κυκλική πεπερασμένη ομάδα G έχει τάξη p^n με p πρώτο, ισχύει $[G_{j-1}:G_j]=p$ για κάθε $j=1,\dots,k$.

(δ') Έστω p,ζ και M όπως στο (β'), παραπάνω. Τότε υπάρχει μία αλυσίδα ενδιάμεσων επεκτάσεων

$$M=M_0<M_1<M_2<\cdots<M_k=M(\zeta),$$

στην οποία κάθε επέκταση M_j/M_{j-1} είναι Galois και ο βαθμός της είναι πρώτος.

Απόδειξη της (α'). Όλες οι διάφορες του 1 p-τάξεως ρίζες της μονάδας είναι οι $\zeta,\zeta^2,\dots,\zeta^{p-1}$ και ταυτίζονται με τις ρίζες του πολυωνύμου $g(X)=X^{p-1}+\cdots+X+1$, το οποίο είναι ανάγωγο

[15] Από τη Στοιχειώδη Θεωρία Αριθμών είναι γνωστό ότι για κάθε πρώτο p υπάρχει g με την εξής ιδιότητα: οι κλάσεις $1,2,\dots,p-1 \mod p$ ταυτίζονται (με διαφορετική, εν γένει, σειρά) με τις κλάσεις $g^k,\ k=0,1,\dots,p-2$. Αυτό σημαίνει ότι η ομάδα $\mathbb{Z}_p^*$ παράγεται από την κλάση $g \bmod p$, άρα είναι κυκλική. Παραδείγματα: $(p,g)=(7,3),(13,2),(17,3),(23,5),(41,6),(71,7),(1741,2),(3881,13),(3943,3)$.

(Πρόταση Γ'.6 του Παραρτήματος Γ'). Κάθε $\sigma \in \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ χαρακτηρίζεται από την τιμή του $\sigma(\zeta)$. Αλλά $\sigma(\zeta)$ πρέπει να είναι ρίζα του g, άρα ισούται με ζ^k για κάποιο $k \in \{1, \dots, p-1\}$. Επειδή $k_1 \equiv k_2 \pmod p \Rightarrow \zeta^{k_1} = \zeta^{k_2}$, η απεικόνιση $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) \ni \sigma \mapsto k \bmod p \in \mathbb{Z}_p^*$ είναι μονομορφισμός. Επιπλέον, ο $\phi(\sigma)$ είναι «επί». Πράγματι, για κάθε $k \in \{1, \dots, p-1\}$, η ζ^k είναι αρχική ρίζα της μονάδος, άρα $\mathbb{Q}(\zeta^k) = \mathbb{Q}(\zeta)$ ενώ, λόγω του Θεωρήματος 1.4.3, υπάρχει ισομορφισμός $\sigma : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta^k)$, ο οποίος αφήνει αναλλοίωτα όλα τα στοιχεία του $\mathbb{Q}$ και στέλνει το ζ στο ζ^k. Δηλαδή, $\sigma \in \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ και $\sigma(\zeta) = \zeta^k$, που σημαίνει ότι, κατά τον παραπάνω ορισθέντα μονομορφισμό ομάδων, ο σ αντιστοιχεί στην κλάση $k \bmod p$.

Απόδειξη της (β'). Η απεικόνιση

$$\mathcal{G}(M(\zeta)/M) \ni \sigma \xrightarrow{\phi} \sigma|_{\mathbb{Q}(\zeta)} \in \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}).$$

διαπιστώνεται εύκολα ότι είναι καλά ορισμένος ομομορφισμός ομάδων Επιπλέον, είναι 1-1. Πράγματι, αν $\phi \in \ker\phi$, τότε $\phi(\sigma) = \mathrm{id}_{\mathbb{Q}(\zeta)}$, άρα $\sigma(\zeta) = \zeta$. Επιπλέον, ο σ αφήνει αναλλοίωτα τα στοιχεία του M, συνεπώς $\sigma = \mathrm{id}_{M(\zeta)}$. Συνεπώς, ο ϕ είναι μονομορφισμός ομάδων, οπότε $\mathcal{G}(M(\zeta)/M) \cong \mathrm{Im}\,\phi$. Όμως, από την πρόταση (α'), η ομάδα $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ είναι ισόμορφη με την $\mathbb{Z}_p^*$, η οποία είναι κυκλική, άρα η $\mathcal{G}(M(\zeta)/M)$ είναι κυκλική, ως ισόμορφη με υποομάδα κυκλικής ομάδας.

Απόδειξη της (γ'). Έστω $G = \langle g \rangle$ και η τάξη του g (άρα και της G) είναι n. Έστω $n = p_1 \cdots p_k$ η ανάλυση του n σε πρώτους (όχι κατ' ανάγκη διαφορετικούς) παράγοντες. Αν θέσομε

$$G = G_0 = \langle g \rangle,\ G_1 = \langle g^{p_1} \rangle,\ G_2 = \langle g^{p_1 p_2} \rangle,\ \dots G_k = \langle g^{p_1 \cdots p_k} \rangle = \langle g^n \rangle = \langle e \rangle\ ,$$

τότε

$$\langle e \rangle = G_k \lhd G_{k-1} \lhd G_{k-2} \cdots \lhd G_0 = G$$

και για κάθε j, $|G_j| = n/p_1 \cdots p_j$, οπότε

$$[G_{j-1} : G_j] = \frac{|G_{j-1}|}{|\mathcal{G}_j|} = \frac{n}{p_1 \cdots p_{j-1}} : \frac{n}{p_1 \cdots p_{j-1} p_j} = p_j.$$

Στην ειδική περίπτωση που $p_1 = p_2 = \dots = p_k = p$, είναι, προφανώς, $[G_{j-1} : G_j] = p$.

Απόδειξη της (δ'). Θέτομε $L = M(\zeta)$. Η επέκταση L/M είναι κανονική, ως σώμα ανάλυσης του $X^p - 1 \in M[X]$, άρα είναι επέκταση Galois. Έστω $G = \mathcal{G}(L/M)$. Λόγω της πρότασης (β'), η G είναι κυκλική, οπότε θεωρούμε την αλυσίδα

$$\langle \mathrm{id} \rangle = G_k \lhd G_{k-1} \lhd G_{k-2} \cdots \lhd G_1 \lhd G_0 = G$$

που μας εξασφαλίζει η πρόταση (γ'). Σε αυτήν αντιστοιχεί, μέσω της αντιστοιχίας Galois, η

αλυσίδα επεκτάσεων

$$L = M(\zeta) = M_k > M_{k-1} > M_{k-2} > \cdots > M_1 > M_0 = M$$

όπου M_j $(j = 0, 1, \dots, k)$ είναι η ενδιάμεση επέκταση της L/M που αντιστοιχεί, μέσω της αντιστοιχίας Galois, στην ομάδα G_j, δηλαδή $G_j = \mathcal{G}(L/M_j)$.

Έστω ένα οποιοδήποτε $j \in \{1, \dots, k\}$. Από το Θεώρημα 2.2.12 (3), η επέκταση L/M_{j-1} είναι Galois. Τώρα εφαρμόζουμε αυτό το θεώρημα στις επεκτάσεις $M_{j-1} < M_j < L$. Για τις αντίστοιχες υποομάδες ισχύει $G_j \lhd G_{j-1}$, άρα βάσει του Θεωρήματος 2.2.12 (5) η M_j/M_{j-1} είναι επέκταση Galois. Τέλος, εφαρμόζοντας το Θεώρημα 2.2.12 (4) στην επέκταση L/M με $E_2 = M_j$ και $E_1 = M_{j-1}$ (οπότε $H_2 = G_{j-1}$ και $H_1 = G_j$) συμπεραίνομε ότι $[M_j : M_{j-1}] = [G_{j-1} : G_j] =$ πρώτος, σύμφωνα με την πρόταση (γ').

Ασκήσεις

1. Έστω $K \subseteq L \subseteq M$ διαδοχικές επεκτάσεις, τέτοιες ώστε, οι L/K και M/L είναι ριζικές. Δείξτε ότι και η M/K είναι ριζική.

2. Έστω K υπόσωμα του $\mathbb{C}$,[16] και ακέραιος $n \geq 2$, $n = p_1 \cdots p_k$, όπου $p_1, \dots, p_k$ είναι πρώτοι, όχι κατ' ανάγκη διαφορετικοί. Έστω L το σώμα ανάλυσης πάνω απ' το K του $X^n - 1 \in K[X]$. Για κάθε $j \in \{1, \dots, k\}$ θέτομε

$$z_j = \cos \frac{2\pi}{p_1 \cdots p_{j-1} p_j} + i \sin \frac{2\pi}{p_1 \cdots p_{j-1} p_j}.$$

   Αποδείξτε ότι, $z_j^{p_j} = z_{j-1}$ για κάθε $j \in \{2, \dots, k\}$ και συμπεράνατε ότι η επέκταση L/K είναι ριζική υπό την έννοια του Ορισμού 2.4.1.

3. Έστω K υπόσωμα του $\mathbb{C}$, $a \in K$ και ακέραιος $n \geq 2$. Έστω $b \in \mathbb{C}$ με $b^n = a$ και L το σώμα ανάλυσης πάνω απ' το $K(b)$ του $X^n - 1$. Αποδείξτε ότι το L είναι σώμα ανάλυσης του $X^n - a$ πάνω από το K και η επέκταση L/K είναι ριζική υπό την έννοια του Ορισμού 2.4.1.

   Υπόδειξη. Σε κάποια σημεία της απόδειξης οι ασκήσεις 2 και 1 είναι χρήσιμες.

   Έστω $\zeta = \cos(2\pi/n) + i \sin(2\pi/n)$. Δείξτε πρώτα ότι $L = K(b, \zeta)$ και, μετά, ότι το L είναι σώμα ανάλυσης του $X^n - a$ πάνω από το K. Στη συνέχεια, δείξτε ότι κάθε μία από τις επεκτάσεις $K(b)/K$ και $L/K(b)$ είναι ριζική υπό την έννοια του Ορισμού 2.4.1.

4. Έστω ότι το $f \in \mathbb{Q}[X]$ είναι επιλύσιμο με ριζικά. Έστω ακέραιος $n \geq 2$ και $g(X) = f(X^n)$. Αποδείξτε ότι και το g είναι επιλύσιμο με ριζικά.

   Υπόδειξη. Έστω K σώμα ανάλυσης του f πάνω από το $\mathbb{Q}$. Εξ υποθέσεως, υπάρχει ριζική επέκταση $L/\mathbb{Q}$ που περιέχει το K. Στον ορισμό της ριζικής επέκτασης, εμφανίζονται κάποιοι πρώτοι $p_j, j = 1, \dots, r$. Για κάθε $j = 1, \dots, r$, έστω $\zeta_j \neq 1$ μια p_j-ρίζα της μονάδας. Δείξτε ότι η επέκταση $L(\zeta_1, \dots, \zeta_r)/\mathbb{Q}$ είναι ριζική και περιέχει σώμα ανάλυσης του g.

[16] Είναι απλό να δείξει κανείς ότι κάθε υπόσωμα του $\mathbb{C}$ είναι επέκταση του $\mathbb{Q}$, άρα $\mathbb{Q} \subseteq K$.

2.5 Μελετη του τεταρτοβαθμιου πολυωνυμου

Έστω σώμα K με $\mathrm{char}\,(K) \neq 2$. Κάθε $X^4 + aX^3 + bX^2 + cX + d \in K[X]$ μπορεί να να μετασχηματισθεί σε πολυώνυμο της μορφής

$$f(X) = X^4 + qX^2 + rX + s, \quad q, r, s \in K, \tag{2.5}$$

δηλαδή, σε πολυώνυμο με μηδενικό συντελεστή στο X^3, μέσω της αντικατάστασης $X \leftarrow X - a/4$. Το f έχει το ίδιο σώμα διάσπασης και την ίδια διακρίνουσα με το αρχικό.

Σκοπός μας είναι να μελετήσομε την ομάδα Galois του f, *το οποίο υποθέτομε ανάγωγο.* Λόγω της υπόθεσης $\mathrm{char}\,(K) \neq 2$, το f είναι διαχωρίσιμο. Έστω L σώμα διάσπασης του f πάνω από το K και $t_1, \ldots, t_4 \in L$ οι (διαφορετικές) ρίζες του f. Την ομάδα $\mathbf{S}_4$ βλέπομε ως ομάδα μεταθέσεων των t_1, t_2, t_3, t_4. Χρησιμοποιούμε τους εξής συμβολισμούς:

$$G = \mathcal{G}\,(L/K) < \mathbf{S}_4 \quad \text{και} \quad V = \langle (t_1\,t_2)(t_3\,t_4), (t_1\,t_3)(t_2\,t_4) \rangle < \mathbf{S}_4.$$

Η V είναι ομάδα Klein (τάξεως 4).

Επίσης, ορίζομε

$$\alpha = (t_1 + t_2)(t_3 + t_4), \quad \beta = (t_1 + t_3)(t_2 + t_4), \quad \gamma = (t_1 + t_4)(t_2 + t_3). \tag{2.6}$$

Με απλές πράξεις διαπιστώνομε ότι $\alpha \neq \beta \neq \gamma \neq \alpha$, καθώς επίσης και ότι κάθε $\sigma \in \mathbf{S}_4$ προκαλεί μια μετάθεση των α, β, γ. Συνεπώς, το πολυώνυμο

$$g(X) := (X - \alpha)(X - \beta)(X - \gamma)$$

μένει αναλλοίωτο από κάθε $\sigma \in G$ (η συγκεκριμένη μορφή του υπολογίζεται στην άσκηση 4), άρα είναι πολυώνυμο του $K[X]$, με τρεις διαφορετικές ρίζες, όχι κατ' ανάγκη ανάγωγο πάνω από το K.

Τέλος, έστω

$$E := K(\alpha, \beta, \gamma) < L.$$

Η E/K είναι επέκταση Galois, αφού το E είναι σώμα διάσπασης του διαχωρίσιμου πολυωνύμου $g \in K[X]$.

Ένας υπολογισμός ρουτίνας δείχνει ότι $V \trianglelefteq \mathbf{S}_4$ και

$$\mathbf{S}_4/V = \{V,\ (t_1\,t_2)V,\ (t_2\,t_3)V,\ (t_1\,t_3)V,\ (t_1\,t_2\,t_3)V,\ (t_1\,t_3\,t_2)V\}. \tag{2.7}$$

Λήμμα 2.5.1. *$\mathcal{G}\,(L/E) = G \cap V$. Ισοδύναμα $\mathcal{F}(G \cap V) = E$.*

Απόδειξη. Ένας απλός έλεγχος δείχνει ότι κάθε $\sigma \in V$ αφήνει αναλλοίωτα τα α, β, γ, επομένως, αφήνει αναλλοίωτο και κάθε στοιχείο του E. Άρα, $G \cap V \leq \mathcal{G}\,(L/E)$. Αντιστρόφως, έστω $\sigma \in \mathcal{G}\,(L/E)$. Λόγω της (2.7) είναι $\sigma = \tau\sigma_0$, όπου $\sigma_0 \in V$ και $\tau \in \{id, (t_1\,t_2), (t_2\,t_3), (t_1\,t_3), (t_1\,t_2\,t_3), (t_1\,t_3\,t_2)\}$.

Το σ_0 αφήνει αναλλοίωτα τα α, β, γ, άρα $\sigma(\alpha) = \tau(\alpha)$, $\sigma(\beta) = \tau(\beta)$, $\sigma(\gamma) = \tau(\gamma)$. Ένας απλός έλεγχος, και πάλι, αρκεί για να μας δείξει ότι από τους έξι αυτομορφισμούς του παραπάνω συνόλου, ο μόνος που αφήνει αναλλοίωτα και τα τρία α, β, γ είναι ο id. Αλλά ο $\sigma \in \mathcal{G}(L/E)$ αφήνει αναλλοίωτα τα στοιχεία του E, άρα αφήνει αναλλοίωτα και τα τρία α, β, γ· επομένως $\tau = id$ και $\sigma = \sigma_0 \in V$, άρα $\sigma \in G \cap V$. Συνεπώς, $\mathcal{G}(L/E) < G \cap V$, οπότε $\mathcal{G}(L/E) = G \cap V$. □

Έστω $[E : K] = m$. Έχομε το παρακάτω διάγραμμα αντιστοιχίας Galois:

$$\begin{array}{ccc} L & \longleftrightarrow & \langle id \rangle \\ | & & | \\ E & \longleftrightarrow & G \cap V \\ |m & & | \\ K & \longleftrightarrow & G \end{array}$$

Επειδή η E/K είναι επέκταση Galois, συμπεραίνομε ότι $G \cap V \trianglelefteq V$ και

$$\mathcal{G}(E/K) \cong G/(G \cap V) \quad \therefore \quad \frac{|G|}{|G \cap V|} = |G/(G \cap V)| = |\mathcal{G}(E/K)| = [E : K] = m. \tag{2.8}$$

Είναι η $G \cap V$ υποομάδα της V, άρα $|G \cap V| \in \{1, 2, 4\}$. Επίσης, επειδή m είναι ο βαθμός του σώματος διάσπασης κυβικού πολυωνύμου, είναι $m \in \{1, 2, 3, 6\}$. Συγκεκριμένα, αν το g είναι ανάγωγο πάνω από το E, τότε $m = 3$ ή $m = 6$, ανάλογα με το αν $\mathrm{D}(g)$ είναι ή δεν είναι ίση με τετράγωνο ενός στοιχείου του K (βλ. Παράδειγμα 2 στη σελίδα 31 και, πιο συγκεκριμένα, το συμπέρασμα στη σελίδα 32).

Ακόμη, είναι $K(t_1) < L$ και $[K(t_1) : K] = 4$ γιατί το f είναι ανάγωγο πάνω από το K, άρα $|G| = [L : K]$ είναι πολλαπλάσιο του 4. Όμως $|G|$ είναι και διαιρέτης του $|\mathbf{S}_4| = 24$, άρα, συνοψίζοντας τα παραπάνω:

$$|G| \in \{4, 8, 12, 24\}, \quad |G \cap V| \in \{1, 2, 4\}, \quad m \in \{1, 2, 3, 6\}, \quad |G| = m \cdot |G \cap V|. \tag{2.9}$$

Στην απόδειξη του Θεωρήματος 2.5.6, το οποίο ταξινομεί τα τεταρτοβάθμια πολυώνυμα σε σχέση με τις ομάδες Galois αυτών, θα χρησιμοποιήσομε τις επόμενες καθαρά Ομαδο-θεωρητικές Προτάσεις 2.5.2 και 2.5.3 (δίχως απόδειξη), καθώς και τα Λήμματα 2.5.5 και 2.5.4 που αφορούν στην ειδική περίπτωση της G την οποία μελετούμε.

Πρόταση 2.5.2. *Αν $H \leq \mathbf{S}_n$ και $[\mathbf{S}_n : H] = 2$, τότε $H = \mathbf{A}_n$, δηλαδή, η μόνη υποομάδα της $\mathbf{S}_n$ με δείκτη 2 στην $\mathbf{S}_n$ είναι η εναλλάσουσα ομάδα $\mathbf{A}_n$.*

Πρόταση 2.5.3. *Έστω πεπερασμένη ομάδα H τάξεως $p^n m$, όπου ο p είναι πρώτος, $n \geq 1$ και $p \nmid m$. Αν J_1, J_2 είναι υποομάδες της H τάξεως p^n (δηλαδή, οι J_1, J_2 είναι p-υποομάδες Sylow της H[17]), τότε αυτές είναι ισόμορφες* [18].

[17] Η H περιέχει τέτοιες υποομάδες βάσει του *Πρώτου Θεωρήματος Sylow*.
[18] Βάσει του *Δεύτερου Θεωρήματος Sylow*.

Λήμμα 2.5.4. *Η G είναι μεταβατική υποομάδα της $\mathbf{S}_4$. Δηλαδή, για κάθε ζεύγος δεικτών $i, j \in \{1,2,3,4\}$ υπάρχει $\sigma \in G$ ώστε $\sigma(t_i) = t_j$.*

Απόδειξη. Βάσει του Θεωρήματος 1.4.3 υπάρχει ισομορφισμός $\sigma_0 : K(t_i) \to K(t_j)$, ο οποίος αφήνει αναλλοίωτα τα στοιχεία του K και $\sigma_0(t_i) = t_j$. Το L είναι σώμα ανάλυσης του f πάνω από το K, άρα είναι σώμα ανάλυσης του f και πάνω από τα $K(t_1)$ και $K(t_2)$. Επομένως, βάσει του Θεωρήματος 1.4.4, ο σ_0 επεκτείνεται σε ισομορφισμό $\sigma : L \to L$, δηλαδή, σε $\sigma \in G$ με την ιδιότητα $\sigma(t_i) = t_j$. □

Λήμμα 2.5.5. *Αν η $G = \mathcal{G}(L/K)$ είναι τάξεως 4 και δεν είναι κυκλική, τότε $G = V$.*

Απόδειξη. Οι υποομάδες της $\mathbf{S}_4$ τάξεως 4 είναι οι εξής:

$$\langle (t_1\, t_2\, t_3\, t_4) \rangle,\ \langle (t_1\, t_2\, t_4\, t_3) \rangle,\ \langle (t_1\, t_3\, t_2\, t_4) \rangle,$$

$$\langle (t_1\, t_3), (t_2\, t_4) \rangle,\ \langle (t_1\, t_4), (t_2\, t_3) \rangle,\ \langle (t_1\, t_2), (t_3\, t_4) \rangle,\ \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle.$$

Οι τρεις πρώτες από αυτές είναι κυκλικές, οπότε απορρίπτονται εξ υποθέσεως. Σύμφωνα με το Λήμμα 2.5.4, η G είναι μεταβατική, ενώ η τέταρτη, η πέμπτη και η έκτη είναι, προφανώς, μη μεταβατικές, άρα απορρίπτονται και αυτές και μένει δεκτή μόνο η τελευταία υποομάδα, η οποία είναι η V (διαπιστώστε ότι είναι μεταβατική). □

Στηριζόμενοι στα προηγούμενα είμαστε σε θέση τώρα να αποδείξομε το εξής:

Θεώρημα 2.5.6. (1) *Αν $m = 6$, τότε $G = \mathbf{S}_4$.*

(2) *Αν $m = 3$, τότε $G = \mathbf{A}_4$.*

(3) *Αν $m = 1$, τότε $G = V$.*

(4) *Αν $m = 2$ και το f είναι ανάγωγο πάνω από το E, τότε $G \cong \mathbf{D}_4$.*

(5) *Αν $m = 2$ και το f δεν είναι ανάγωγο πάνω από το E, τότε $G \cong \mathbb{Z}_4$.*

Απόδειξη. Έστω $m \in \{3, 6\}$. Τότε, από την 4^{η} και την 1^{η} σχέσης στην (2.9), έπεται ότι $|G| \in \{12, 24\}$. Αν $|G| = 24$, τότε, προφανώς, $G = \mathbf{S}_4$. Αν $|G| = 12$, τότε $[\mathbf{S}_4 : G] = 2$ και από την Πρόταση 2.5.2 συμπεραίνομε ότι $G = \mathbf{A}_4$. Τα στοιχεία της υποομάδας V είναι άρτιες μεταθέσεις, άρα, και στις δύο περιπτώσεις, $V \leq G$ και, συνεπώς, $G \cap V = V$, άρα $|G \cap V| = 4$. Τότε, από την 4^{η} σχέση στην (2.9), $|G| = 4m$. Από αυτή τη σχέση, σε συνδυασμό και με τα παραπάνω συμπεράσματα, γίνεται φανερό ότι, $m = 6 \Rightarrow G = \mathbf{S}_4$ και $m = 3 \Rightarrow G = \mathbf{A}_4$. Έτσι αποδείχθηκαν τα (1) και (2).

Έστω $m = 1$. Τότε, στο διάγραμμα αμέσως μετά την απόδειξη του Λήμματος 2.5.1, είναι $E = K$, άρα $G \cap V = V$. Αυτό σημαίνει ότι $G \leq V$. Η G δεν μπορεί να είναι γνήσια υποομάδα της V, διότι η τάξη της G είναι πολλαπλάσιο του 4, άρα $G = V$, οπότε αποδείχθηκε και το (3).

Έστω $m = 2$. Από την 1^{η}, 2^{η} και 4^{η} στη (2.9) έπεται ότι $|G| \in \{4, 8\}$. Σύμφωνα με την άσκηση 2, η $\mathbf{S}_4$ έχει υποομάδες ισόμορφες με τη $\mathbf{D}_4$, οπότε αν $|G| = 8$, τότε η G είναι 2-ομάδα Syllow της $\mathbf{S}_4$, όπως και η $\mathbf{D}_4$, συνεπώς, από την Πρόταση 2.5.3, $G \cong \mathbf{D}_4$ (δεν μπορούμε να ξέρομε με ποια από τις $\mathbf{D}_4$-υποομάδες της $\mathbf{S}_4$ είναι ίση η G). Αν $|G| = 4$ και η G δεν είναι

κυκλική, τότε, από το Λήμμα 2.5.5, είναι $G = V$, κάτι που αποκλείεται για τον εξής λόγο: Αν $G = V$, τότε $|G \cap V| = 4$ και,συνεπώς, από την 4^{η} σχέση (2.9), $|G| = 8$, αντίφαση. Συνεπώς, μέχρι στιγμής καταλήξαμε στο εξής συμπέρασμα: Αν $m = 2$ τότε $G \cong \mathbf{D}_4$ ή η G είναι κυκλική τάξεως 4, δηλαδή, $G \cong \mathbb{Z}_4$. Θα έχομε ολοκληρώσει την απόδειξη των (4) και (5) αν αποδείξομε ότι $G \cong \mathbf{D}_4 \Leftrightarrow f$ είναι ανάγωγο πάνω από το E.

Απόδειξη του τελευταίου ισχυρισμού. Έστω ότι το f είναι ανάγωγο πάνω από το E. Τότε $[L : E] = 4$, άρα, από το διάγραμμα αμέσως μετά την απόδειξη του Λήμματος 2.5.1 είναι $[L : K] = 8$, οπότε $|G| = 8$, άρα $G \cong \mathbf{D}_4$. Αντιστρόφως, έστω $G \cong \mathbf{D}_4$. Τότε, η 4^{η} σχέση (2.9) συνεπάγεται ότι $|G \cap V| = 4$, άρα $G \cap V = V$, δηλαδή, $\mathcal{G}(L/E) = V$. Το L είναι, προφανώς, σώμα διάσπασης του f πάνω από το E και για κάθε $i \in \{1, 2, 3, 4\}$ υπάρχει $\sigma \in V$ με $\sigma(t_1) = t_i$, άρα, από την άσκηση 3, το f είναι ανάγωγο πάνω από το E. □

Παράδειγμα 2.5.7. *Με τη βοήθεια του Θεωρήματος 2.5.6 θα υπολογίσομε τον ισομορφικό τύπο της ομάδας Galois G του $f(X) = X^4 + 5X + 5 \in \mathbb{Q}[X]$.*

Βασισμένος στην άσκηση 4 υπολογίζω $g(X) = X^3 - 20X + 25 = (X + 5)(X^2 - 5X + 5)$. Άρα $m = 2$ και E είναι το σώμα διάσπασης του g πάνω από το $\mathbb{Q}$, δηλαδή, το σώμα διάσπασης του $X^2 - 5X + 5$. Συνεπώς, $E = \mathbb{Q}(\sqrt{5})$. Τώρα πρέπει να αποφασίσω αν $G \cong \mathbf{D}_4$ ή $G \cong \mathbb{Z}_4$. Σύμφωνα με το θεώρημα, αυτό εξαρτάται από το αν το f είναι ή όχι ανάγωγο πάνω από το $\mathbb{Q}(\sqrt{5})$. Είναι $[\mathbb{Q}(t_i) : \mathbb{Q}] = 4$ για κάθε $i = 1, \dots, 4$, άρα το f δεν έχει ρίζα μέσα στο $E = \mathbb{Q}(\sqrt{5})$. Συνεπώς, το f δεν είναι ανάγωγο πάνω από το E αν και μόνο αν $f(X) = (X^2 + aX + b)(X^2 + cX + d)$ με τα $a, b, c, d \in E$. Αναπτύσσοντας το δεξιό μέλος και εξισώνοντας συντελεστές των ίσων δυνάμεων του X στα δύο μέλη, οδηγούμαι στις σχέσεις

$$c + a = 0, \quad ac + b + d = 0, \quad ad + bc = 5, \quad bd = 5.$$

Οι δύο πρώτες δίνουν $c = -a$ και $d = -b - ac = a^2 - b$. Αντικαθιστώντας στην τρίτη παίρνω $b = (a^3 - 5)/(2a)$ και τώρα η τελευταία γίνεται

$$5 = bd = \frac{a^3 - 5}{2a}(a^2 - b) = \frac{a^3 - 5}{2a}\left(a^2 - \frac{a^3 - 5}{2a}\right) = \frac{a^6 - 25}{4a^2}.$$

Έτσι, $a^6 - 20a^2 - 25 = 0$. Και παρατηρώ ότι η τιμή $a = \sqrt{5}$ επαληθεύει την τελευταία σχέση. Γι' αυτή την τιμή του a είναι και $c, b, d \in \mathbb{Q}(\sqrt{5}) = E$, άρα το f δεν είναι ανάγωγο πάνω από το E. Συνεπώς, σύμφωνα με το Θεώρημα 2.5.6 (5), είναι $G \cong \mathbb{Z}_4$.

Παρατήρηση. Αν και το πολυώνυμο $X^4 + 3X + 3 \in \mathbb{Q}[X]$ είναι «εντελώς όμοιο» με το f αυτού του παραδείγματος, έχει ομάδα Galois διαφορετικού ισομορφικού τύπου. Δείτε την άσκηση 5 (4).

2.5.1 Τύποι για τις ρίζες του τεταρτοβάθμιου πολυωνύμου

Θεωρούμε το τεταρτοβάθμιο πολυώνυμο που ορίζεται στην (2.5) και συμβολίζομε με $t_1, \dots, t_4$ τις ρίζες του. Επίσης, θεωρούμε τα α, β, γ που ορίζονται στην (2.6).

Σύμφωνα με την άσκηση 4 είναι $t_1+t_2=\sqrt{-\alpha}$ και, συνεπώς (λόγω της $t_1+t_2+t_3+t_4=0$), $t_3+t_4=-\sqrt{-\alpha}$. Προς το παρόν δεν προσδιορίζομε ποια από τις δύο τετραγωνικές ρίζες του $-\alpha$ συμβολίζει το $\sqrt{-\alpha}$. Με ανάλογο τρόπο παίρνομε και τις σχέσεις $t_1+t_3=\sqrt{-\beta}$, $t_2+t_4=-\sqrt{-\beta}$ και $t_1+t_4=\sqrt{-\gamma}$, $t_2+t_3=-\sqrt{-\gamma}$. Όπως και στην περίπτωση του $\sqrt{-\alpha}$, δεν προσδιορίζομε, προς το παρόν, ποια από τις δύο τετραγωνικές ρίζες των $-\beta$ και $-\gamma$ προσδιορίζουν τα σύμβολα $\sqrt{-\beta}$ και $\sqrt{-\gamma}$.

Από την ίδια άσκηση, τα α,β,γ είναι ρίζες του πολυωνύμου $g(X)$ που ορίζεται στην (2.11), άρα, από τους τύπους του Viète,

$$\alpha+\beta+\gamma=2q,\quad \alpha\beta+\beta\gamma+\gamma\alpha=q^2-4s,\quad \alpha\beta\gamma=-r^2$$

Για απλούστευση του συμβολισμού θέτομε $\xi_1=\sqrt{-\alpha},\xi_2=\sqrt{-\beta},\xi_3=\sqrt{-\gamma}$,[19] οπότε, βάσει των παραπάνω έχομε το σύστημα γραμμικών εξισώσεων

$$\begin{pmatrix} 1 & 1 & 0 & 0\\ 0 & 0 & 1 & 1\\ 1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & 0 & 1\\ 0 & 1 & 1 & 0 \end{pmatrix}\begin{pmatrix} t_1\\ t_2\\ t_3\\ t_4 \end{pmatrix}=\begin{pmatrix} \xi_1\\ -\xi_1\\ \xi_2\\ -\xi_2\\ \xi_3\\ -\xi_3 \end{pmatrix}$$

Αυτό το μη ομογενές γραμμικό σύστημα έχει ακριβώς μία λύση, την

$$t_1=\tfrac{1}{2}(\xi_1+\xi_2+\xi_3),\ \ t_2=\tfrac{1}{2}(\xi_1-\xi_2-\xi_3),\ \ t_3=\tfrac{1}{2}(-\xi_1+\xi_2-\xi_3),\ \ t_4=\tfrac{1}{2}(-\xi_1-\xi_2+\xi_3).$$

Μένει να προσδιορίσομε ποια από τις δύο τετραγωνικές ρίζες των $-\alpha,-\beta,-\gamma$ συμβολίζουν, αντιστοίχως, τα ξ,ξ_2,ξ_3. Σύμφωνα με τους τύπους του Viète, πρέπει και αρκεί να ισχύουν οι σχέσεις

$$\sum_{1\le i\le 4} t_i=0,\quad \sum_{1\le i<j\le 4} t_it_j=q,\quad \sum_{1\le i<j<k\le 4} t_it_jt_k=-r,\quad t_1t_2t_3t_4=s \tag{2.10}$$

Η πρώτη από τις σχέσεις (2.10) είναι προφανής και ισχύει ανεξαρτήτως επιλογής των τετραγωνικών ριζών $\xi_1,\dots,\xi_4$.

Υπολογίζομε

$$\sum_{1\le i<j\le 4} t_it_j=-\tfrac{1}{2}(\xi^2+\xi_2^2+\xi_3^2=\tfrac{1}{2}(\alpha+\beta+\gamma)=q,$$

άρα ισχύει και η δεύτερη σχέση (2.10) ανεξαρτήτως επιλογής των τετραγωνικών ριζών $\xi_1,\dots,\xi_4$.

[19] Τα ξ δεν είναι όλα 0 γιατί, σε αντίθετη περίπτωση, το $g(X)$ είναι μηδενικό πολυώνυμο, άρα $q=r=s=0$, που αντιβάινει στις υποθέσεις για το $f(X)$.

Υπολογίζομε

$$t_1t_2t_3t_4 = \tfrac{1}{16}\{\xi_1^4+\xi_2^4+\xi_3^4-2\left((\xi\xi_2)^2+(\xi_2\xi_3)^2+(\xi_3\xi_1)^2\right)\} = \tfrac{1}{16}\{\alpha^2+\beta^2+\gamma^2-2(\alpha\beta+\beta\gamma+\gamma\alpha)\}$$
$$= \tfrac{1}{16}\{(\alpha+\beta+\gamma)^2-4(\alpha\beta+\beta\gamma+\gamma\alpha)\} = \tfrac{1}{16}\{4q^2-4(q^2-4s)\} = s,$$

συνεπώς ισχύει και η τέταρτη σχέση (2.10) ανεξαρτήτως επιλογής των τετραγωνικών ριζών $\xi_1,\dots,\xi_4$ και μένει ο έλεγχος της τρίτης σχέσης. Υπολογίζομε $\sum_{1\le i<j<k\le 4} t_it_jt_k = \xi_1\xi_2\xi_3$. Είναι $(\xi_1\xi_2\xi_3)^2 = -\alpha\beta\gamma = r^2$, συνεπώς, στον ορισμό των $\xi_1=\sqrt{-\alpha}$, $\xi_2=\sqrt{-\beta}$ και $\xi_3=\sqrt{-\gamma}$, η επιλογή των τετραγωνικών ριζών πρέπει να γίνει έτσι ώστε το γινόμενό τους να ισούται με $-r$ (προφανώς υπάρχουν περισσότερες από μία επιλογές).

Συνοψίζοντας, οι ρίζες $t_1,\dots,t_4$ του $f(X)=X^4+qX^2+rX+s\in F[X]$ $(\mathrm{char}\,(F)\neq 2,3)$, δίδονται από τις σχέσεις

$$\begin{aligned} t_1 &= \tfrac{1}{2}\left(\sqrt{-\alpha}+\sqrt{-\beta}+\sqrt{-\gamma}\right)\\ t_2 &= \tfrac{1}{2}\left(\sqrt{-\alpha}-\sqrt{-\beta}-\sqrt{-\gamma}\right)\\ t_3 &= \tfrac{1}{2}\left(-\sqrt{-\alpha}+\sqrt{-\beta}-\sqrt{-\gamma}\right)\\ t_4 &= \tfrac{1}{2}\left(-\sqrt{-\alpha}-\sqrt{-\beta}+\sqrt{-\gamma}\right) \end{aligned}$$

όπου α,β,γ είναι οι ρίζες του $g(X)=X^3-2qX^2+(q^2-4s)X+r^2$ και οι τετραγωνικές ρίζες $\sqrt{-\alpha},\sqrt{-\beta},\sqrt{-\gamma}$ είναι έτσι επιλεγμένες ώστε $\sqrt{-\alpha}\sqrt{-\beta}\sqrt{-\gamma}=-r$. Ο υπολογισμός των ριζών γίνεται με τη βοήθεια της άσκησης 1.[20]

Ασκήσεις

1. *Τύποι του Cardano για τις ρίζες κυβικού πολυωνύμου.*
   Έστω K σώμα χαρακτηριστικής $\neq 2,3$ και το πολυώνυμο $f=X^3+pX+q\in K[X]$. Έστω
   $$R=\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3,\quad \alpha^3=-\frac{q}{2}+\sqrt{R},\quad \beta=-\frac{p}{3\alpha},$$
   όπου $\sqrt{R}$ είναι μια οποιαδήποτε από τις δύο τετραγωνικές ρίζες του R. Παρατηρήστε ότι το α είναι μια οποιαδήποτε επιλογή κυβικής ρίζας του $\sqrt{R}-q/2$. Αν $\omega\neq 1$ είναι κυβική ρίζα της μονάδας (σε κάποια επέκταση του K[21]), τότε
   $$f(X)=(X-r_0)(X-r_1)(X-r_2),\quad r_i=\omega^i\alpha+\omega^{2i}\beta,\ \ i=0,1,2.$$
   Υπόδειξη. Δείξτε ότι $\beta^3=-\frac{q}{2}-\sqrt{R}$. Επίσης, ίσως σας χρησιμεύει η παρατήρηση ότι $-108R=D$, η διακρίνουσα του f.

2. Έστω $i,j,k\in\{2,3,4\}$ με $i\neq j\neq k\neq 1$. Αποδείξτε ότι η υποομάδα $\langle(1\,j),\,(1\,i\,j\,k)\rangle$ της $\mathbf{S}_4$ είναι ισόμορφη με τη διεδρική ομάδα $\mathbf{D}_4$.

[20] Η αλλαγή μεταβλητής $X\leftarrow X+2q/3$ μετασχηματίζει το $g(X)$ σε κυβικό πολυώνυμο δίχως τον όρο X^2.
[21] Υπάρχει τέτοιο ω γιατί $\mathrm{char}\,K\neq 3$

3. Έστω σώμα K και $f \in K[X]$ βαθμού $n > 1$ το οποίο έχει n διαφορετικές ρίζες $t_1, \dots, t_n$ σε ένα σώμα διάσπασής του L πάνω από το K. Αποδείξτε το εξής: Αν για κάθε $i = 1, \dots, n$ υπάρχει K-αυτομορφισμός του L που στέλνει το t_1 στο t_i, τότε το f είναι ανάγωγο πάνω από το K.

4. *Μέθοδος του Descartes για την εύρεση των ριζών του τεταρτοβάθμιου πολυωνύμου.* Έστω σώμα K του οποίου η χαρακτηριστική είναι $\neq 2, 3$ και ανάγωγο πολυώνυμο

$$f(X) = X^4 + qX^2 + rX + s \in K[X].^{22}$$

Έστω L σώμα διάσπασης του f πάνω από το K, $t_1, \dots, t_4 \in L$ οι διαφορετικές (όπως έχομε ήδη 'δει) ρίζες του και τα στοιχεία $\alpha, \beta, \gamma \in L$ που ορίζονται στη σχέση (2.6). Τα α, β, γ είναι διαφορετικά (αρκεί ένας απλός υπολογισμός), ορίσαμε το πολυώνυμο $g(X) = (X - \alpha)(X - \beta)(X - \gamma)$ και αποδείξαμε ότι $g \in K[X]$.

(1) Δείξτε ότι $\mathrm{D}(g) = \mathrm{D}(f)$.

(2) Έστω $t_1 + t_2 = -k$, $t_1 t_2 = l$ και $t_3 t_4 = m$ με $k, l, m \in E$. Παρατηρήστε ότι $t_3 + t_4 = k$ και εξηγήστε (δίχως καθόλου πράξεις) γιατί

$$f(X) = (X^2 + kX + l)(X^2 - kX + m).$$

(3) Εξισώνοντας τους συντελεστές στα δύο μέλη της παραπάνω ισότητας εκφράστε τα l, m, s συναρτήσει των q, r, k και στη συνέχεια δείξτε πώς, απαλείφοντας τα l, m μεταξύ των τριών αυτών σχέσεων, θα οδηγηθείτε στη στη σχέση $k^6 + 2qk^4 + (q^2 - 4s)k^2 - r^2 = 0$. Παρατηρήστε ότι $-k^2 = \alpha$ και συμπεράνετε ότι το α είναι ρίζα του $X^3 - 2qX^2 + (q^2 - 4s)X + r^2$. Ειδικότερα, επειδή $-\alpha = k^2 = (t_1 + t_2)^2$, είναι $\sqrt{-\alpha} \in E$. Θεωρήστε δεδομένο ότι με εντελώς ανάλογο τρόπο μπορεί να αποδειχθεί ότι τα β και γ είναι, επίσης, ρίζες του ίδιου πολυωνύμου, με $\sqrt{-\beta}, \sqrt{-\gamma} \in E$, και εξηγήστε γιατί

$$g(X) = X^3 - 2qX^2 + (q^2 - 4s)X + r^2. \tag{2.11}$$

(4) Έστω $z \in L$ μια οποιαδήποτε μη μηδενική ρίζα του g. Αποδείξτε ότι

$$f(X) = \left(X^2 + \sqrt{-z}\, X + \frac{1}{2}\left(-z + q - \frac{r}{\sqrt{-z}}\right)\right) \cdot \left(X^2 - \sqrt{-z}\, X + \frac{1}{2}\left(-z + q + \frac{r}{\sqrt{-z}}\right)\right).$$

Συμπεράνετε ότι οι ρίζες των δύο δευτεροβάθμιων πολυωνύμων του δεξιού μέλους μας δίνουν τις τέσσερις ρίζες του f.

Σημείωση. Η κυβική εξίσωση $g(x) = 0$ λέγεται *επιλύουσα* της τεταρτοβάθμιας εξίσωσης $f(x) = 0$.

[22] Κάθε $X^4 + aX^3 + bX^2 + cX + d \in K[X]$ μπορεί να πάρει αυτή τη μορφή (δηλαδή, με μηδενικό συντελεστή στο X^3), μέσω της αντικατάστασης $X \leftarrow X - a/4$ και το πολυώνυμο που προκύπτει έχει την ίδια διακρίνουσα με το αρχικό.

5. Με τη βοήθεια του Θεωρήματος 2.5.6 υπολογίστε τον ισομορφικό τύπο των ομάδων Galois καθενός από τα παρακάτω πολυώνυμα του $\mathbb{Q}[X]$:

   (α') $X^4 + 8X + 12$

   (β') $X^4 + 4X^2 - 2$

   (γ') $X^4 - X - 1$

   (δ') $X^4 + 3X + 3$

   (ε') $X^4 + 8X + 14$

Παράρτημα Α΄

Δακτύλιοι, Ιδεώδη και μία σημαντική εφαρμογή

Σ' αυτό το παράρτημα υπενθυμίζονται έννοιες και προτάσεις που εμπίπτουν σ' ένα μάθημα Άλγεβρας ΙΙ και, ως εφαρμογή, αποδεικνύεται το πολύ σμαντικό Θεώρημα Α'.5.

Οι δακτύλιοι σε τούτες τις σημειώσεις είναι πάντοτε *μεταθετικοί* με *μοναδιαίο στοιχείο*.

Ένα μη κενό υποσύνολο I ενός δακτυλίου R καλείται *ιδεώδες* αν ικανοποιεί τις εξής δύο απαιτήσεις:

(1) Αν $\iota_1, \iota_2 \in I$ τότε $\iota_1 + \iota_2 \in I$.

(2) Αν $\iota \in I$ και $r \in R$, τότε $r\iota \in I$.

Ορισμός Α΄.1. *Έστω δακτύλιος R και I ιδεώδες του R. Για κάθε $r \in R$ ορίζεται το σύνολο $r + I = \{r + \iota : \iota \in I\} \subseteq R$. Το σύνολο όλων αυτών των υποσυνόλων του R, καθώς το r διατρέχει τον R συμβολίζεται R/I. Δηλαδή,*

$$R/I = \{r + I : r \in R\}.$$

Μεσω των πράξεων του R, ορίζονται πράξεις και στο R/I ως εξής:

$$\begin{aligned} (r_1 + I) + (r_2 + I) &= (r_1 + r_2) + I \\ (r_1 + I) \cdot (r_2 + I) &= (r_1 r_2) + I \end{aligned}$$

Αποδεικνύεται ότι οι πράξεις αυτές είναι καλά ορισμένες και καθιστούν το σύνολο R/I μεταθετικό δακτύλιο με μοναδιαίο στοιχείο το $1 + I$ και μηδενικό το $0 + I = I$. Ο δακτύλιος αυτός χαρακτηρίζεται δακτύλιος-πηλίκο του R ως προς I.

Ορισμός Α΄.2. *Έστω δακτύλιος R.*

- *Ένα ιδεώδες I του R χαρακτηρίζεται πρώτο αν $I \neq R$ και ικανοποιεί την εξής συνθήκη: Αν $a, b \in R$ και $ab \in I$, τότε $a \in I$ είτε $b \in I$.*

- *Ένα ιδεώδες I του R χαρακτηρίζεται maximal (μεγιστοειδές) αν $I \neq R$ και δεν περιέχεται γνήσια σε κανένα γνήσιο ιδεώδες του R.*
  Ισοδύναμα: Αν J είναι ένα ιδεώδες του R και $I \subseteq J$, τότε $J = I$ ή $J = R$.

Ισχύουν οι επόμενες προτάσεις:

Πρόταση Α΄.3. *Έστω δακτύλιος R.*

1. *Κάθε maximal ιδεώδες του R είναι πρώτο ιδεώδες. Το αντίστροφο δεν ισχύει, εν γένει.*
2. *Το ιδεώδες I του R είναι πρώτο, αν και μόνο αν ο δακτύλιος πηλίκο R/I είναι ακέραια περιοχή.*
3. *Το ιδεώδες I του R είναι maximal, αν και μόνο αν ο δακτύλιος πηλίκο R/I είναι σώμα.*

Πολύ σημαντικό ρόλο στη Θεωρία Σωμάτων παίζουν οι δακτύλιοι των πολυωνύμων μιας ή περισσότερων μεταβλητών, με συντελεστές από ένα σώμα K.

Πρόταση Α΄.4. *Έστω ο δακτύλιος $R = K[X]$ (K σώμα και X η μεταβλητή των πολυωνύμων). Έστω μη σταθερό πολυώνυμο $f(X) \in R$. Θεωρούμε το ιδεώδες $I = f(X)R$.*
Ισχύει το εξής: Το I είναι maximal αν και μόνο αν το $f(\mathrm{X})$ είναι ανάγωγο.

Θεώρημα Α΄.5. *Έστω σώμα K και ανάγωγο πολυώνυμο $f(X) \in K[X]$ βαθμού > 1. Τότε υπάρχει σώμα L με τις εξής ιδιότητες:*

1. *Το L περιέχει ένα υπόσωμα ισόμορφο με το K, άρα το K μπορεί να θεωρηθεί υπόσωμα του L.*
2. *Το f έχει ρίζα στο L.*
3. *Αν το $v \in L$ είναι ρίζα του f, τότε $L = K[v]$, δηλαδή τα στοιχεία του L ταυτίζονται με τις πολυωνυμικές εκφράσεις του v που έχουν συντελεστές στο K.*

Απόδειξη. Το ιδεώδες $I = f(X)K[X]$ είναι maximal, σύμφωνα με την Πρόταση Α'.4, οπότε, σύμφωνα με την Πρόταση Α'.3 (3), ο δακτύλιος-πηλίκο $L = K[X]/I$ είναι σώμα. Η απεικόνιση $K \ni c \mapsto c + I \in L$ είναι μονομορφισμός σωμάτων (πολύ εύκολο ν' αποδειχθεί), οπότε το K μπορεί να θεωρηθεί υπόσωμα του L: απλούστατα, κάθε $c \in K$ ταυτίζεται με το $c + I \in L$. Επειδή το σύμβολο X έχει χρησιμοποιηθεί στον ορισμό του L, θα χρησιμοποιήσομε το Y για τη μεταβλητή των πολυωνύμων με συντελεστές στο L. Έτσι, αν $f(X) = a_nX^n + \cdots + a_1X + a_0$, θεωρούμενο ως πολυώνυμο με συντελεστές από το L, γράφεται

$$f(Y) = (a_n + I)Y^n + \cdots + (a_1 + I)Y + (a_0 + I).$$

Τώρα θα δείξομε ότι το $f(Y)$ έχει ρίζα το $v = X + I \in L$. Πράγματι, έχοντας κατά νου το πώς

ορίζονται οι πράξεις σ' ένα δακτύλιο-πηλίκο, υπολογίζομε:

$$\begin{aligned} f(v) &= (a_n + I)(X + I)^n + (a_{n-1} + I)(X + I)^{n-1} + \cdots + (a_1 + I)(X + I) + (a_0 + I) \\ &= (a_n + I)(X^n + I) + (a_{n-1} + I)(X^{n-1} + I) + \cdots + (a_1 + I)(X + I) + (a_0 + I) \\ &= (a_n X^n + I) + (a_{n-1} X^{n-1} + I) + \cdots + (a_1 X + I) + (a_0 + I) \\ &= (a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0) + I = f(X) + I = I \text{ το } 0 \text{ του } L). \end{aligned}$$

Μένει ν' αποδειχθεί ότι κάθε στοιχείο του L μπορεί να γραφτεί ως $g(v)$ για κατάλληλο πολυώνυμο $g(Y) \in L[Y]$. Πράγματι, από τον ορισμό του L, το τυπικό στοιχείο-του έχει τη μορφή $h(X) + I$, όπου $h(X) \in K[X]$. Έστω $h(X) = b_m X^m + \cdots + b_1 X + b_0$ $(b_0, \ldots, b_m \in K)$. Τότε, από τον τρόπο που ορίζονται οι πράξεις στον δακτύλιο-πηλίκο και τον ορισμό του v,

$$\begin{aligned} h(X) + I &= (b_m X^m + \cdots + b_1 X + b_0) + I \\ &= (b_m + I)(X + I)^m + \cdots + (b_1 + I)(X + I) + (b_0 + I) \\ &= (b_m + I)v^m + \cdots + (b_1 + I)v(X + I) + (b_0 + I) = h(v), \end{aligned}$$

όπου, στην τελευταία ισότητα, το h θεωρείται ως πολυώνυμο του L μέσω της ταύτισης των $b_0, b_1, \ldots, b_m$ με τις εικόνες τους $b_0 + I, b_1 + I, \ldots, b_m + I$ στο L. □

Παράρτημα Β΄

Πολυώνυμα και ΜΚΔ αυτών

Β'.1 Λίγα περί πολυωνύμων

[1] Έστω μεταθετικός δακτύλιος R με μοναδιαίο στοιχείο και $R[X]$ ο δακτύλιος πολυωνύμων με συντελεστές από τον R. Ένα πολυώνυμο $f(X) \in R[X]$ μπορεί να γραφεί και ως άπειρο άθροισμα $\sum'_{i\geq 0} r_i X^i$, όπου ο τόνος στο $\sum$ δηλώνει ότι «σχεδόν όλα» τα r_i είναι 0 (δηλαδή, πεπερασμένο, το πολύ πλήθος από τα r_i είναι $\neq 0$). Αυτός ο τρόπος γραφής των πολυωνύμων βοηθά στα εξής (θα παραλείπομε στο εξής τον τόνο στο $\sum$).

- Στον ορισμό του αθροίσματος και του γινομένου πολυωνύμων:

$$\sum_{i\geq 0} a_i X^i + \sum_{i\geq 0} b_i X^i = \sum_{i\geq 0} (a_i + b_i) X^i \tag{Β'.1}$$

$$\left(\sum_{i\geq 0} a_i X^i\right) \cdot \left(\sum_{i\geq 0} b_i X^i\right) = \sum_{k\geq 0} c_k X^k, \quad c_k = \sum_{i,j\geq 0, i+j=k} a_i b_j \tag{Β'.2}$$

- Στην απόδειξη του ότι, για κάθε $r \in R$ η συνάρτηση αντικατάστασης $R[X] \ni f(X) \mapsto f(r) \in R$ είναι ομομορφισμός δακτυλίων, δηλαδή,

$$(f+g)(r) = f(r) + g(r), \quad (f \cdot g)(r) = f(r) \cdot g(r). \tag{Β'.3}$$

- Στην απόδειξη του επόμενου θεωρήματος:

Θεώρημα Β΄.1. *Κάθε ισομορφισμός δακτυλίων (μεταθετικών με μοναδιαίο) $\sigma : R \to S$ επεκτείνεται σε ισομορφισμό δακτυλίων $R[X] \to S[X]$, ο οποίος συμβολίζεται με το ίδιο γράμμα σ και ορίζεται ως εξής:*

$$\sigma\left(\sum_{i\geq 0} a_i X^i\right) = \sum_{i\geq 0} \sigma(a_i) X^i.$$

Απόδειξη. Το ότι η απεικόνιση $\sigma : R[X] \to S[X]$ είναι 1-1 και επί, προκύπτει εύκολα από το ότι η $\sigma : R \to S$ έχει αυτές τις ιδιότητες. Επίσης, αν γράψομε $f = \sum_{i\geq 0} a_i X^i$ και $g = \sum_{i\geq 0} b_i X^i$

[1] Κάποιες υπενθυμίσεις, όχι συστηματική ανάπτυξη.

και χρησιμοποιήσομε τη σχέση (Β'.1) και το ότι η απεικόνιση $\sigma : R \to S$ είναι ομομορφισμός, διαπιστώνομε πολύ εύκολα ότι $\sigma(f+g) = \sigma(f) + \sigma(g)$. Κάποια δυσκολία έχει μόνο η απόδειξη της σχέσης $\sigma(f \cdot g) = \sigma(f) \cdot \sigma(g)$, την οποία δίνομε τώρα.

Από την (Β'.2), $f \cdot g = \sum_{k\geq 0} c_k X^k$, όπου $c_k = \sum_{i+j=k} a_i b_j$ (η συνθήκη $i, j \geq 0$ εννοείται). Άρα,

$$\sigma(f \cdot g) = \sum_{k\geq 0} \sigma(c_k) X^k, \quad \sigma(c_k) = \sigma\left(\sum_{i+j=k} a_i b_j\right) = \sum_{i+j=k} \sigma(a_i)\sigma(b_j),$$

όπου η τελευταία ισότητα οφείλεται στον ομομορφισμό $\sigma : R \to S$.

Από την άλλη, $\sigma(f) = \sum_{i\geq 0} \sigma(a_i) X^i$ και $\sigma(g) = \sum_{i\geq 0} \sigma(b_i) X^i$, άρα, βάσει της (Β'.2),

$$\sigma(f) \cdot \sigma(g) = \left(\sum_{i\geq 0} \sigma(a_i) X^i\right) \cdot \left(\sum_{i\geq 0} \sigma(b_i) X^i\right) = \sum_{k\geq 0} d_k X^k,$$

όπου $d_k = \sum_{i+j=k} \sigma(a_i)\sigma(b_j) = (\text{βλ. πιο πάνω}) = \sigma(c_k)$. Άρα, $\sigma(f \cdot g) = \sigma(f) \cdot \sigma(g)$. □

Σημείωση επί του συμβολισμού. Συνήθως, για «ελάφρυνση» του συμβολισμού, θα γράφομε σf αντί $\sigma(f)$· αλλά για γινόμενο δύο ή περισσότερων πολυωνύμων χρησιμοποιούμε την παρένθεση –δεν γράφομε π.χ. σfg, αλλά $\sigma(fg)$.

Β'.2 ΜΚΔ ΠΟΛΥΩΝΥΜΩΝ

Ορισμός Β′.2. *Έστω K σώμα και $f(X), g(X) \in K[X]$. Το πολυώνυμο $d(X) \in K[X]$ λέγεται μέγιστος κοινός διαιρέτης (ΜΚΔ) των $f(X)$ και $g(X)$ αν είναι κοινός διαιρέτης τους, ο οποίος, επιπλέον, διαιρείται από κάθε κοινό διαιρέτη των $f(X)$ και $g(X)$.*

Από τον ορισμό αυτό προκύπτουν (όχι με εντελώς άμεσο τρόπο) τα εξής.

Πρόταση Β′.3.

1. *Αν $d(X)$ είναι ΜΚΔ των $f(X), g(X)$, τότε κανένας άλλος κοινός διαιρέτης αυτών των πολυωνύμων δεν έχει μεγαλύτερο βαθμό από εκείνο του $d(X)$.*

2. *Αν $d(X)$ είναι ΜΚΔ των $f(X), g(X)$, τότε, για κάθε $c \in K^*$ το πολυώνυμο $c \cdot d(X)$ είναι, επίσης ΜΚΔ των $f(X), g(X)$· αντιστρόφως, αν $d'(X)$ είναι ένας άλλος ΜΚΔ των $f(X), g(X)$, τότε υπαρχει $c \in K^*$, έτσι ώστε $d'(X) = c \cdot d(X)$.*

3. *Αν $d(X)$ είναι ΜΚΔ των $f(X), g(X)$, τότε υπάρχουν $f_1(X), g_1(X) \in K[X]$, τέτοια ώστε $f_1(X)f(X) + g_1(X)g(X) = d(X)$.*

4. *Έστω ότι αναλύομε τα μη σταθερά πολυώνυμα $f(X), g(X)$ σε ανάγωγα πολυώνυμα του $K[X]$ και έστω ότι τα ανάγωγα πολυώνυμα $p_1(X), \ldots, p_n(X)$ είναι, ακριβώς, αυτά τα ανάγωγα, πού εμφανίζονται στην ανάλυση και των δύο πολυωνύμων, με εκθέτες $a_1, \ldots, a_n$ στην ανάλυση του $f(X)$ και με εκθέτες $b_1, \ldots, b_n$ στην ανάλυση του $g(X)$· δηλαδή,*

$$f(X) = p_1(X)^{a_1} \cdots p_n(X)^{a_n} f_1(X), \quad g(X) = p_1(X)^{b_1} \cdots p_n(X)^{b_n} g_1(X),$$

όπου τα πολυώνυμα $f_1(X)$ *και* $g_1(X)$ *δεν έχουν κοινά ανάγωγα πολυώνυμα. Τότε, το πολυώνυμο*

$$d(X) = p_1(X)^{c_1} \cdots p_n(X)^{c_n}, \quad c_i = \min\{a_i, b_i\} \;\; i = 1, \ldots, n$$

είναι ΜΚΔ των $f(X), g(X)$.

Οι δύο πρώτες από τις παραπάνω προτάσεις είναι άμεσες συνέπειες του ορισμού, ενώ η απόδειξη της τρίτης είναι αρκετά πιο σύνθετη. Επίσης, λόγω της δεύτερης – η οποία, ουσιαστικά, μας λέει ότι, όταν ξέρομε ένα ΜΚΔ δύο πολυωνύμων, τους ξέρομε όλους – λέμε συχνά ((*d*(*X*) είναι ο ΜΚΔ των $f(X), g(X)$)) και εννούμε, φυσικά, ότι και κάθε $c \cdot d(X)$ είναι ΜΚΔ των $f(X), g(X)$.

Ορισμός Β′.4. *Έστω* K *σώμα και* $f(X), g(X) \in K[X]$. *Τα πολυώνυμα αυτά λέγονται πρώτα μεταξύ τους, αν ένας ΜΚΔ τους είναι σταθερόπολυώνυμο· μ' άλλα λόγια, αν οι μόνοι κοινοί διαιρέτες των δύο πολυωνύμων είναι τα σταθερά πολυώνυμα.*

Στην παρακάτω πρόταση, το (1) αποδεικνύεται πολύ εύκολα απ' τους ορισμούς· η απόδειξη του (2) είναι σχεδόν άμεση συνέπεια του (3) της πρότασης Β′.3.

Πρόταση Β′.5. *1. Αν* $f(X), g(X) \in K[X]$ *και το* $g(X)$ *είναι ανάγωγο, τότε, τα πολυώνυμα αυτά, ή είναι πρώτα μεταξύ τους, ή* $g(X) | f(X)$· *στη δεύτερη περίπτωση, το* $g(X)$ *είναι ΜΚΔ των δύο πολυωνύμων.*

2. Έστω ότι $f(X), g(X) \in K[X]$. *Αν υπάρχει επέκταση* L *του* K, *η οποία να περιέχει μία κοινή ρίζα των* $f(X), g(X)$, *τότε τα πολυώνυμα αυτά δεν είναι πρώτα μεταξύ τους. Αν, επιπλέον, το* $g(X)$ *είναι ανάγωγο πάνω απ' το* K, *τότε* $g(X) | f(X)$.

Αν, για παράδειγμα, ξέρομε ότι δύο πολυώνυμα με ρητούς συντελεστές έχουν μία κοινή μιγαδική ρίζα (εδώ $K = \mathbb{Q}$ και $L = \mathbb{C}$), τότε αποκλείεται να είναι πρώτα μεταξύ τους: ο ΜΚΔ τους είναι μη σταθερό πολυώνυμο με ρητούς συντελεστές. Αν, επιπλέον, το ένα από τα δύο πολυώνυμα είναι ανάγωγο, πάνω απ' το $\mathbb{Q}$, τότε αυτό το πολυώνυμο διαιρεί (στο $\mathbb{Q}[X]$) το άλλο πολυώνυμο.

Εύρεση του ΜΚΔ

Η εύρεση του ΜΚΔ δύο πολυωνύμων $f(X), g(X) \in K[X]$ γίνεται με τον *Ευκλείδειο Αλγόριθμο*,

εκτελώντας διαδοχικές διαιρέσεις μέχρις ότου βρούμε υπόλοιπο 0 [2], ως εξής:

$$\begin{aligned} f(X) &= g(X)q(X) + r_1(X) \\ g(X) &= r_1(X)q_1(X) + r_2(X) \\ r_1(X) &= r_2(X)q_2(X) + r_3(X) \\ r_2(X) &= r_3(X)q_3(X) + r_4(X) \\ &\vdots \quad\quad \vdots \\ r_{n-2}(X) &= r_{n-1}(X)q_{n-1}(X) + r_n(X) \\ r_{n-1}(X) &= r_n(X)q_n(X) + 0 \end{aligned}$$

Το τελευταίο μη μηδενικό υπόλοιπο, έστω $r_n(X)$, είναι ΜΚΔ των $f(X), g(X)$.

Παράδειγμα 1. Έστω $f(X) = X^3 - 1,\ g(X) = X^3 + 3X + 3 \in \mathbb{Q}[X]$. Εδώ $q(X) = 1$ και $r(X) = -3X - 4$, άρα $f_1(X) = g(X) = X^3 + 3X + 3$ και $g_1(X) = r(X) = -3X - 4$. Η ευκλείδεια διαίρεση του $f_1(X)$ με το $g_1(X)$ δίνει $q_1(X) = -\frac{1}{3}X^2 + \frac{4}{9}X - \frac{43}{27}$ και $r_1(X) = -\frac{91}{27}$. Το $r_1(X)$ είναι το τελευταίο μη μηδενικό υπόλοιπο. Διότι, αν θέσομε $f_2(X) = g_1(X)$ και $g_2(X) = r_1(X)$, επειδή το $r_1(X)$ είναι σταθερό πολυώνυμο, η ευκλείδεια διαίρεση του $f_2(X)$ με το σταθερό πολυώνυμο θά δώσει υπόλοιπο 0.[3] Άρα, ο μέγιστος κοινός διαιρέτης των $X^3 - 1$ και $X^3 + 3X + 3$ είναι $-\frac{91}{27}$. Αλλά τότε, το σύνολο των μεγίστων κοινών διαιρετών των $X^3 - 1$ και $X^3 + 3X + 3$ είναι το σύνολο $\{c(-\frac{91}{27}) : c \in \mathbb{Q}\} = \mathbb{Q}$ (άρα, ένας μέγιστος κοινός διαιρέτης είναι και το σταθερό πολυώνυμο 1). Τα συγκεκριμένα πολυώνυμα, λοιπόν, είναι *πρώτα μεταξύ τους*.

Η διαδικασία εύρεσης του μεγίστου κοινού διαιρέτη, μας επιτρέπει να βρούμε πολυώνυμα $f'(X)$ και $g'(X)$, τέτοια ώστε $f'(X)f(X) + g'(X)g(X) = \text{μκδ} = 1$. Πράγματι, έχομε

(Β'.4)

$$f(X) = g(X) \cdot 1 + (-3X - 4) \quad \text{και} \quad X^3 + 3X + 3 = (-3X - 4)\left(-\frac{1}{3}X^2 + \frac{4}{9}X - \frac{43}{27}\right) - \frac{91}{27}.$$

Η δεύτερη σχέση (Β'.4) γράφεται

$$-\frac{91}{27} = X^3 + 3X + 3 + (-3X - 4)\left(\frac{1}{3}X^2 - \frac{4}{9}X + \frac{43}{27}\right). \tag{Β'.5}$$

Πολλαπλασιάζοντας την πρώτη σχέση (Β'.4) με $\left(\frac{1}{3}X^2 - \frac{4}{9}X + \frac{43}{27}\right)$ βλέπομε ότι

$$(-3X - 4)\left(\frac{1}{3}X^2 - \frac{4}{9}X + \frac{43}{27}\right) = (f(X) - g(X))\left(\frac{1}{3}X^2 - \frac{4}{9}X + \frac{43}{27}\right),$$

[2] Αποδεικνύεται εύκολα ότι αυτό θά συμβεί οπωσδήποτε.

[3] Γενικά, η ευκλείδεια διαίρεση του $f(X) \in K[X]$ με το σταθερό ($\neq 0$) πολυώνυμο c είναι $f(X) = cg(X) + 0$, όπου $g(X) = c^{-1}f(X)$.

και τότε, από την (B'.5),

$$-\frac{91}{27} = g(X) + (f(X) - g(X))\left(\frac{1}{3}X^2 - \frac{4}{9}X + \frac{43}{27}\right)$$
$$f(X)\left(\frac{1}{3}X^2 - \frac{4}{9}X + \frac{43}{27}\right) + g(X)\left(-\frac{1}{3}X^2 + \frac{4}{9}X - \frac{16}{27}\right).$$

Πολλαπλασιάζοντας την τελευταία σχέση επί $-\frac{27}{91}$ βρίσκομε

$$1 = f(X)\underbrace{\left(-\frac{9}{91}X^2 + \frac{12}{91}X - \frac{43}{91}\right)}_{f'(X)} + g(X)\underbrace{\left(\frac{9}{91}X^2 - \frac{12}{91}X + \frac{16}{91}\right)}_{g'(X)}.$$

Παράδειγμα 2. Ας θεωρήσομε τα πολυώνυμα του προηγουμένου παραδείγματος, αλλά τώρα πάνω από το σώμα $\mathbb{Z}_5$: $f(X) = X^3 - 1 = X^3 + 4$, $g(X) = X^3 + 3X + 3 \in \mathbb{Z}_5[X]$. Η ευκλείδεια διαίρεση του $f(X)$ διά $g(X)$ δίνει πηλίκο $q(X) = 1$ και υπόλοιπο $r(X) = 2X - 1$, άρα $f(X) = g(X) + (2X + 1)$. Μετά, $f_1(X) = g(X) = X^3 + 3X + 3$, $g_1(X) = r(X) = 2X + 1$ και η σχέση της ευκλείδειας διαίρεσης είναι $X^3+3X+3 = (2X+1)(3X^2+X+1)+2$ ($q_1(X) = 3X^2+X+1$ και $r_1(X) = 2$). Αφού καταλήξαμε σε υπόλοιπο, πού είναι σταθερό πολυώνυμο, έπεται ότι αυτό είναι ο ζητούμενος μέγιστος κοινός διαιρέτης (όπως και στο παράδειγμα 1). Οι σχέσεις

$$f(X) = g(X) + (2X + 1), \quad g(X) = (2X + 1)(3X^2 + X + 1) + 2$$

μας επιτρέπουν να γράψομε το 2 ως γραμμικό συνδυασμό των $f(X)$ και $g(X)$:

$$\begin{aligned} 2 &= g(X) - (2X + 1)(3X^2 + X + 1) = g(X) - (f(X) - g(X))(3X^2 + X + 1) \\ &= f(X)(-3X^2 - X - 1) + (3X^2 + X + 2) \\ &= (2X^2 + 4X + 4)f(X) + (3X^2 + X + 2)g(X). \end{aligned}$$

Αν προτιμούμε στη θέση του 2 να έχομε το 1, πολλαπλασιάζομε την παραπάνω σχέση επί 3 ($3 \cdot 2 = 1$ στο $\mathbb{Z}_5$), οπότε παίρνομε τη σχέση

$$1 = (X^2 + 2X + 2)f(X) + (4X^2 + 3X + 1)g(X).$$

Ασκησεις

1. Για κάθ' ένα από τα παρακάτω ζεύγη πολυωνύμων $f(X), g(X)$ υπολογίστε, με τον ευκλείδειο αλγόριθμο, τον ΜΚΔ τους, καθώς και πολυώνυμα $f'(X), g'(X)$, τέτοια ώστε $f'(X)f(X) + g'(X)g(X) = \text{ΜΚΔ}(f(X), g(X))$.

   - $f(X) = X^4 + X^3 + X + 1$, $g(X) = X^2 + X + 1 \in \mathbb{Q}[X]$
   - $f(X) = X^4 + X^3 + X + 1$, $g(X) = X^2 + X + 1 \in \mathbb{Z}_5[X]$
   - $f(X) = X^5 + 2X^4 + X^2 + 3X + 2$, $g(X) = X^3 + 2X^2 + X + 2 \in \mathbb{Q}[X]$

- $f(X) = X^5 + 2X^4 + X^2 + 3X + 2$, $g(X) = X^3 + 2X^2 + X + 2 \in \mathbb{Z}_5[X]$
- $f(X) = X^5 + 2X^4 + X^2 + 3X + 2$, $g(X) = X^3 + 2X^2 + X + 2 \in \mathbb{Z}_7[X]$

2. Έστω ότι τα $f(X), g(X) \in K[X]$ είναι πρώτα μεταξύ τους και L είναι επέκταση του K. Αποδείξτε ότι τα $f(X), g(X)$, θεωρούμενα ως πολυώνυμα του $L[X]$, εξακολουθούν να παραμένουν πρώτα μεταξύ τους.

   Υπόδειξη. Χρησιμοποιείστε την Πρόταση 3.

Παράρτημα Γ΄

Χρήσιμες προτάσεις για πολυώνυμα

Έστω σώμα K. Θά δώσομε κάποιες χρήσιμες προτάσεις για πολυώνυμα με συντελεστές από το K. Κάποιες προτάσεις ισχύουν μόνο για $K = \mathbb{Q}$.

Πρόταση Γ΄.1. *1. Το να έχει το $f(X) \in K[X]$ πρωτοβάθμιο παράγοντα με συντελεστές από το K, ισοδυναμεί με το να υπάρχει ρίζα του $f(X)$ στο K.*

2. Αν ο βαθμός του $f(X) \in K[X]$ είναι 2 ή 3 και το $f(X)$ δεν είναι ανάγωγο στο $K[X]$, τότε, το $f(X)$ έχει ρίζα στο K. *Άρα, αν διαπιστώσομε ότι ένα τέτοιο πολυώνυμο δεν έχει ρίζα στο K, τότε το πολυώνυμο είναι ανάγωγο.*

Προσοχή! Αν το $f(X)$ έχει βαθμό τουλάχιστον 4, τότε, η μη ύπαρξη ρίζας στο K δεν σημαίνει ότι το $f(X)$ είναι ανάγωγο. Για παράδειγμα, το $f(X) = X^4 - 5X^2 + 6 \in \mathbb{Q}[X]$ δεν έχει ρίζα στο $\mathbb{Q}$, αλλά δεν είναι ανάγωγο, αφού $f(X) = (X^2 - 2)(X^2 - 3)$.

Σε κάποιες ειδικές, αλλά σημαντικές περιπτώσεις, η εύρεση του συνόλου όλων των ριζών του $f(X)$, οι οποίες ανήκουν στο K (αυτό το σύνολο μπορεί να είναι κενό), είναι πεπερασμένη διαδικασία. Προφανώς, αυτό είναι αληθές όταν $K = \mathbb{Z}_p$, p πρώτος και, γενικότερα, όταν το K είναι πεπερασμένο σώμα. Τότε, για κάθε $u \in K$ εξετάζομε κατα πόσον $f(u) = 0$ και το πλήθος των δοκιμών μας είναι πεπερασμένο, αφού το K είναι πεπερασμένο.

Μία άλλη σημαντική περίπτωση είναι όταν $K = \mathbb{Q}$. Επειδή ένα πολυώνυμο $f(X) \in \mathbb{Q}[X]$ μπορεί να πολλαπλασισαθεί με κατάλληλο ακέραιο d για να διαγραφούν οι τυχόν παρονομαστές των συντελεστών του, και το $d \cdot f(X)$ έχει τίς ἴδιες ρίζες με το $f(X)$, γι' αυτό, αρκεί να εξετάσομε πολυώνυμα με ακέραιους συντελεστές.

Πρόταση Γ΄.2. *Έστω $f(X) \in \mathbb{Z}[X]$ με συντελεστή μεγιστοβαθμίου όρου a και σταθερό όρο c. Αν το $f(X)$ έχει ρητή ρίζα και την γράψομε με τη μορφή αναγώγου κλάσματος m/n (δηλαδή, $(m, n) = 1$), τότε $m|c$ και $n|a$.*

Για παράδειγμα, αν το πολυώνυμο $f(X) = 10X^5 + 3X^4 - X^3 + 7X^2 - 2X + 4 \in \mathbb{Z}[X]$ έχει ρητή ρίζα, αυτή πρέπει να αναζητηθεί μεταξύ των αριθμών της εξής λίστας:

$\pm\frac{1}{1} = \pm 1$, $\pm\frac{1}{2}$, $\pm\frac{1}{5}$, $\pm\frac{1}{10}$, $\pm\frac{2}{1} = \pm 2$, $\pm\frac{2}{2} = \pm 1$, $\pm\frac{2}{5}$, $\pm\frac{2}{10} = \pm\frac{1}{5}$, $\pm\frac{4}{1} = \pm 4$, $\pm\frac{4}{2} = \pm 2$, $\pm\frac{4}{5}$, $\pm\frac{4}{10} = \pm\frac{2}{5}$.

Δοκιμάζοντας έναν-έναν αυτούς τους αριθμούς, βλέπομε ποιοί είναι ρίζες του $f(X)$. Στη συγκεκριμένη περίπτωση, διαπιστώνομε ότι ουδείς από αυτούς τους αριθμούς είναι ρίζα του $f(X)$, άρα, σύμφωνα με την πρόταση Γ'.2, το πολυώνυμο αυτό δεν έχει ρητές ρίζες.

Όσον αφορά στην εξέταση του κατά πόσον ένα πολυώνυμο με ακέραιους συντελεστές είναι ανάγωγο πάνω από το $\mathbb{Q}$, εξαιρετικά χρήσιμο είναι το

Πρόταση Γ΄.3 (Λήμμα του Gauss)**.** *Για να εξετάσομε αν το μη σταθερό $f(X) \in \mathbb{Z}[X]$ είναι ανάγωγο πάνω από το $\mathbb{Q}$, αρκεί να εξετάσομε αν υπάρχει ανάλυση $f(X) = g(X)h(X)$ με τα $g(X), h(X) \in \mathbb{Z}[X]$ μη σταθερά.*

Για παράδειγμα, έστω ότι θέλομε να εξετάσομε κατά πόσον το $f(X) = X^4 - 6X^3 + kX^2 + 3X + 4$, όπου $k \in \mathbb{Z}$, είναι ανάγωγο πάνω από το $\mathbb{Q}$. Εξετάζομε πρώτα αν έχει πρωτοβάθμιο παράγοντα. Από το 1 της πρότασης Γ'.1 αρκεί να εξετάσομε αν το $f(X)$ έχει ρητές ρίζες. Οι μόνες *πιθανές* ρητές ρίζες, σύμφωνα με την πρόταση Γ'.2 είναι $\pm 1, \pm 2, \pm 4$. Υπολογίζομε $f(1) = 2 + k$, $f(-1) = 8 + k$, $f(2) = -22 + 4k$, $f(-2) = 62 + 4k$, $f(4) = -112 + 16k$ και $f(-4) = 632 + 16k$. Ουδεμία ακέραια τιμή του k μηδενίζει τα $f(\pm 2)$, $f(-4)$, ενώ τα $f(1)$, $f(-1)$, $f(4)$ μηδενίζονται για $k = -2, -8, 7$, αντιστοίχως. Συνεπώς, για $k = -2, -8, 7$, το $f(X)$ έχει πρωτοβάθμιο παράγοντα και, συνεπώς, δεν είναι ανάγωγο. Για τίς υπόλοιπες ακέραιες τιμές του k δεν μπορούμε *ακόμη* να αποφανθούμε με βεβαιότητα. Πρέπει να εξετάσομε αν το $f(X)$ αναλύεται σε δευτεροβάθμιους παράγοντες, πράγμα το οποίο κάνομε αμέσως παρακάτω: $f(X) = (aX^2+bX+c)(a'X^2+b'X+c')$. Το λήμμα του Gauss μας λέει ότι, αρκεί να υποθέσομε τους a, b, c, a', b', c' ακεραίους. Αλλά τότε, συγκρίνοντας τους μεγιστοβαθμίους όρους, έχομε $aa' = 1$, άρα, καθώς τα a, a' είναι ακέραιοι, συμπεραίνομε ότι $a = a' = \pm 1$. Χωρίς βλάβη της γενικότητας, μπορούμε να πάρομε $a = a' = 1$ και τώρα,

$$X^4 - 6X^3 + kX^2 + 3X + 4 = X^4 + (b + b')X^3 + (c + c' + bb')X^2 + (bc' + cb')X + cc' \,,$$

οπότε

$$b + b' = -6\,, \quad bc' + cb' = 3\,, \quad b + b' + cc' = k\,, \quad cc' = 4\,.$$

Από την τελευταία, λόγω του ότι οι c, c' είναι ακέραιοι, παίρνομε

$$(c, c') = (4, 1), (-4, -1), (2, 2), (-2, -2).$$

Οι δύο τελευταίες περιπτώσεις πρέπει να αποκλεισθούν, γιατί συνεπάγονται ότι $3 = bc' + cb' = \pm 2(b + b')$, αδύνατον, αφού οι b, b' είναι ακέραιοι. Αν $c = 4, c' = 1$, τότε, λύνοντας ως πρός b, b' το σύστημα των δύο πρώτων εξισώσεων, παίρνομε $b = -9, b' = 3$, οπότε η τρίτη σχέση δίνει $-22 = k$. Αν $c = -4, c' = -1$, τότε, με ανάλογο τρόπο βρίσκομε $b = -7, b' = 1$ και $-12 = k$.

Συμπέρασμα. Για $k \neq -2, -8, 7, -12, -22$ το $f(X)$ είναι ανάγωγο στο $\mathbb{Q}[X]$, ενώ για τίς

εξαιρεθείσες τιμές, το $f(X)$ παραγοντοποιείται ως εξής:

$$\begin{aligned} k=-2: &\quad f(X)=(X-1)(X^3-5X^2-7X-4)\\ k=-8: &\quad f(X)=(X+1)(X^3-7X^2-X+4)\\ k=7: &\quad f(X)=(X-4)(X^3-2X^2-X-1)\\ k=-12: &\quad f(X)=(X^2+X-1)(X^2-7X-4)\\ k=-22: &\quad f(X)=(X^2+3X+1)(X^2-9X+4) \end{aligned}$$

Πρόταση Γ'.4 (Κριτήριο Eisenstein)**.** *Έστω*

$$f(X)=a_nX^n+a_{n_1}X^{n-1}+\cdots+a_1X+a_0\in\mathbb{Z}[X],\ n\geq 2.$$

Αν υπάρχει πρώτος p ώστε να ισχύει

$$p|a_i \quad \textit{για όλα τα } i=0,1,\ldots,n-1\,,\quad p\nmid a_n\,,\quad p^2\nmid a_0,$$

τότε το $f(X)$ είναι ανάγωγο στο $\mathbb{Q}[X]$.

Μία άμεση, πολύ ενδιαφέρουσα εφαρμογή του κριτηρίου του Eisenstein είναι ότι, για κάθε ακέραιο $n\geq 2$, κάθε πρώτο p και κάθε ακέραιο a, ο οποίος δεν διαιρείται διά p, το πολυώνυμο X^n-pa είναι ανάγωγο στο $\mathbb{Q}[X]$.

Το παρακάτω τέχνασμα, παρά την απλότητά του, είναι πολύ χρήσιμο.

Πρόταση Γ'.5. *Έστω $c\in k$ και $f(X)\in K[X]$. Το $f(X)$ είναι ανάγωγο στο $K[X]$ αν, και μόνο αν, το $f(X+c)$ είναι ανάγωγο στο $K[X]$.*

Μία ενδιαφέρουσα εφαρμογή αυτού του τεχνάσματος, σε συνδυασμό με το κριτήριο του Eisenstein , είναι η εξής:

Πρόταση Γ'.6. *Έστω p πρώτος. Το p-τάξεως κυκλοτομικό πολυώνυμο $f_p(X)=X^{p-1}+\cdots+X+1$ είναι ανάγωγο στο $\mathbb{Q}[X]$.*

Πράγματι, είναι $f_p(X)=\dfrac{X^p-1}{X-1}$, οπότε

$$f_p(X+1)=\frac{(X+1)^p-1}{X}=X^{p-1}+\begin{pmatrix}p\\1\end{pmatrix}X^{p-2}+\cdots\begin{pmatrix}p\\p-1\end{pmatrix}.$$

Είναι γνωστή άσκηση της στοιχειώδους Θεωρίας Αριθμών ότι, για κάθε $k=1,\ldots,p-1$, ο διωνυμικός συντελεστής $\begin{pmatrix}p\\k\end{pmatrix}$ είναι πολλαπλάσιο του p. Άρα, το κριτήριο του Eisenstein , εφαρμόζεται στο τελευταίο πολυώνυμο (του οποίου ο σταθερός όρος ισούται με p), οπότε συμπεραίνομε ότι το $f_p(X+1)$ είναι ανάγωγο, άρα και το $f_p(X)$ είναι ανάγωγο στο $\mathbb{Q}[X]$.

Παράρτημα Δ΄

Συμμετρικά πολυώνυμα

Σε αυτό το Παράρτημα δίνομε την απόδειξη του Θεωρήματος 1.6.1. Στην πραγματικότητα, αποδεικνύομε κάτι περισσότερο· βλ. την εκφώνηση παρακάτω. Έστω R ένας δακτύλιος και μη μηδενικό $f \in R[X_1, \dots, X_n]$. Ορίζομε το *βάρος* του f ως εξής: Το βάρος ενός μονωνύμου $X_1^{j_1} \cdots X_n^{j_n}$ του f είναι, εξ ορισμού, ο αριθμός $j_1 + 2j_2 + \dots + nj_n$. Βάρος του f ορίζεται να είναι το μέγιστο των βαρών όλων των μονωνύμων πού εμφανίζονται στο f (εννοείται, με μη μηδενικό συντελεστή). Αν το f είναι σταθερό (μη μηδενικό), το βάρος του είναι 0. Θά αποδείξομε το θεμελιώδες θεώρημα των συμμετρικών πολυωνύμων υπό την εξής ακριβέστερη μορφή:

Θεώρημα Δ΄.1. *Έστω $f \in R[X_1, \dots, X_n]$ συμμετρικό βαθμού d. Τότε, για κάποιο $g \in R[X_1, \dots, X_n]$ βάρους $\leq d$, $f(X_1, \dots, X_n) = g(S_1, \dots, S_n)$, όπου $S_1, \dots, S_n$ είναι τα στοιχειώδη συμμετρικά πολυώνυμα των $X_1, \dots, X_n$.*

Απόδειξη. Με επαγωγή επί του n. Αν $n = 1$, ο ισχυρισμός του θεωρήματος είναι τετριμμένος.Υποθέτομε ότι αληθεύει για όλα τα συμμετρικά πολυώνυμα $n-1$ μεταβλητών ($n > 1$) κι άς θεωρήσομε ένα συμμετρικό πολυώνυμο $f(X_1, \dots, X_n) \in R[X_1, \dots, X_n]$. Με $S_1, \dots, S_n$ συμβολίζομε τα στοιχειώδη συμμετρικά πολυώνυμα των $X_1, \dots, X_n$ και με $S'_1, \dots, S'_{n-1}$ τα αντίστοιχα για τίς μεταβλητές $X_1, \dots, X_{n-1}$. Προφανώς, για κάθε $i = 1, \dots, n-1$,

$$S'_i(X_1, \dots, X_{n-1}) = S_i(X_1, \dots, X_{n-1}, 0)\ . \tag{Δ'.1}$$

Τώρα κάνομε επαγωγή επί του d. Για $d = 0$ δεν έχομε τίποτε να αποδείξομε. Έστω ότι $d \geq 1$ και το θεώρημα έχει ήδη αποδειχθεί για όλα τα πολυώνυμα του $R[X_1, \dots, X_{n-1}]$ βαθμού $< d$. Το $f(X_1, \dots, X_{n-1}, 0) \in R[X_1, \dots, X_{n-1}]$ είναι συμμετρικό πολυώνυμο οπότε, λόγω επαγωγικής υπόθεσης,

$$f(X_1, \dots, X_{n-1}, 0) = g_1(S'_1, \dots, S'_{n-1}) \tag{Δ'.2}$$

για κάποιο $g_1 \in R[X_1, \dots, X_{n-1}]$ βάρους $\leq d$. Αν $X_1^{j_1} \cdots X_{n-1}^{j_{n-1}}$ είναι το μονώνυμο του g_1 με το μέγιστο βάρος, τότε $j_1 + 2j_2 + \dots + (n-1)j_{n-1} \leq d$. Άς θεωρήσομε τώρα το πολυώνυμο $g_1(S_1, \dots, S_{n-1}) \in R[X_1, \dots, X_n]$. Αν το δούμε ως R-γραμμικό συνδυασμό όρων της μορφής

$S_1^{k_1}\cdots S_{n-1}^{k_{n-1}}$, ο όρος με το μέγιστο βαθμό (ως πρός $X_1,\dots,X_n$) είναι, προφανώς, ο $S_1^{j_1}\cdots S_{n-1}^{j_{n-1}}$. ο βαθμός του είναι, φυσικά, $j_1+2j_2+\dots+(n-1)j_{n-1}\le d$. Ορίζομε τώρα το πολυώνυμο

$$f_1(X_1,\dots,X_n)=f(X_1,\dots,X_n)-g_1(S_1,\dots,S_{n-1})\,, \tag{Δ'.3}$$

το οποίο είναι συμμετρικό, βαθμού $\le d$. Λόγω των (Δ'.1), (Δ'.2),

$$f_1(X_1,\dots,X_{n-1},0)=0\,,$$

πού σημαίνει ότι το f_1 διαιρείται από το X_n. Συνεπώς, λόγω συμμετρίας, το f_1, διαιρείται επίσης από τα $X_1,\dots,X_{n-1}$, άρα

$$f_1(X_1,\dots,X_n)=S_n\cdot f_2(X_1,\dots,X_n) \tag{Δ'.4}$$

για κάποιο $f_2\in R[X_1,\dots,X_n]$ συμμετρικό, βαθμού $\le d-n<d$. Η επαγωγική υπόθεση στο d συνεπάγεται ότι υπάρχει $g_2\in R[X_1,\dots,X_n]$ βάρους $\le d-n$, τέτοιο ώστε

$$f_2(X_1,\dots,X_n)=g_2(S_1,\dots,S_n)\,.$$

Η τελευταία σχέση, εν συνδυασμώ, με τίς (Δ'.3) και (Δ'.4) δίνουν

$$f(X_1,\dots,X_n)=g_1(S_1,\dots,S_{n-1})+g_2(S_1,\dots,S_n)\cdot S_n\,.$$

Το δεξιό μέλος προκύπτει όταν στο πολυώνυμο

$$g(X)\overset{ορσ}{=}g_1(X_1,\dots,X_{n-1})+g_2(X_1,\dots,X_n)\cdot X_n$$

τα $X_1,\dots,X_n$ αντικαταστηθούν από τα $S_1,\dots,S_n$, αντιστοίχως. Επιπλέον, το βάρος του g_1, όπως εἴδαμε παραπάνω, είναι $\le d$ και το βάρος του $g_2(X_1,\dots,X_n)\cdot X_n$ είναι $\le (d-n)+n\cdot 1\le n$. Συνεπώς το βάρος του g είναι $\le d$. □

Ασκήσεις

1. Εκφράστε τα πολυώνυμα $X_1^2+X_2^2$ και $X_1^3+X_2^3$ συναρτήσει των στοιχειωδών συμμετρικών πολυωνύμων $S_1=X_1+X_2, S_2=X_1X_2$.

2. Εκφράστε τα πολυώνυμα $X_1^2+X_2^2+X_3^2$ και $X_1^3+X_2^3+X_3^3$ συναρτήσει των στοιχειωδών συμμετρικών πολυωνύμων $S_1=X_1+X_2+X_3, S_2=X_1X_2+X_2X_3+X_3X_1, S_3=X_1X_2X_3$.

3. Αν u_1,u_2 είναι οι ρίζες του aX^2+bX+c, εκφράστε την παράσταση

$$(u_1-u_2)^2$$

συναρτήσει των a,b,c.

Υπόδειξη. Παρατηρήστε ότι η παράσταση αυτή είναι συμμετρική ως πρός τα u_1, u_2. Χρησιμοποιήστε, επίσης, τους τύπους του Viète για τίς σχέσεις ριζών και συντελεστών ενός πολυωνύμου.

4. Αν u_1, u_2, u_3 είναι οι ρίζες του $X^3 + pX + q$, εκφράστε την παράσταση

$$((u_1 - u_2)(u_1 - u_3)(u_2 - u_3))^2$$

συναρτήσει των p, q.

Υπόδειξη. Όπως και στην άσκηση 3.

Παράρτημα Ε΄

Εξισώσεις βαθμού 3 και 4

Θά ασχοληθούμε μέ τήν επίλυση πολυωνυμικών εξισώσεων τρίτου καί τετάρτου βαθμού μέ συντελεστές από ένα σώμα K χαρακτηριστικής $\neq 2, 3$.

Ε'.1 Η εξίσωση τριτου βαθμου.

Όπως εἴδαμε στήν ενότητα 1.5, αρκεί νά μπορούμε νά λύνομε τριτοβάθμιες εξισώσεις τής μορφής $x^3 + ax + b = 0$ (λείπει τό x^2). Άν x_1, x_2, x_3 είναι οι ρίζες της σε κάποια επέκταση του K, τότε

$$x_1 + x_2 + x_3 = 0 \ , \ x_1x_2 + x_2x_3 + x_3x_1 = a \ , \ x_1x_2x_3 = -b \ . \tag{Ε'.1}$$

Θέτομε

$$x = z - \frac{a}{3z} \ , \tag{Ε'.2}$$

οπότε η αρχική εξίσωση μετασχηματίζεται στήν $27z^6 + 27bz^3 - a^3 = 0$, η οποία είναι δευτεροβάθμια ως πρός z^3 καί λύνοντάς την παίρνομε

$$z^3 = -\frac{b}{2} + \epsilon\sqrt{R} \ , \ R = \left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3 \ , \ \epsilon \in \{-1, +1\} \ . \tag{Ε'.3}$$

Εδώ $\sqrt{R}$ υποδηλώνει οποιαδήποτε από τίς δύο τετραγωνικές ρίζες τού αριθμού R σε κάποια επέκταση του K. Έστω ζ μία οποιαδήποτε από τίς τρείς κυβικές ρίζες τού $-(b/2) + \epsilon\sqrt{R}$ σε κάποια επέκταση του K. Άν $\omega \neq 1$ είναι μία κυβική ρίζα τής μονάδος, τότε, λόγω τής (Ε'.3), οι πιθανές τιμές τού z είναι $\zeta, \omega\zeta, \omega^2\zeta$, άρα από τήν (Ε'.2), οι πιθανές τιμές γιά τό x είναι

$$\zeta - \frac{a}{3\zeta} \ , \ \zeta\omega - \frac{a}{3\zeta\omega} = \zeta\omega - \frac{a}{3\zeta}\omega^2 \ , \ \zeta\omega^2 - \frac{a}{3\zeta\omega^2} = \zeta\omega^2 - \frac{a}{3\zeta}\omega \ . \tag{Ε'.4}$$

ένας υπολογισμός (βλ. άσκηση 1) δείχνει ότι οι στοιχειώδεις συμμετρικές παραστάσεις τών τριών αριθμών στήν (Ε'.4) είναι ἴσες, αντιστοίχως, μέ $0, a, -b$. άρα, από τήν (Ε'.1) καί τήν άσκηση 2,

συμπεραίνομε ότι αυτοί οι αριθμοί είναι οι τρείς λύσεις τής εξισώσεως $x^3+ax+b=0$. Επειδή τό ίδιο αποτέλεσμα προκύπτει ανεξαρτήτως τού άν ϵ είναι 1 ή -1, συμπεραίνομε ότι μπορούμε στήν (Ε'.4) νά πάρομε, χωρίς βλάβη τής γενικότητος, $\epsilon=1$. Οι τρείς αριθμοί στήν (Ε'.4) γράφονται καί ως εξής:

$$\zeta\omega^j-\frac{a}{3\zeta}\omega^{2j}\ ,\ j\in\{0,1,2\}\ . \tag{Ε'.5}$$

Όπως είπαμε προηγουμένως, ζ είναι μία οποιαδήποτε κυβική ρίζα τού $-(b/2)+\sqrt{R}$. Αυτό τό γράφομε συμβολικώς

$$\zeta=\sqrt[3]{-\frac{b}{2}+\sqrt{R}}\ . \tag{Ε'.6}$$

Έστω τώρα ζ' μία οποιαδήποτε κυβική ρίζα τού $-(b/2)-\sqrt{R}$. Τότε,

$$(\zeta\zeta')^3=(-\frac{b}{2}+\sqrt{R})(-\frac{b}{2}-\sqrt{R})=\frac{b^2}{4}-R=\left(-\frac{a}{3}\right)^3\ .$$

Άρα, $\zeta\zeta'=-\omega^k a/3$ γιά κάποιο $k\in\{0,1,2\}$. Ο αριθμός $\omega^{-k}\zeta'$ είναι κυβική ρίζα τού $-(b/2)-\sqrt{R}$, τήν οποία συμβολίζομε

$$\sqrt[3]{-\frac{b}{2}-\sqrt{R}}\ . \tag{Ε'.7}$$

Δηλαδή δείξαμε ότι, άπαξ καί οριστεί (αυθαιρέτως) η τιμή τής (Ε'.6), η τιμή τής (Ε'.7) μπορεί νά επιλεγεί έτσι ώστε

$$\sqrt[3]{-\frac{b}{2}+\sqrt{R}}\cdot\sqrt[3]{-\frac{b}{2}-\sqrt{R}}=-\frac{a}{3}\ . \tag{Ε'.8}$$

Λόγω τής (Ε'.5) τώρα, οι τρείς ρίζες εκφράζονται από τούς παρακάτω *τύπους τού Cardano*

$$\omega^j\sqrt[3]{-\frac{b}{2}+\sqrt{R}}+\omega^{2j}\sqrt[3]{-\frac{b}{2}-\sqrt{R}}\ ,\qquad j=0,1,2\ ,$$

υπό τόν περιορισμό, οι τιμές τών κυβικών ριζών νά επιλέγονται έτσι ώστε νά ισχύει η (Ε'.8).

Σημείωση: Παρατηρήστε ότι $R=-D/108$, όπου D η διακρίνουσα τού πολυωνύμου X^3+aX+b (βλ. άσκηση 1.4.2).

Ε'.2 Η εξίσωση τεταρτου βαθμου

Γράφομε τή γενική τεταρτοβάθμια εξίσωση μέ τή μορφή

$$f(x)=x^4+4ax^3+6bx^2+4cx+d=0 \tag{Ε'.9}$$

καί επιδιώκομε νά εκφράσομε τό πολυώνυμο $f(X)$ ως διαφορά τετραγώνων. Θέτομε

$$h_1(X) = 2mX + n \ , \ h_2(X) = X^2 + 2aX + b + 2l \ , \tag{Ε'.10}$$

όπου l, m, n είναι παράμετροι, πού θά προσδιορίσομε, από τήν απαίτηση νά ισχύει

$$f(X) = h_2(X)^2 - h_1(X)^2 \ . \tag{Ε'.11}$$

Η (Ε'.11) γράφεται

$$(2mX + n)^2 = 4(l + a^2 - b)X^2 + 4(ab + 2al - c)X + (b + 2l)^2 - d \ , \tag{Ε'.12}$$

η οποία λέει ότι τό δεξιό μέλος είναι τέλειο τετράγωνο, οπότε η διακρίνουσά του είναι 0:

$$4(ab + 2al - c)^2 - 4(l + a^2 - b)[(b + 2l)^2 - d] = 0 \ .$$

ύστερα από τίς πράξεις καταλήγομε στήν

$$4l^3 - g_2 l + g_3 = 0 \ , \tag{Ε'.13}$$

όπου g_2, g_3 είναι οι λεγόμενες *αναλλοίωτες* (βλ. άσκηση 3) τού $f(X)$:

$$g_2 = d - 4ac + 3b^2 \ , \ g_3 = bd + 2abc - b^3 - c^2 - a^2 d = \begin{vmatrix} 1 & a & b \\ a & b & c \\ b & c & d \end{vmatrix} \ . \tag{Ε'.14}$$

Αρκεί, λοιπόν, νά βρούμε μία οποιαδήποτε λύση l τής *επιλύουσας* τριτοβάθμιας εξίσωσης (Ε'.13) καί μετά νά προσδιορίσομε τά m, n από τήν πολυωνυμική ισότητα (Ε'.12), δηλαδή,

$$m^2 = l + a^2 - b \ , \ mn = ab + 2al - c \ , \ n^2 = (b + 2l)^2 - d \ . \tag{Ε'.15}$$

Προσδιορίζοντας κατ" αυτόν τόν τρόπο, τά l, m, n μπορούμε, στή συνέχεια, λόγω τής (Ε'.10), νά γράψομε τήν (Ε'.9) ως $(h_2(x) + h_1(x))(h_2(x) - h_1(x)) = 0$, ανάγοντας τήν επίλυσή της στήν επίλυση δύο δευτεροβαθμίων εξισώσεων.

Ε'.3 Η ΔΙΑΚΡΙΝΟΥΣΑ ΕΝΟΣ ΠΟΛΥΩΝΥΜΟΥ

Έστω τό πολυώνυμο

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots a_1 X + a_0$$

μέ συντελεστές από οποιοδήποτε σώμα καί $x_1, \dots, x_n$ οι ρίζες του σέ κάποια κατάλληλη επέκταση (σώμα ριζών). Ορίζομε ως *διακρίνουσα* τού $f(X)$ τήν ποσότητα

$$D = \prod_{1 \le i < j \le n} (x_i - x_j)^2 \ .$$

Παρατηρούμε ότι $D \in \mathbb{Z}[x_1, \dots, x_n]$ καί είναι συμμετρική παράσταση τών $x_1, \dots, x_n$, άρα από τό Θεώρημα Δ΄.1 καί τούς τύπους τού Vète συμπεραίνομε ότι $D \in \mathbb{Z}[a_1, \dots, a_n]$, δηλαδή,

> Η διακρίνουσα τού $f(X)$ είναι πολυωνυμική έκφραση τών $a_1, \dots, a_n$ μέ ακέραιους συντελεστές.

Επίσης, παρατηρούμε ότι

> Η διακρίνουσα τού $f(X)$ είναι μηδέν, άν καί μόνο άν, τό $f(X)$ έχει μία τουλάχιστον πολλαπλή ρίζα.

Η διακρίνουσα τού $f(X) = X^2 + aX + b$ είναι $(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = (-a)^2 - 4b = a^2 - 4b$, ενώ από τά εκτεθέντα στήν ενότητα 1.5, η διακρίνουσα τού $X^3 + aX + b$ είναι $-4a^3 - 27b^2$.

Παρακάτω θά υπολογίσομε τή διακρίνουσα τού πολυωνύμου $X^4 + 4aX^3 + 6bX^2 + 4cX + d$. Χρειαζόμαστε πρώτα τό εξής λήμμα:

Λήμμα Ε΄.3.1. *Έστω $f_1(X) = X^2 + aX + b$, $f_2(X) = X^2 + cX + d$ καί $f(X) = f_1(X)f_2(X)$. Άν x_1, x_2 είναι οι ρίζες τού $f_1(X)$ τότε η διακρίνουσα τού $f(X)$ είναι*

$$D = D_1 D_2 (f_2(x_1) f_2(x_2))^2 \ ,$$

όπου D_1, D_2 οι διακρίνουσες τών $f_1(X), f_2(X)$, αντιστοίχως.

Απόδειξη. Άς συμβολίσομε μέ x_3, x_4 τίς ρίζες τού $f_2(X)$. Είναι $D_1 = (x_1 - x_2)^2$, $D_2 = (x_3 - x_4)^2$ καί $x_3 + x_4 = -c$, $x_3x_4 = d$. Οι ρίζες τού $f(X)$ είναι $x_1, \dots, x_4$, άρα

$$\begin{aligned} D &= [(x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)]^2 \\ &= (x_1 - x_2)^2 (x_3 - x_4)^2 [(x_1 - x_3)(x_1 - x_4)]^2 [(x_2 - x_3)(x_2 - x_4)]^2 \\ &= D_1 D_2 [x_1^2 - (x_3 + x_4)x_1 + x_3x_4]^2 [x_2^2 - (x_3 + x_4)x_2 + x_3x_4]^2 \\ &= D_1 D_2 (x_1^2 + cx_1 + d)^2 (x_2^2 + cx_2 + d)^2 \\ &= D_1 D_2 (f_2(x_1) f_2(x_2))^2 \end{aligned}$$

□

Έστω τώρα $f(X) = X^4 + 4aX^3 + 6bX^2 + 4cX + d$. Σύμφωνα μέ τήν προηγούμενη ενότητα, $f(X) = f_1(X)f_2(X)$, όπου $f_1(X) = h_2(X) + h_1(X)$, $f_2(X) = h_2(X) - h_1(X)$ καί τά $h_1(X), h_2(X)$ δίνονται από τήν Ε΄.10. Άν D_1, D_2 είναι, αντιστοίχως, οι διακρίνουσες τών $f_1(X), f_2(X)$,

$$D_1 = 4[(a + m)^2 - (b + n + 2l)] \ , \ D_2 = 4[(a - m)^2 - (b - n + 2l)] \ .$$

Επίσης, $f_1(x_1) = 0 = f_1(x_2)$, άρα $h_2(x_1) = -h_1(x_1)$ καί $h_2(x_2) = -h_1(x_2)$. Συνεπώς, $f_2(x_1) = h_2(x_1) - h_1(x_1) = -2h_1(x_1)$ καί, ανάλογα, $f_2(x_2) = -2h_1(x_2)$, οπότε, σύμφωνα μέ τό Λήμμα E'.3.1,

$$D = 2^8[(a+m)^2 - (b+n+2l)][(a-m)^2 - (b-n+2l)](2mx_1+n)(2mx_2+n) \; .$$

Τά x_1, x_2, ως ρίζες τού $f_1(X)$, ικανοποιούν τίς σχέσεις $x_1+x_2 = -2(a+m), x_1x_2 = b+n+2l$, οπότε $(2mx_1+n)(2mx_2+n) = 4m^2(b+n+2l) - 4mn(a+m) + n^2$ καί η D, ύστερα από κάποιες πράξεις παίρνει τή μορφή

$$\begin{aligned} D &= 2^8[(a+m)^2 - (b+n+2l)][(a-m)^2 - (b-n+2l)] \\ &\quad \times[4m^2(b+n+2l) - 4mn(a+m) + n^2]^2 \\ &= 2^8[(b+2l)^2 - 2(a^2+m^2)(b+2l) + (a^2-m^2)^2 + 4amn - n^2] \\ &\quad \times[4m^2(b+2l) - (4amn - n^2)]^2 \; . \end{aligned}$$

Λόγω τών (E'.13) καί (E'.14) έχομε $4l^3 = g_2l - g_3$ καί $4l^4 = g_2l^2 - g_3l$. Επίσης, ισχύουν οι (E'.15), οπότε, μετά τίς πράξεις βρίσκομε

$$D = 2^8(-3l^2 + g_2)(12l^2 - g_2)^2 = 2^8(g_2^3 - 27g_3^2) \; .$$

Αποδείξαμε έτσι τό εξής θεώρημα.

Θεώρημα Ε′.3.2. *Η διακρίνουσα τού πολυωνύμου* $X^4 + 4aX^3 + 6bX^2 + 4cX + d$ *είναι*

$$D = 2^8(g_2^3 - 27g_3^2) \; ,$$

όπου τά g_2, g_3 *δίνονται από τήν (Ε′.14)*

Παρατήρηση. Η διακρίνουσα τού κυβικού πολυωνύμου $X^3 - (g_2/4)X + (g_3/4)$, τό οποίο έχει ως ρίζες τίς λύσεις τής επιλύουσας (E'.13), είναι $4(g_2/4)^3 - 27(g_3/4)^2) = 2^{-4}(g_2^3 - 27g_3^2)$, άρα

> Η διακρίνουσα τού τεταρτοβαθμίου πολυωνύμου ισούται μέ 2^{12} φορές τή διακρίνουσα τού αντιστοίχου επιλύοντος κυβικού πολυωνύμου.

Ασκήσεις

1. Αποδείξτε ότι οι στοιχειώδεις συμμετρικές παραστάσεις τών τριών αριθμών στήν (E'.4) είναι ίσες μέ $0, a, -b$, αντιστοίχως.

2. Άς υποθέσομε ότι $x_1, \ldots, x_n$ καί $y_1, \ldots, y_n$ είναι στοιχεία ενός σώματος καί οι στοιχειώδεις συμμετρικές παραστάσεις τής πρώτης n-άδας είναι ίσες μέ τίς αντίστοιχες τής δεύτερης n-άδας. Δείξτε τότε ότι η δεύτερη n-άδα αποτελεί μετάθεση τής πρώτης. (Υπόδειξη: Θεωρήστε τά πολυώνυμα μέ ρίζες $x_1, \ldots, x_n$ καί $y_1, \ldots, y_n$, αντιστοίχως. Εφαρμόστε τούς τύπους τού Viète.)

3. Η ονομασία *αναλλοίωτες* γιά τίς παραστάσεις g_2, g_3 δικαιολογείται από τό ότι, άν στήν εξίσωση Ε'.9 γίνει η αλλαγή μεταβλητής $x = y + k$, στή νέα, ως πρός y, εξίσωση πού θά προκύψει, θά αντιστοιχούν g_2, g_3 ίσα μέ τά αρχικά. Αποδείξτε αυτό τόν ισχυρισμό.

4. Αυτή η άσκηση περιγράφει ένα κάπως διαφορετικό τρόπο επιλύσεως τής (Ε'.9). Δείξτε ότι η αλλαγή μεταβλητής $x = y - a$ μετασχηματίζει τήν (Ε'.9) σέ εξίσωση τής μορφής $y^4+py^2+qy+r = 0$ καί γράψτε τό αριστερό μέλος τής τελευταίας ως διαφορά τετραγώνων μέ τόν εξής τρόπο: Παρατηρήστε ότι, γιά κάθε l, ισχύει η ταυτότητα

$$y^4 + py^2 + qy + r = \left(y + \frac{l}{2}\right)^2 - \left\{(l-p)y^2 - qy + \left(\frac{l^2}{4} - r\right)\right\}$$

καί βρείτε κατάλληλο l, ώστε η παράσταση μέσα στά άγκυστρα νά γίνεται τέλειο τετράγωνο. Εφαρμόστε τήν παραπάνω μέθοδο γιά τήν επίλυση μιάς συγκεκριμένης τεταρτοβάθμιας εξίσωσης πού θά διαλέξετε. Τήν ίδια εξίσωση επιλύστε καί μέ τή μέθοδο πού περιγράφεται στή Θεωρία.