ΤΣΙΤΣΙΝΑΚΗ ΣΤΑΜΑΤΙΝΑ

ΘΕΩΡΙΑ GALOIS

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Πανεπιστήμιο Αιγαίου, Τμήμα Μαθηματικών
Σάμος Ιούνιος 2005

Περιεχόμενα

Κεφάλαιο 1

Παραγοντοποίηση πολυωνύμων

1.1 Αναγωγισιμότητα

Ορισμός 1.1.1 *Ένα πολυώνυμο με συντελεστές από ένα μεταθετικό δακτύλιο λέγεται παραγοντοποιήσιμο αν είναι το γινόμενο δύο πολυωνύμων μικρότερου βαθμού. Διαφορετικά λέγεται ανάγωγο. Στο εξής θα συμβολίζουμε τον βαθμό ενός πολυωνύμου g με ∂g.*

Παράδειγμα 1.1.1 *Όλα τα πολυώνυμα βαθμού 0 ή 1 είναι ανάγωγα αφού δεν μπορούν να εκφραστούν σαν γινομενο πολυωνύμων μικρότερου βαθμού.*

Παράδειγμα 1.1.2 *Το πολυώνυμο t^2-2 είναι ανάγωγο στο $\mathbb{Q}$. Για να το αποδείξουμε υποθέτουμε ότι είναι παραγοντοποιήσιμο. Δηλαδή έστω ότι το πολυώνυμο γράφεται:*

$$t^2-2=(at+b)(ct+d)$$

όπου τα a, b, c, $d\in\mathbb{Q}$. Δηλαδή

$$t^2-2=act^2+(ad+bc)t+bd.$$

Θα πρέπει να ισχύει $ac=1$, $ad+bc=0$ και $bd=-2$. Υποθέτουμε ότι $a=c=1$. Άρα θα έχουμε $b=-d$ δηλαδή $b^2=2$. Αυτό όμως δεν συμβαίνει για κανένα ρητό αριθμό. Επομένως το παραπάνω πολυώνυμο είναι ανάγωγο.

Παράδειγμα 1.1.3 *Το πολυώνυμο t^2-2 είναι παραγοντοποιήσιμο στο $\mathbb{R}$ αφού γραφεται*

$$t^2-2=(t-\sqrt{2})(t+\sqrt{2}).$$

Αυτό μας δείχνει ότι ένα πολυώνυμο που είναι ανάγωγο σ'ενα σώμα μπορεί να είναι παραγοντοποιήσιμο σ'ενα μεγαλύτερο σώμα.

Κάθε παραγοντοποιήσιμο πολυώνυμο μπορεί να γραφεί ως το γινόμενο δύο πολυωνύμων μικρότερου βαθμού. Αν κάποιο από αυτά είναι επίσης παραγοντοποιήσιμο, μπορεί να διασπαστεί σε δύο παράγοντες μικρότερου βαθμού κ.τ.λ. Αυτή η διαδικασία θα τερματιστεί όταν κανένας από τους παράγοντες δεν μπορεί να γραφεί ως γινόμενο πολυωνύμων μικρότερου βαθμού. Αυτή είναι η ιδέα που θα χρησιμοποιήσουμε για να αποδείξουμε το παρακάτω θεώρημα.

Θεώρημα 1.1.1 *Κάθε μη μηδενικό πολυώνυμο με συντελεστές από ένα σώμα K είναι γινόμενο ανάγωγων πολυωνύμων με συντελεστές από το K.*

Απόδειξη: Έστω g ένα μη-μηδενικό πολυώνυμο με συντελεστές απο το K. Θα αποδείξουμε το θεώρημα με επαγώγη στο βάθμο του g. Έστω οτι $\partial g = 0$ ή 1. Τότε το g είναι ανάγωγο. Σε αυτή την περίπτωση το g γράφεται στη μορφή $1g$ που είναι γινόμενο ανάγωγων πολυωνύμων. Αν $\partial g > 1$ τότε ή το g είναι ανάγωγο ή $g = hj$, όπου $\partial h, \partial j < \partial g$. Συνεχίζουμε την ίδια διαδικασία για τα h, j. Επαγωγικά καταλήγουμε ότι τα πολυώνυμα h και j είναι γινόμενα ανάγωγων πολυωνύμων άρα και το g είναι γινόμενο ανάγωγων πολυωνύμων.□

Ορισμός 1.1.2 *Ένα πολυώνυμο d με συντελεστές από ένα σώμα K λέγεται μέγιστος κοινός διαιρέτης (Μ.Κ.Δ) των f και g αν $d|f$ και $d|g$ και επιπλέον αν $e|f$ και $e|g$ τότε $e|d$. Αν d είναι μέγιστος κοινός διαιρέτης των f, g τότε και ο kd $(k \neq 0 \in K)$ είναι μέγιστος κοινός διαιρέτης των f, g.*

Θεώρημα 1.1.2 *Έστω f και g μη μηδενικά πολυώνυμα με συντελεστές από ένα σώμα K. Τότε υπάρχει ο μέγιστος κοινός διαιρέτης, έστω d των f και g και υπάρχουν πολυώνυμα a και b με συντελεστές από το K έτσι ώστε:*

$$d = af + bg.$$

Απόδειξη: Έστω $f = r_{-1}$, $g = r_0$. Χρησιμοποιώντας τον αλγόριθμο του Ευκλείδη βρίσκουμε πολυώνυμα q_i, r_i με συντελεστές από το K έτσι ώστε

$$\begin{aligned}
r_{-1} &= q_1 r_0 + r_1 && \partial r_1 < \partial r_0 && (1.1)\\
r_0 &= q_2 r_1 + r_2 && \partial r_2 < \partial r_1 && (1.2)\\
r_1 &= q_3 r_2 + r_3 && \partial r_3 < \partial r_2 && (1.3)\\
&\dots\\
r_i &= q_{i+2} r_{i+1} + r_{i+2} && \partial r_{i+2} < \partial r_{i+1} && (1.4)\\
&\dots
\end{aligned}$$

Η παραπάνω διαδικασία θα σταματήσει όταν το υπόλοιπο γίνει μηδέν, δηλαδή όταν $r_{s+2} = 0$. Επομένως θα έχουμε την σχέση

$$r_s = q_{s+2} r_{s+1} \tag{1.5}$$

Ισχυριζόμαστε ότι το r_{s+1} είναι ένας μέγιστος κοινός διαιρέτης για τα πολυώνυμα f και g. Θα το αποδείξουμε. Θα δείξουμε ότι το r_{s+1} διαιρεί και το f και το g. Θα δέιξουμε ότι το $r_{s+1}|r_i$ για κάθε i. Φανερά, $r_{s+1}|r_{s+1}$. Από την σχέση (1.5) το $r_{s+1}|r_s$. Αν συνεχίσουμε την ίδια διαδικασία επαγωγικά βασιζόμενοι στις παραπάνω σχέσεις θα καταλήξουμε ότι $r_{s+1}|r_{i+2}$ και $r_{s+1}|r_{i+1}$ και τελικά $r_{s+1}|r_i$. Εφόσον το $r_{s+1}|r_i$ για κάθε i τότε $r_{s+1}|r_0 = g$ και $r_{s+1}|r_{-1} = f$. Υποθέτουμε ότι $e|f$ και $e|g$. Από την σχέση (1.4) προκύπτει επαγωγικά ότι το $e|r_i$. Επομένως προκύπτει ότι $e|r_{s+1}$. Άρα δείξαμε ότι το r_{s+1} είναι ο μέγιστος κοινός διαιρέτης των f, g.
Υποθέτουμε ότι υπάρχουν πολυώνυμα a_i, b_i έτσι ώστε

$$d = a_i r_i + b_i r_{i+1}$$

Αυτό ισχύει όταν $i = s + 1$ άρα παίρνουμε $a_i = 1$ και $b_i = 0$. Από την σχέση (1.4) έχουμε

$$r_{i+1} = r_{i-1} - q_{i+1} r_i.$$

Άρα επαγωγικά έχουμε

$$d = a_i r_i + b_i (r_{i-1} - q_{i+1} r_i)$$

επομένως αν θέσουμε

$$a_{i-1} = b_i$$

$$b_{i-1} = a_i - b_i q_{i+1}$$

έχουμε

$$d = a_{i-1} r_{i-1} + b_{i-1} r_i.$$

Και αν συνεχίσουμε αυτήν την διαδικασία επαγωγικά στις αρχικές σχέσεις παίρνουμε

$$\begin{aligned} d &= a_{-1} r_{-1} + b_{-1} r_0 \\ &= af + bg \end{aligned}$$

όπου $a = a_{-1}$, $b = b_{-1}$.□

Ορισμός 1.1.3 *Αν f και g είναι πολυώνυμα με συντελεστές από ένα σώμα K και μέγιστο κοινο διαιρέτη την μονάδα του δακτυλίου $K[x]$ τότε τα f και g λέμε ότι είναι πρώτα μεταξύ τους.*

Λήμμα 1.1.1 *Αν K είναι ένα σώμα, f είναι ένα ανάγωγο πολυώνυμο με συντελεστές από το K και g, h είναι πολυώνυμα με συντελεστές από το K έτσι ώστε το f να διαιρεί το gh, τότε το f διαιρεί είτε το g είτε το h.*

Απόδειξη: Έστω ότι το $f \not| g$. Ισχυριζόμαστε ότι τα f και g είναι πρώτα μεταξύ τους. Αν f, g δεν είναι πρώτα μεταξύ τους τότε έστω d να είναι ο μέγιστος κοινός διαιρέτης των f και g. Εφόσον το f είναι ανάγωγο και το $d|f$ ισχύει ότι είτε $d = kf$ $(k \in K)$ είτε $d = k \in K$. Αν $d = kf$ έχουμε ότι $d|g$ άρα $kf|g$ δηλαδή $f|g$ που είναι άτοπο από την υπόθεση. Αν $d = k \in K$, το 1 είναι ο μέγιστος κοινός διαιρέτης των f, g συνεπώς τα f και g είναι πρώτα μεταξύ τους. Τότε από το θεώρημα 1.1.2 υπάρχουν πολυώνυμα a, b με συντελεστές από το K έτσι ώστε:

$$1 = af + bg$$

οπότε

$$h = haf + hbg.$$

Το $f|haf$ και το $f|hbg$ εφόσον το $f|gh$. Άρα το $f|h$. Αν υποθέσουμε ότι το $f \not| h$ θα καταλήξουμε με την ίδια λογική ότι πρέπει το $f|g$.□

Θεώρημα 1.1.3 *Για κάθε σώμα K, η παραγοντοποίηση των πολυωνύμων με συντελεστές απο το K σε ανάγωγα πολυώνυμα είναι μοναδική αν δεν λάβουμε υπόψιν τους σταθερους παράγοντες και την σειρά με την οποία είναι γραμμένοι οι ανάγωγοι παράγοντες.*

Απόδειξη: Υποθέτουμε ότι $f = f_1 \dots f_r = g_1 \dots g_s$ όπου το f είναι ένα πολυώνυμο με συντελεστές από το K και $f_1, \dots, f_r, g_1, \dots, g_s$ είναι ανάγωγα πολυώνυμα με συντελεστές από το K. Αν όλα τα f_i είναι σταθεροί όροι τότε το $f \in K$ οπότε και όλα τα g_j είναι σταθεροί όροι. Άρα το f γράφεται σαν γινόμενα σταθερών όρων μόνο και το θεώρημα ισχύει. Αλλιώς μπορούμε να θεωρήσουμε ότι κανενα από τα f_i δεν είναι σταθερός όρος διότι μπορούμε να διαγράψουμε τους σταθερούς όρους από τα δύο μέλη της παραπάνω εξίσωσης. Αυτό μπορεί να συμβεί γιατί το K είναι σώμα και για κάθε σταθερό όρο υπάρχει ο αντίστροφός του. Το $f_1|g_1 \dots g_s$. Από το λήμμα 1.1.1 καταλήγουμε στο συμπέρασμα οτι το $f_1|g_i$ για κάποια $i \in K$. Επιλέγουμε $i = 1$ αφού δεν μας ενδιαφέρει η σειρά των ανάγωγων παραγόντων και έχουμε ότι το $f_1|g_1$. Εφόσον τα f_1, g_1 είναι ανάγωγα και το f_1 δεν είναι σταθερός όρος θα πρέπει να ισχύει $f_1 = k_1 g_1$ για κάποιο σταθερό όρο $k_1 \in K$. Ομοίως έχουμε $f_2 = k_2 g_2, \dots, f_r = k_r g_r$ όπου $k_2, \dots, k_r \in K$. Το υπόλοιπο $g_j (j > r)$ θα πρέπει να είναι σταθερός όρος έστω k διαφορετικά ο βαθμός στο αριστερό μέλος της εξίσωσης θα ήταν μεγαλύτερος από τον βαθμό στο δεξιό μέλος,

κάτι που δεν μπορεί να ισχύει. Άρα δείξαμε ότι $f_1 \dots f_r = kk_1g_1k_2g_2 \dots k_rg_r$ άρα τελικά $f = f_1 \dots f_r = kk_1g_1k_2g_2 \dots k_rg_r$ και $f = g_1 \dots g_s = kg_1g_2 \dots g_r$ και το θεώρημα αποδείχτηκε.□

1.2 Κριτήρια αναγωγισιμότητας

Είναι πολυ δύσκολο να πούμε πότε ένα δεδομένο πολυώνυμο είναι ανάγωγο ή παραγοντοποιήσιμο. Για παράδειγμα αν μας δοθεί το πολυώνυμο:

$$t^{16}+t^{15}+t^{14}+t^{13}+t^{12}+t^{11}+t^{10}+t^9+t^8+t^7+t^6+t^5+t^4+t^3+t^2+t+1$$

δεν μπορουμε εύκολα να ελέξουμε αν παραγοντοποιείται με δοκιμές γιατι θα χρειαζόταν πολλές πράξεις και πολύς χρόνος. Για το λόγο αυτό θα δούμε κάποια κριτήρια που απλοποιούν τέτοιου είδους προβλήματα.

Λήμμα 1.2.1 ***(Gauss)*** *Έστω f ένα πολυώνυμο με συντελεστές από το $\mathbb{Z}$ το οποίο είναι ανάγωγο στο $\mathbb{Z}$. Τότε το f, ως πολυώνυμο με συντελεστές από το $\mathbb{Q}$, είναι επίσης ανάγωγο στο $\mathbb{Q}$.*

Απόδειξη: Όταν έχουμε ένα πολυώνυμο με συντελεστές από το $\mathbb{Z}$ και θέλουμε να το μελετήσουμε στο $\mathbb{Q}$ παρατηρούμε πως υπάρχουν πολλά νέα πολυώνυμα τα οποία φαίνεται πως θα μπορούσαν να είναι παράγοντες του f. Στην πραγματικότητα δεν συμβαίνει αυτό και θα το αποδείξουμε. Θεωρούμε f ένα πολυώνυμο που είναι ανάγωγο στο $\mathbb{Z}$ αλλά είναι παραγοντοποιήσιμο στο $\mathbb{Q}$ οπότε στο $\mathbb{Q}$ γράφεται $f = gh$ όπου g, h είναι πολυώνυμα πάνω από το $\mathbb{Q}$ με $\partial g, \partial h < \partial f$. Αν πολλαπλασιάσουμε και τα δύο μέλη της παραπάνω εξίσωσης με το γινόμενο των παρονομαστών των συντελεστών των h και g θα πάρουμε το

$$nf = g^{'}h^{'}$$

όπου $n \in \mathbb{Z}$ και $g^{'}, h^{'}$ είναι πολυώνυμα με συντελεστές από το $\mathbb{Z}$. Θα δείξουμε τώρα ότι μπορούμε να διαγράψουμε τους πρώτους παράγοντες του n έναν προς έναν χωρίς να βρεθούμε έξω από το $\mathbb{Z}[t]$. Έστω ότι το p είναι ένας πρώτος παράγοντας του n. Ισχυριζόμαστε ότι αν

$$g^{'} = g_0 + g_1t + \ldots + g_rt^r$$

$$h^{'} = h_0 + h_1t + \ldots + h_st^s$$

τότε το p διαιρεί όλους τους συντελεστες g_i ή το p διαιρεί όλους τους συντελεστες h_j. Έστω i, j οι μικρότερες τιμές έτσι ώστε $p \not| g_i$ και $p \not| h_j$. Όμως το p διαιρει τον συντελεστή του t^{i+j} στο $g^{'}h^{'}$, ο οποίος είναι

$$h_0g_{i+j} + h_1g_{i+j-1} + \ldots + h_jg_i + \ldots + h_{i+j}g_0$$

και από την επιλόγη των i και j ο πρώτος p διαιρει κάθε όρο αυτής της έκφρασης εκτός ίσως από το $h_j g_i$. Όμως το p διαιρεί όλη την έκφραση άρα $p|h_j g_i$. Όμως $p \not| h_j$ και $p \not| g_i$ που είναι άτοπο. Άρα ισχύει ο ισχυρισμός μας ότι το p διαιρεί όλους τους συντελεστές g_i ή το p διαιρεί όλους τους συντελεστες h_j. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι το p διαιρεί όλους τους συντελεστες g_i. Τότε $g^{'} = pg^{''}$ όπου το $g^{''}$ είναι πολυώνυμο στο $\mathbb{Z}$ ίδιου βαθμού με το $g^{'}$(ή το g). Έστω $n = pn_1$. Τότε

$$pn_1 f = pg^{''}h^{'}$$

και άρα

$$n_1 f = g^{''}h^{'}.$$

Συνεχίζοντας αυτή την διαδικασία μπορούμε να διαγράψουμε όλους τους πρώτους παράγοντες του n και να καταλήξουμε στην σχέση:

$$f = \bar{g}\bar{h}$$

όπου τα $\bar{g}$, $\bar{h}$ είναι πολυώνυμα στο $\mathbb{Z}$ και είναι ρητά πολλαπλάσια των g, h. Αυτό όμως έρχεται σε αντίθεση με την αναγωγιμότητα του f στο $\mathbb{Z}$. Άρα το f είναι ανάγωγο στο $\mathbb{Q}$.□

Θεώρημα 1.2.1 *(**Το κριτήριο αναγωγιμότητας του Eisenstein**).*
Έστω

$$f(t) = a_0 + a_1 t + \ldots + a_n t^n$$

ένα πολυώνυμο με συντελεστές από το $\mathbb{Z}$. Αν υπάρχει πρώτος p έτσι ώστε:

1. $p \not| a_n$
2. $p|a_i$ $(i = 0, \ldots, n-1)$
3. $p^2 \not| a_0$

τότε το f είναι ανάγωγο σαν πολυώνυμο με συντελεστές από το $\mathbb{Q}$.

Απόδειξη: Από την προταση 2.1.1 αρκεί να δείξουμε ότι το πολυώνυμο f είναι ανάγωγο στο $\mathbb{Z}$. Υποθέτουμε ότι το πολυώνυμο δεν είναι ανάγωγο, επομένως γράφεται στη μορφή $f = gh$ όταν

$$g = b_0 + b_1 t + \ldots + b_r t^r$$

$$h = c_0 + c_1 t + \ldots + c_s t^s$$

είναι πολυώνυμα μικρότερου βαθμού από το f στο $\mathbb{Z}$. Οπότε πρέπει να ισχύει $r+s=n$. Επίσης ισχύει $b_0c_0=a_0$. Έστω ότι υπάρχει πρώτος p ώστε να ισχύουν οι προυποθέσεις (1), (2), (3) του θεωρήματος. Επομένως πρέπει $p|b_0$ ή $p|c_0$. Από την προυπόθεση (3) συμπεραίνουμε ότι το p δεν μπορεί να διαιρεί και το b_0 και το c_0 γιατί θα είχαμε τότε ότι $p^2|a_0$. Άρα χωρίς βλάβη της γενικότητας μπορώ να θεωρήσω ότι $p|b_0, p\not|c_0$. Αν το $p|b_i, \forall i$ τότε $p|a_n=b_rc_s$ το οποίο δεν ισχύει από την προυπόθεση (1). Επομένως έστω ότι b_i είναι ο πρώτος συντελεστής του g που δεν διαιρείται από το p. Τότε

$$a_i = b_ic_0 + \ldots + b_0c_i$$

όταν $i<n$. Εφόσον το $p|a_i, b_0, \ldots, b_{i-1}$ θα πρέπει το p να διαιρεί και το c_0 το οποίο είναι άτοπο εφόσον υποθέσαμε ότι $p\not|c_0$. Άρα το f είναι ανάγωγο.□

Παράδειγμα 1.2.1 *Έστω το πολυώνυμο*

$$f(t) = \frac{2}{9}t^5 + \frac{5}{3}t^4 + t^3 + \frac{1}{3}$$

με συντελεστές από το $\mathbb{Q}$. *Είναι ανάγωγο αν και μόνο αν το πολυώνυμο*

$$g = 9f(t) = 2t^5 + 15t^4 + 9t^3 + 3$$

είναι ανάγωγο στο $\mathbb{Q}$. *Σύμφωνα με το κριτήριο του Eisenstein και για* $q=3$ *συμπεραίνουμε ότι το* g *είναι ανάγωγο. Επομένως και το* f *είναι ανάγωγο.*

Παράδειγμα 1.2.2 *Έστω το πολυώνυμο*

$$f(t) = t^{16}+t^{15}+t^{14}+t^{13}+t^{12}+t^{11}+t^{10}+t^9+t^8+t^7+t^6+t^5+t^4+t^3+t^2+t+1.$$

Δεν είναι εύκολο να πούμε αν είναι ανάγωγο ή όχι. Όμως είναι φανερό πως το πολυώνυμο είναι ανάγωγο αν και μόνο αν το πολυώνυμο $f(t+1)$ *είναι ανάγωγο. Έστω ότι έχουμε ένα ανάγωγο πολυώνυμο*

$$f(t) = a_0 + a_1t + \ldots + a_nt^n.$$

Τότε

$$f(t+1) = a_0 + a_1(t+1) + \ldots + a_n(t+1)^n.$$

Θέτουμε $t+1=x$ *και έχουμε*

$$f(x) = a_0 + a_1x + \ldots + a_nx^n$$

το οποίο είναι προφανώς ανάγωγο αφού και το $f(t)$ *είναι ανάγωγο. Από το διώνυμο του Νεύτωνα γνωρίζουμε ότι*

$$\begin{aligned}(a+b)^n &= \binom{n}{0}a^n b^0 + \binom{n}{1}a^{n-1}b^1 + \binom{n}{2}a^{n-2}b^2 \\ &+ \ldots + \binom{n}{n-1}a^1 b^{n-1} + \binom{n}{n}a^0 b^n\end{aligned}$$

Άρα έχουμε

$$\begin{aligned}f(t+1) &= (t+1)^{16} + (t+1)^{15} + \ldots + (t+1) + 1 \\ &= t^{16} + \left(1 + \binom{16}{1}\right)t^{15} + \left(1 + \binom{16}{2} + \binom{15}{1}\right)t^{14} \\ &+ \ldots + \left(\binom{16}{15} + \binom{15}{14} + \ldots + 1\right)t + 17 \\ &= t^{16} + \binom{17}{1}t^{15} + \binom{17}{2}t^{14} + \ldots + \binom{17}{15}t + \binom{17}{16}.\end{aligned}$$

Παρατηρώ πως το πολυώνυμο σύμφωνα με το κριτήριο του Eisenstein και για $q = 17$ είναι ανάγωγο. Άρα και το $f(t)$ είναι ανάγωγο στο $\mathbb{Q}$.

Υπάρχει άλλο ένα χρήσιμο κριτήριο αναγωγιμότητας των πολυωνύμων. Το κριτήριο αυτό βασίζεται στο ότι ο φυσικός ομομορφισμός $\mathbb{Z} \to \mathbb{Z}_p$ μπορεί να επεκταθεί σε ομομορφισμό $\mathbb{Z}[t] \to \mathbb{Z}_p[t]$. Ένα παραγοντοποιήσιμο πολυώνυμο στο $\mathbb{Z}$ είναι το γινόμενο gh δύο πολυωνύμων μικρότερου βαθμού και αυτή η παραγοντοποίηση διατηρείται από τον ομομορφισμό. Εφόσον το p δεν διαιρει τον συντελεστή του μεγιστοβάθμιου όρου ενός πολυωνύμου, η εικόνα του πολυωνύμου αυτού είναι ανάγωγη στο $\mathbb{Z}_p$. Έστω $f(t) = a_0 + a_1 t + \ldots + a_n t^n \in \mathbb{Z}[t]$. Έστω p πρώτος έτσι ώστε $p \not| a_n$. Έστω $\phi : \mathbb{Z} \to \mathbb{Z}_p$ η αναγωγή $mod p$ και $f' = \phi(f)$. Θα δείξουμε ότι αν f' είναι ανάγωγο στο $\mathbb{Z}_p[t]$ τότε το f είναι ανάγωγο στο $\mathbb{Z}$. Έστω ότι το f είναι παραγοντοποιήσιμο. Τότε $f = gh$ με $g(t) = \beta_m t^m + \ldots + \beta_0$ και $h(t) = \gamma_r t^r + \ldots + \gamma_0$. Ισχύει $a_n = \beta_m \gamma_r$ και επειδή $p \not| a_n$ τότε $p \not| \beta_m$ και $p \not| \gamma_r$. $f' = \phi(f) = \phi(gh) = \phi(g)\phi(h) = g'h'$ όπου $\partial g', \partial h' \geq 1$ που είναι άτοπο αφού υποθέσαμε ότι το f' είναι ανάγωγο. Άρα αν η εικόνα ενός πολυωνύμου είναι ανάγωγη στο $\mathbb{Z}_n$ τότε το αρχικό πολυώνυμο είναι ανάγωγο στο $\mathbb{Z}$. Εφόσον το $\mathbb{Z}_n$ είναι πεπερασμένο υπάρχουν πεπερασμένες δοκιμές για την αναγωγιμότητα ή όχι του πολυωνύμου. Σημασία σε αυτό το κριτήριο έχει να επιλέξουμε το κατάλληλο n.

Παράδειγμα 1.2.3 *Έστω ότι μας δίνεται το πολυώνυμο*

$$f(t) = t^4 + 15t^3 + 7$$

στο $\mathbb{Z}$. Στο $\mathbb{Z}_5$ αυτό γίνεται t^4+2. Αν αυτό το πολυώνυμο είναι παραγοντοποιήσιμο στο $\mathbb{Z}_5$ τότε είτε έχει ένα παράγοντα βαθμού 1 είτε έχει δύο παράγοντες βαθμού 2. Στην πρώτη περίπτωση θα έπρεπε να υπάρχει $x \in \mathbb{Z}_5$ έτσι ώστε να ισχύει $x^4+2=0$. Κάνοντας δοκιμές με τα 5 στοιχεία του $\mathbb{Z}_5$ παρατηρούμε πως κανένα δεν επαληθεύει την παραπάνω εξίσωση. Στην δεύτερη περίπτωση μπορούμε χωρίς βλάβη της γενικότητας να υποθέσουμε ότι

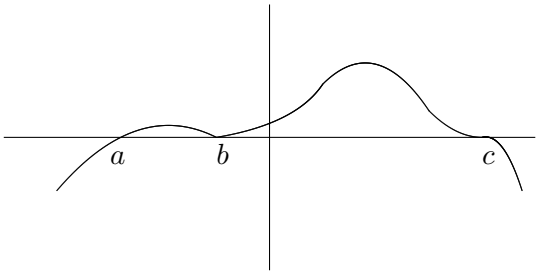
$$t^4+2=(t^2+at+b)(t^2+ct+d).$$

Κάνοντας πράξεις παίρνω τη σχέση $t^4+2=t^4+(a+c)t^3+(ac+b+d)t^2+(ad+bc)t+bd$. Οπότε θα πρέπει να ισχύει $a+c=0$, $ac+b+d=0$, $ad+bc=0$, $bd=2$ δηλαδή $b+d=a^2$ και $bd=2$. Άρα $b+d=0$ ή 1 ή 4 αφού αυτά είναι τα μοναδικά τετράγωνα στο $\mathbb{Z}_5$. Δηλαδή $-b^2=2$ ή $b(1-b)=2$ ή $b(4-b)=2$. Αντικαθιστώντας όπου b τις τιμές 0, 1, 2, 3, 4 του $\mathbb{Z}_5$ βλέπουμε πως καμία δεν επαληθεύει κάποια από τις εξισώσεις. Επομένως το πολυώνυμο t^4+2 είναι ανάγωγο στο $\mathbb{Z}_5$ άρα το αρχικό $f(t)$ είναι ανάγωγο στο $\mathbb{Z}$ και επομένως είναι ανάγωγο και στο $\mathbb{Q}$. Αν δουλεύαμε στο $\mathbb{Z}_3$ το πολυώνυμο θα γινόταν t^4+1 το οποίο είναι παραγοντοποιήσιμο αφού $t^4+1=(t^2+t-1)(t^2-t-1)$. Άρα το πολυώνυμο δεν είναι ανάγωγο στο $\mathbb{Z}_3$ και επομένως δεν γνωρίζουμε αν είναι ανάγωγο στο $\mathbb{Q}$ ή όχι. Στην περίπτωση αυτή το n που επιλέξαμε δεν μας βοήθησε να ελέξουμε την αναγωγιμότητα του πολυωνύμου στο $\mathbb{Q}$. Γι΄ αυτό και η επιλογή του n έχει μεγάλη σημασία στην εφαρμογή αυτού του κριτηρίου.

1.3 Ρίζες πολυωνύμων

Ορισμός 1.3.1 *Έστω R ένας μεταθετικός δακτύλιος και f ένα πολυώνυμο στο R. Ονομάζουμε ρίζα του f στο R κάθε στοιχείο $a \in R$ έτσι ώστε $f(a)=0$.*

Προς το παρόν θεωρούμε πολυώνυμα με συντελεστές από το $\mathbb{R}$. Στο παρακάτω σχήμα βλεπουμε την γραφική παράσταση μιας εξίσωσης $y=f(x)$ όπου $f(x)$ είναι ένα πολυώνυμο με συντελεστές από το $\mathbb{R}$.



Οι ρίζες ενός πολυωνύμου f είναι τα σημεία στα οποία η γραφική παράσταση της f τέμνει τον άξονα των x.

Λήμμα 1.3.1 *Έστω f ένα πολυώνυμο με συντελεστές από ένα σώμα K. Ένα στοιχείο $a \in K$ είναι ρίζα του f αν και μόνο αν $(t-a)|f(t)$.*

Απόδειξη: Αν $(t-a)|f(t)$ τότε

$$f(t) = (t-a)g(t)$$

για κάποιο πολυώνυμο g με συντελεστές από το K. Επομένως

$$f(a) = (a-a)g(a) = 0.$$

Άρα το a είναι ρίζα του f.

Αντίστροφα, έστω ότι $f(a) = 0$. Υπάρχουν πολυώνυμα q, r με συντελεστές από το K έτσι ώστε

$$f(t) = (t-a)q(t) + r(t)$$

όταν $\partial r < 1$. Άρα $r(t) = r \in K$. Αντικαθιστώ όπου t το a και έχω

$$0 = f(a) = (a-a)q(a) + r$$

άρα $r = 0$ και επομένως το $(t-a)|f(t)$.□

Ορισμός 1.3.2 *Έστω f ένα πολυώνυμο με συντελεστές από ένα σώμα K. Ένα στοιχείο $a \in K$ είναι απλή ρίζα του f αν $(t-a)|f(t)$ αλλά $(t-a)^2 \not| f(t)$. Το στοιχείο a είναι ρίζα του f πολλαπλότητας m αν $(t-a)^m|f(t)$ αλλά $(t-a)^{m+1} \not| f(t)$. Οι ρίζες πολλαπλότητας μεγαλύτερης του 1 ονομάζονται πολλαπλές ρίζες.*

Παράδειγμα 1.3.1 *Έστω το πολυώνυμο t^3-3t+2 στο $\mathbb{Q}$. Οι ρίζες του είναι 1 και -2 και παραγοντοποιείται ως εξής: $t^3-3t+2=(t-1)^2(t+2)$. Άρα το -2 είναι μια απλή ρίζα και το 1 είναι μία ρίζα πολλαπλότητας 2.*

Όταν $K=\mathbb{R}$ και σχεδιάζουμε την γραφική παράσταση όπως στο σχήμα, σημεία όπως το a είναι απλές ρίζες, σημεία όπως το b είναι ρίζες περιττής πολλαπλότητας και σημεία όπως το c είναι ρίζες άρτιας πολλαπλότητας >1. Για σώματα διαφορετικά από το $\mathbb{R}$ (εκτός ίσως από το $\mathbb{Q}$ ή υποσώματα του $\mathbb{R}$) μια γραφικη παράσταση δεν έχει κάποιο νόημα. Όμως αν και μια εικόνα μόνο δεν θεωρείται απόδειξη, στα σώματα των πραγματικών μπορεί να μας βοηθήσει να καταλάβουμε τι συμβαίνει γενικά.

Λήμμα 1.3.2 *Έστω f ένα μη-μηδενικό πολυώνυμο στο σώμα K και έστω $a_1,\ldots,a_r$ οι διακριτές του ρίζες με πολλαπλότητες $m_1,\ldots,m_r$ αντίστοιχα. Τότε*

$$f(t)=(t-a_1)^{m_1}\ldots(t-a_r)^{m_r}g(t)$$

όπου το πολυώνυμο g δεν έχει ρίζες στο K.

Αντίστροφα αν ισχύει η παραπάνω σχέση και το g δεν έχει ρίζες στο K τότε οι ρίζες του f στο K είναι τα $a_1,\ldots,a_r$ με πολλαπλότητες $m_1,\ldots,m_r$ αντίστοιχα.

Απόδειξη: Για κάθε $a\in K$ το πολυώνυμο $t-a$ είναι ανάγωγο. Επίσης για διακεκριμένα $a,b\in K$ τα πολυώνυμα $t-a$ και $t-b$ είναι πρώτα μεταξύ τους. Από την μοναδικότητα της παραγοντοποίησης η παραπάνω σχέση ισχυει. Το g δεν θα μπορούσε να έχει ρίζες στο K γιατί τότε το f θα είχε παραπάνω ρίζες ή ρίζες μεγαλύτερης πολλαπλότητας.

Αντίστροφα αν ισχύει η παραπάνω σχέση τότε από την μοναδικότητα της παραγοντοποίησης τα $a_1,\ldots,a_r$ είναι οι μοναδικές ρίζες του f με πολλαπλότητες $m_1,\ldots,m_r$ αντίστοιχα. □

Θεώρημα 1.3.1 *Ο αριθμός των ριζών ενός πολυωνύμου σε ένα σώμα, μετρώντας τις πολλαπλότητες των ριζών, είναι μικρότερος ή ίσος του βαθμού του πολυωνύμου.*

Απόδειξη: Έστω f ένα μη-μηδενικό πολυώνυμο στο σώμα K και έστω $a_1,\ldots,a_r$ οι διακριτές του ρίζες με πολλαπλότητες $m_1,\ldots,m_r$ αντίστοιχα. Τότε

$$f(t)=(t-a_1)^{m_1}\ldots(t-a_r)^{m_r}g(t)$$

όπου το πολυώνυμο g δεν έχει ρίζες στο K. Θα πρεπει να ισχύει
$\partial f=m_1+\ldots+m_r+\partial g$ δηλαδή $m_1+\ldots+m_r\leq\partial f$.□

1.4 Συμμετρικά πολυώνυμα

Θα δούμε πως μπορούμε να κατασκευάσουμε ένα πολυώνυμο αν μας δοθούν οι ρίζες με τις πολλαπλότητες τους. Έστω λοιπόν ένα πολυώνυμο βαθμού n με συντελεστες από ένα σώμα K και έστω ότι έχει όλες του τις ρίζες στο K. Το πλήθος των ριζών αυτών είναι n αν μετρήσουμε και την πολλαπλότητα κάθε ρίζας. Επομένως μπορούμε να το γράψουμε ως:

$$f(t) = k(t - a_1) \dots (t - a_n)$$

όταν $k \in K$ και τα a_i είναι ρίζες του. Υποθέτω ότι το πολυώνυμο γράφεται επίσης

$$f(t) = b_0 + b_1 t + \dots + b_n t^n.$$

Αν κάνουμε πράξεις στην πρώτη εξίσωση θα έχουμε

$$\begin{aligned} f(t) &= k\{t^n - (a_1 + \dots + a_n)t^{n-1} + (a_1a_2 + a_1a_3 + \dots + a_{n-1}a_n)t^{n-2} \\ &+ \dots + (-1)^n a_1a_2 \dots a_n\}. \end{aligned}$$

Επομένως έχουμε τις σχέσεις

$$\begin{aligned} b_n &= k && (1.6) \\ b_{n-1} &= -k(a_1 + \dots + a_n) && (1.7) \\ b_{n-2} &= k(a_1a_2 + a_1a_3 + \dots + a_{n-1}a_n) && (1.8) \\ &\dots \\ b_0 &= k(-1)^n a_1a_2 \dots a_n. && (1.9) \end{aligned}$$

Οι εκφράσεις των $a_1, \dots, a_n$ στο αριστερό μέλος των εξισώσεων έχουν ένα συγκεκριμένο όνομα.

Ορισμός 1.4.1 *Το r-οστό στοιχειώδες συμμετρικό πολυώνυμο*

$$s_r(t_1, \dots, t_n)$$

των $t_1, \dots, t_n$ είναι το άθροισμα όλων των δυνατών διακεκριμένων γινομένων, παίρνοντας το κατάλληλο r κάθε φορά, των στοιχείων $t_1, \dots, t_n$. Δηλαδή

$$\begin{aligned} s_1 &= t_1 + t_2 + t_3 + \ldots + t_n \\ s_2 &= t_1t_2 + t_1t_3 + \ldots + t_1t_n + t_2t_3 + t_2t_4 + \ldots + t_2t_n + \ldots + t_{n-1}t_n \\ &\ldots \end{aligned}$$

Παράδειγμα 1.4.1 *Τα στοιχειώδη συμμετρικά πολυώνυμα των a, b, c είναι τα εξής:*

$$s_1 = a + b + c$$

$$s_2 = ab + ac + bc$$

$$s_3 = abc$$

Αν αντικαταστήσουμε τα $t_1, \ldots, t_n$ με τα στοιχεία $a_1, \ldots, a_n$ που είδαμε στο παραπάνω πολυώνυμο θα έχουμε το r-οστό στοιχειώδες συμμετρικό πολυώνυμο των $a_1, \ldots, a_n$. Δηλαδή:

$$\begin{aligned} s_1(a_1, \ldots, a_n) &= a_1 + a_2 + a_3 + \ldots + a_n \\ s_2(a_1, \ldots, a_n) &= a_1a_2 + a_1a_3 + \ldots + a_1a_n + a_2a_3 + a_2a_4 + \ldots + a_2a_n + \ldots + a_{n-1}a_n \\ &\ldots \\ s_n(a_1, \ldots, a_n) &= a_1a_2 \ldots a_n \end{aligned}$$

Επομένως μπορούμε να ξαναγράψουμε τις σχέσεις (1.6)-(1.9) ως εξής

$$\begin{aligned} b_n &= k \\ b_{n-1} &= -ks_1(a_1, \ldots, a_n) \\ b_{n-2} &= ks_2(a_1, \ldots, a_n) \\ &\ldots \\ b_0 &= k(-1)^n s_n(a_1, \ldots, a_n) \end{aligned}$$

Μπορούμε να γενικεύσουμε γράφοντας τον τύπο

$$b_{n-r} = k(-1)^r s_r(a_1, \ldots, a_n).$$

Αυτά τα πολυώνυμα είναι συμμετρικά με την έννοια ότι τα πιθανά γινόμενα παράγονται από τους συντελεστές των αγνώστων t. Υπάρχουν και άλλα συμμετρικά πολυώνυμα εκτός από τα στοιχειώδη συμμετρικά όπως το $t_1^2 + \ldots + t_n^2$ όμως όλα μπορούν να εκφραστούν με όρους των στοιχειωδών συμμετρικών πολυωνύμων.

Παράδειγμα 1.4.2 *Το πολυώνυμο $t_1^2 + t_2^2$ είναι συμμετρικό αλλα όχι στοιχειώδες και μπορει να γραφεί ως ένα πολυώνυμο με όρους των στοιχειωδών πολυωνύμων. Δηλαδή:*

$$t_1^2 + t_2^2 = (t_1 + t_2)^2 - 2t_1t_2 = s_1^2 - 2s_2$$

Παράδειγμα 1.4.3 *Βρείτε ποια από τα παρακάτω πολυώνυμα είναι ανάγωγα η όχι και γράψτε σε γινόμενο ανάγωγων πολυωνύμων αυτά που δεν είναι ανάγωγα.*
(a) $t^4 + 1$ *με συντελεστές από το* $\mathbb{R}$
(b) $t^4 + 1$ *με συντελεστές από το* $\mathbb{Q}$
(c) $t^7 + 11t^3 - 33t + 22$ *με συντελεστές από το* $\mathbb{Q}$
(d) $t^4 + t^3 + t^2 + t + 1$ *με συντελεστές από το* $\mathbb{Q}$
(e) $t^3 - 7t^2 + 3t + 3$ *με συντελεστές από το* $\mathbb{Q}$
(f) $t^4 + 7$ *με συντελεστές από το* $\mathbb{Z}_{17}$
(g) $t^3 - 5$ *με συντελεστές από το* $\mathbb{Z}_{11}$
(h) $t^2 - at + b$ *με συντελεστές από το σώμα* $\{0,\ 1,\ a,\ \beta\}$ *με πράξεις:*

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$.$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Απαντηση:
(a)

$$\begin{aligned} t^4 + 1 &= (t^2 + at + b)(t^2 + ct + d) \quad (a, b, c, d \in \mathbb{R}) \\ &= t^4 + (a + c)t^3 + (b + ac + d)t^2 + (ad + bc)t + bd \end{aligned}$$

οπότε έχουμε τις σχέσεις:

$$\begin{cases} a + c = 0 \\ b + ac + d = 0 \\ bc + ad = 0 \\ bd = 1 \end{cases}$$

Από τις παραπάνω σχέσεις έχουμε τις λύσεις:
(a) $a=0,\ b=i,\ c=0,\ d=-i$
ή $a=0,\ b=-i,\ c=0,\ d=i$
(b) $a=\sqrt{2},\ b=1,\ c=-\sqrt{2},\ d=1$
ή $a=-\sqrt{2},\ b=1,\ c=\sqrt{2},\ d=1$
(c) $a=\sqrt{2}i,\ b=-1,\ c=-\sqrt{2}i,\ d=-1$
ή $a=-\sqrt{2}i,\ b=-1,\ c=\sqrt{2}i,\ d=1$
Άρα το πολυώνυμο στο $\mathbb{R}$ παραγοντοποιείται ως εξής:

$$t^4+1=(t^2+\sqrt{2}t+1)(t^2-\sqrt{2}t+1)$$

(b) Είναι ανάγωγο στο $\mathbb{Q}$ γιατί όπως δείξαμε στο (b) δεν μπορεί να γραφεί ως γινόμενο πολυωνύμων με συντελεστές από το $\mathbb{Q}$

(c) Για $p=11$, από το κριτήριο του *Eisenstein*, το πολυώνυμο είναι ανάγωγο στο $\mathbb{Q}$.

(d) Το $f(t+1)=t^4+5t^3+10t^2+10t+5$ και για $p=5$, από το κριτήριο του *Eisenstein*, είναι ανάγωγο στο $\mathbb{Q}$. Επομένως το $f(t)=t^4+t^3+t^2+t+1$ είναι ανάγωγο στο $\mathbb{Q}$.

(e) $t^3-7t^2+3t+3=(t-1)(t^2-6t-3)$.

(f) Αν αυτό το πολυώνυμο είναι παραγοντοποιήσιμο στο $\mathbb{Z}_{17}$ τότε είτε έχει ένα παράγοντα βαθμού 1 είτε έχει δύο παράγοντες βαθμού 2. Στην πρώτη περίπτωση θα έπρεπε να υπάρχει $x\in\mathbb{Z}_{17}$ έτσι ώστε να ισχύει $x^4+7=0$. Κάνοντας δοκιμές με τα 17 στοιχεία του $\mathbb{Z}_{17}$ παρατηρούμε πως κανένα δεν επαληθεύει την παραπάνω εξίσωση. Στην δεύτερη περίπτωση μπορούμε χωρίς βλάβη της γενικότητας να υποθέσουμε ότι

$$t^4+7=(t^2+at+b)(t^2+ct+d).$$

Κάνοντας πράξεις παίρνω τη σχέση

$$t^4+7=t^4+(a+c)t^3+(ac+b+d)t^2+bd.$$

Οπότε έχουμε τις σχέσεις: $\begin{cases} a+c=0 \\ b+ac+d=0 \\ bc+ad=0 \\ bd=7 \end{cases} \Rightarrow \begin{cases} c=-a \\ b+d=a^2 \\ ad-ab=0 \\ bd=7 \end{cases}$
Άρα $b+d=0$ ή $b+d=1$ ή $b+d=4$ ή $b+d=9$ ή $b+d=16$ αφού αυτά είναι τα μοναδικά τετράγωνα στο $\mathbb{Z}_{17}$. Επομένως $-b^2=7$ ή $b(1-b)=7$ ή

$b(4-b) = 7$ ή $b(9-b) = 7$ ή $b(16-b) = 7$. Αντικαθιστώντας όπου b τα στοιχεία του $\mathbb{Z}_{17}$ παρατηρούμε πως κανένα δεν επαληθεύει τις εξισώσεις. Άρα το πολυώνυμο $t^4 + 7$ είναι ανάγωγο στο $\mathbb{Z}_{17}$.

(g) $t^3 - 5 = (t-3)(t^2+3t+9)$.

(h) Παρατηρούμε πως το 1 και το β είναι ρίζες του πολυωνύμου, επομένως $t^2 - at + b = (t-1)(t-\beta)$.

Παράδειγμα 1.4.4 *Αν K είναι ένα σώμα με άπειρα στοιχεία και f, g είναι πολυώνυμα με συντελεστές από το K έτσι ώστε $f(a) = g(a), \forall a \in K$, δείξτε ότι $f = g$.*

Απάντηση:
Έστω $h = f - g$. Αρκεί να δείξουμε ότι το h είναι το μηδενικό πολυώνυμο. Έστω ότι το h δεν είναι το μηδενικό πολυώνυμο. Έστω $a_1, a_2, \ldots \in K$. Τότε:
$h(a_1) = f(a_1) - g(a_1) = 0$ οπότε το $t - a_1 | h$
$h(a_2) = f(a_2) - g(a_2) = 0$ οπότε το $t - a_2 | h$
...
Επειδή υπάρχουν άπειρα $a_i \in K$ το $(t-a_1)(t-a_2)\ldots$ είναι άπειρου βαθμού άρα το h θα πρέπει να είναι το μηδενικό πολυώνυμο.
Έστω τα πολυώνυμα $f(t) = t^7$ και $g(t) = t$ στο $\mathbb{Z}_7$. Ισχύει $f(a) = g(a)$ $\forall a \in \mathbb{Z}_7$ όμως $f \neq g$.

Παράδειγμα 1.4.5 *Έστω K ένα σώμα. Λέμε ότι ένα πολυώνυμο με συντελεστές από το K είναι πρώτο αν $f|gh$ τότε $f|g$ ή $f|h$. Δείξτε ότι ένα πολυώνυμο $f \neq 0$ είναι πρώτο αν και μόνο αν είναι ανάγωγο.*

Απάντηση:
Έστω ότι το f είναι πρώτο και έστω ότι είναι παραγοντοποιήσιμο, δηλαδή έστω ότι γράφεται $f = gh$. Τότε $f|f = gh$ και επειδή είναι πρώτο $f|g$ ή $f|h$ που είναι άτοπο αφού $\partial g, \partial h < \partial f$. Άρα το f δεν είναι ανάγωγο. Έστω ότι το πολυώνυμο είναι ανάγωγο και $f|gh$. Θα δείξουμε ότι το f είναι πρώτο, δηλαδή ότι $f|g$ ή $f|h$. Αυτό έχει ήδη αποδειχτεί στο λήμμα 1.1.1.

Παράδειγμα 1.4.6 *Γράψτε όλα τα δυνατά πολυώνυμα της μορφής $t^2 + at + b$ με συντελεστές από το $\mathbb{Z}_5$. Βρείτε ποια είναι ανάγωγα. Σε κάθε περίπτωση βρείτε το $a^2 - 4b$. Τι παρατηρείτε; Μπορείτε να αποδείξετε την παρατήρησή σας;*

Απάντηση:

		$\alpha^2 - 4b$
t^2	-	0
t^2+1	-	1
t^2+2	A	2
t^2+3	A	3
t^2+4	-	4
t^2+t	-	1
t^2+t+1	A	2
t^2+t+2	A	3
t^2+t+3	-	4
t^2+t+4	-	0
t^2+2t	-	4
t^2+2t+1	-	0
t^2+2t+2	-	1
t^2+2t+3	-	0
t^2+2t+4	-	4
t^2+3t	-	4
t^2+3t+1	-	0
t^2+3t+2	-	1
t^2+3t+3	A	2
t^2+3t+4	A	3
t^2+4t	-	1
t^2+4t+1	A	2
t^2+4t+2	A	3
t^2+4t+3	-	4
t^2+4t+4	-	0

Παρατηρούμε ότι το πολυώνυμο t^2+at+b είναι ανάγωγο όταν το a^2-4b δεν είναι τέλειο τετράγωνο κάποιου αριθμού. Η διακρίνουσα του πολυωνύμου είναι a^2-4b. Για να παραγοντοποιείται το πολυώνυμο θα πρέπει η διακρίνουσα να είναι τέλειο τετράγωνο αφού οι ρίζες του είναι της μορφής $(-b\pm\sqrt{a^2-4b})/2a$. Επομένως το πολυώνυμο είναι ανάγωγο όταν το a^2-4b δεν είναι τέλειο τετράγωνο.

Παράδειγμα 1.4.7 *Βρείτε τις ρίζες των παρακάτω πολυωνύμων στο* $\mathbb{Q}$*, στο* $\mathbb{R}$ *και στο* $\mathbb{C}$*.*
(a) t^3+1
(b) $t^3-6t^2+11t-6$

(c) $t^5 + t + 1$
(d) $t^2 + 1$
(e) $t^4 + t^3 + t^2 + t + 1$
(f) $t^4 - 6t^2 + 11$.

Απάντηση:
(a) $\mathbb{Q} : -1, \mathbb{R} : -1, \mathbb{C} : -1,\ (1 \pm \sqrt{3}i)/2$

(b) $\mathbb{Q} : 1, 2, 3, \mathbb{R} : 1, 2, 3, \mathbb{C} : 1, 2, 3$

(c) $\mathbb{Q} : -, \mathbb{R} : -, \mathbb{C} : \exp(2\pi i/5),\ \exp(4\pi i/5),\ \exp(6\pi i/5),\ \exp(8\pi i/5)$

(d) $\mathbb{Q} : -, \mathbb{R} : -, \mathbb{C} : \pm i$

(e) $\mathbb{Q} : -, \mathbb{R} : -, \mathbb{C} : exp(2\pi i/3),\ \exp(4\pi i/3),\ \frac{1}{3} - \frac{1}{3}\left(\frac{2}{25-3\sqrt{69}}\right)^{1/3} - \frac{1}{3}\left(\frac{1}{2}(25 - 3\sqrt{69})\right)^{1/3},\ \frac{1}{3} + \frac{1}{6}(1 + \sqrt{3}i\left(\frac{1}{2}(25 - 3\sqrt{69})\right)^{1/3} + \frac{1-\sqrt{3}i}{32^{2/3}(25-3\sqrt{69})^{1/3}},\ \frac{1}{3} + \frac{1}{6}(1 - \sqrt{3}i\left(\frac{1}{2}(25 - 3\sqrt{69})\right)^{1/3} + \frac{1+\sqrt{3}i}{32^{2/3}(25-3\sqrt{69})^{1/3}},$

(f) $\mathbb{Q} : -, \mathbb{R} : -, \mathbb{C} : \pm\sqrt{3 + i\sqrt{2}},\ \pm\sqrt{3 - i\sqrt{2}}.$

Παράδειγμα 1.4.8 *Δείξτε ότι για κάθε πρώτο p το σώμα $\mathbb{Z}_p(t)$ έχει χαρακτηριστική p. Είναι οι $\mathbb{Z}_p$, $\mathbb{Z}_p(t)$ ισομορφικοί;*

Απάντηση:
Έστω $f(t) = a_0 + a_1 t + \ldots + a_n t^n$ ένα πολυώνυμο με συντελεστές απο το $\mathbb{Z}_p(t)$, $(a_0, a_1, \ldots, a_n, \in \mathbb{Z}_p)$. Τότε

$$pf(t) = pa_0 + pa_1 t + \ldots + pa_n t^n = 0.$$

Άρα το $\mathbb{Z}_p(t)$ έχει χαρακτηριστική p. Οι χώροι δεν είναι ισομορφικοί γιατι ο $\mathbb{Z}_p$ έχει πεπερασμένο πλήθος στοιχείων ενώ ο $\mathbb{Z}_p(t)$ έχει άπειρα στοιχεία.

Παράδειγμα 1.4.9 *Δώστε ένα κριτήριο για την αναγωγιμότητα ενός δευτεροβάθμιου πολυωνύμου με συντελεστές από ένα σώμα K χαρακτηριστικής $\neq 2$.*

Απάντηση:
Έστω $at^2 + bt + c$ ένα τέτοιο πολυώνυμο στο σώμα K. Τότε το πολυώνυμο

είναι ανάγωγο αν και μόνο αν το b^2-4ac δεν είναι τέλειο τετράγωνο. Έστω ότι υπάρχει x τέτοιο ώστε

$$ax^2+bx+c=0 \Leftrightarrow$$

$$\Leftrightarrow x^2+\frac{b}{a}x+\frac{c}{a}=0 \Leftrightarrow$$

όταν η χαρακτηριστική του K είναι $\neq 2$

$$\Leftrightarrow x^2+2\frac{b}{2a}x+\frac{c}{a}+\left(\frac{b}{2a}\right)^2=\left(\frac{b}{2a}\right)^2 \Leftrightarrow$$

$$\Leftrightarrow \left(x+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2}.$$

Άρα για να υπάρχει x έτσι ώστε να παραγοντοποιείται το πολυώνυμο θα πρέπει το $\frac{b^2-4ac}{4a^2}$ να είναι τέλειο τετράγωνο. Δηλαδή το b^2-4ac να είναι τέλειο τετράγωνο. Επομένως το πολυώνυμο είναι ανάγωγο αν και μόνο αν το b^2-4ac δεν είναι τέλειο τετράγωνο.

Παράδειγμα 1.4.10 *Να εκφράσετε με όρους των στοιχειωδών συμμετρικών πολυωνύμων των a, β, γ τα παρακάτω*
(a) $\alpha^2+\beta^2+\gamma^2$
(b) $\alpha^3+\beta^3+\gamma^3$
(c) $\alpha^2\beta+\alpha^2\gamma+\beta^2\alpha+\beta^2\gamma+\gamma^2\alpha+\gamma^2\beta$
(d) $\alpha^2\beta^2\gamma^2$
(e) $(\alpha-\beta)^2+(\beta-\gamma)^2+(\gamma-\alpha)^2$
(f) $\alpha^2+\beta\gamma$

Απάντηση:
(a) $\alpha^2+\beta^2+\gamma^2=\alpha^2+\beta^2+\gamma^2+2\alpha\beta+2\alpha\gamma+2\beta\gamma-2\alpha\beta-2\alpha\gamma-2\beta\gamma=(\alpha+\beta+\gamma)^2-2(\alpha\beta+\alpha\gamma+\beta\gamma=s_1^2-2s_2$

(b) $\alpha^3+\beta^3+\gamma^3=\alpha^3+\beta^3+\gamma^3+3\alpha\beta^2+3\alpha\gamma^2+3\alpha^2\beta+3\alpha^2\gamma+3\beta^2\gamma+3\beta\gamma^2+9\alpha\beta\gamma-3\alpha\beta^2-3\alpha\gamma^2-3\alpha^2\beta-3\alpha^2\gamma-3\beta^2\gamma-3\beta\gamma^2-9\alpha\beta\gamma=(\alpha+\beta+\gamma)^3-3\alpha(\alpha\beta+\alpha\gamma+\beta\gamma)-3\beta(\alpha\beta+\alpha\gamma+\beta\gamma)-3\gamma(\alpha\beta+\alpha\gamma+\beta\gamma)+3\alpha\beta\gamma=(\alpha+\beta+\gamma)^3-3(\alpha+\beta+\gamma)(\alpha\beta+\alpha\gamma+\beta\gamma)+3\alpha\beta\gamma=s_1^3-3s_1s_2+3s_3$

(c) $\alpha^2\beta+\alpha^2\gamma+\beta^2\alpha+\beta^2\gamma+\gamma^2\alpha+\gamma^2\beta=\alpha(\alpha\beta+\alpha\gamma)+\beta(\alpha\beta+\beta\gamma)+\gamma(\alpha\gamma+\beta\gamma)=\alpha(\alpha\beta+\alpha\gamma+\beta\gamma)+\beta(\alpha\beta+\beta\gamma+\alpha\gamma)+\gamma(\alpha\gamma+\beta\gamma+\alpha\beta)-3\alpha\beta\gamma=(\alpha+\beta+\gamma)(\alpha\beta+\alpha\gamma+\beta\gamma)-3\alpha\beta\gamma=s_1s_2-3s_3$

(*d*) $\alpha^2\beta^2\gamma^2 = (\alpha\beta\gamma)^2 = s_3^2$

(*e*) $(\alpha-\beta)^2+(\beta-\gamma)^2+(\gamma-\alpha)^2 = \alpha^2+\beta^2-2\alpha\beta+\beta^2+\gamma^2-2\beta\gamma+\gamma^2+\alpha^2-2\alpha\gamma = 2\alpha^2+2\beta^2+2\gamma^2-2\alpha\beta-2\alpha\gamma-2\beta\gamma = 2(\alpha^2+\beta^2+\gamma^2)-2(\alpha\beta+\alpha\gamma+\beta\gamma) = 2(s_1^2-2s_2)-2s_2 = 2s_1^2-6s_2$

(*f*) Δεν υπάρχει.

Παράδειγμα 1.4.11 *Γιατί δεν έχει νόημα να προσπαθήσουμε να λύσουμε μια πολυωνυμική εξίσωση λύνοντας τις εξισώσεις για τα συμμετρικά πολυώνυμα των ριζών;*

Απάντηση:
Γιατί όταν λύσουμε το σύστημα των εξισώσεων των συμμετρικών πολυωνύμων των ριζών καταλήγουμε στην αρχική εξίσωση.

Παράδειγμα 1.4.12 *Βρείτε ποιες από τις παρακάτω προτάσεις είναι σωστές ή λάνθασμένες*
(*a*) *Κάθε πολυώνυμο με συντελεστές από ένα σώμα K έχει μία ρίζα στο K.*
(*b*) *Κάθε πολυώνυμο το οποίο είναι ανάγωγο στο* $\mathbb{Q}$ *είναι επίσης ανάγωγο στο* $\mathbb{R}$.
(*c*) *Κάθε πολυώνυμο το οποίο είναι ανάγωγο στο* $\mathbb{Z}$ *είναι επίσης ανάγωγο στο* $\mathbb{Q}$.
(*d*) *Τα γραμμικά πολυώνυμα είναι ανάγωγα.*
(*e*) *Όλα τα συμμετρικά πολυώνυμα είναι στοιχειώδη.*
(*f*) *Κάθε πολυώνυμο που γράφεται στη μορφή στοιχειωδών συμμετρικών πολυωνύμων είναι και αυτό συμμετρικό.*
(*g*) *Υπάρχουν άπειρα ανάγωγα πολυώνυμα με συντελεστές από το* $\mathbb{Q}$.
(*h*) *Τα πολυώνυμα που είναι πρώτα μεταξύ τους έχουν διαφορετικούς βαθμούς.*
(*i*) *Ένα πολυώνυμο με βαθμό ένα πρώτο αριθμό είναι ανάγωγο.*
(*j*) *Ένα πολυώνυμο με βαθμό ένα σύνθετο αριθμό είναι παραγοντοποιήσιμο.*

Απάντηση:
(*a*) Λάθος. Το t^2+1 δεν έχει ρίζα στο $\mathbb{R}$.
(*b*) Λάθος. Το t^2-2 είναι ανάγωγο στο $\mathbb{Q}$ αλλά στο $\mathbb{R}$ έχει ρίζες $(\pm\sqrt{2})$.
(*c*) Σωστό. Έχει αποδειχθεί παραπάνω.
(*d*) Σωστό.
(*e*) Λάθος. Το $t_1^2+\ldots+t_n^2$ είναι συμμετρικό αλλά όχι στοιχειώδες.
(*f*) Σωστό.

(g) Σωστό. Για παράδειγμα τα πολυώνυμα της μορφής $at^2 + 2$ $(a \in \mathbb{Z})$ είναι ανάγωγα στο $\mathbb{Q}$ και υπάρχουν άπειρα τέτοια πολυώνυμα.
(h) Λάθος. Τα $t^2 + 1$, $t^2 + 2$ είναι πρώτα μεταξύ τους και έχουν τον ίδιο βαθμό.
(i) Λάθος. Το $t^3 + 1$ είναι παραγοντοποιήσιμο στο $\mathbb{Q}$.
(j) Λάθος. Το $t^4 + 1$ δείξαμε ότι είναι ανάγωγο στο $\mathbb{Q}$.

Κεφάλαιο 2

Επεκτάσεις σωμάτων

Σε αυτό το κεφάλαιο θα ορίσουμε την επέκταση ενός σώματος και θα δούμε ποια είναι η χρησιμότητά της στα πολυώνυμα. Θα κατηγοριοποιήσουμε κάποιους βασικούς τύπους επεκτάσεων και θα δώσουμε μεθόδους με τι οποίες μπορούν να κατασκευαστούν.

2.1 Επεκτάσεις σωμάτων

Έστω ότι έχουμε το πολυώνυμο τετάρτου βαθμού $f(t) = t^4 - 4t^2 - 5$ με συντελεστές από το $\mathbb{Q}$. Οι ρίζες του στο $\mathbb{C}$ είναι $\pm i$, $\pm\sqrt{5}$. Το σύνολο όλων των ρητών εκφράσεων αυτών των ριζών στο $\mathbb{Q}$ αποτελεί ένα σώμα $L \supseteq \mathbb{Q}$. Έστω ότι το L περιέχει όλα τα στοιχεία του $\mathbb{C}$ της μορφής

$$p + qi + r\sqrt{5} + si\sqrt{5} \quad p, q, r, s \in \mathbb{Q}.$$

Τα αθροίσματα και τα γινόμενα τέτοιων στοιχείων έχουν την ίδια μορφή, επομένως ανήκουν στο L. Επίσης μπορούμε να βρούμε για κάθε τέτοιο στοιχείο τον αντίθετο και τον αντίστροφο τα οποία θα είναι στοιχεία της ίδιας μορφής. Δηλαδή το L είναι ένα σώμα. Επομένως η μελέτη ενός πολυωνύμου στο $\mathbb{Q}$ προϋποθέτει την ύπαρξη ενός νέου σώματος L που περιέχει το $\mathbb{Q}$. Γενικότερα η μελέτη ενός πολυωνύμου σ'ενα τυχαίο σώμα K θα μας οδηγήσει στην δημιουργία ενος σώματος L που περιέχει το K. Ονομάζουμε το L μία επέκταση του K. Επίσης υπάρχουν περιπτώσεις που το L θα περιέχει ένα σώμα ισομορφικό με το K και όχι απαραίτητα ίσο με αυτό.

Ορισμός 2.1.1 *Μία επέκταση σώματος είναι ένας μονομορφισμός $i : K \to L$ όταν τα K, L είναι σώματα. Το K θα λέμε ότι είναι το μικρό σώμα και το L θα λέμε ότι είναι το μεγάλο σώμα.*

Παράδειγμα 2.1.1 *Οι συναρτήσεις $i_1 : \mathbb{Q} \to \mathbb{R}$, $i_2 : \mathbb{R} \to \mathbb{C}$, $i_3 : \mathbb{Q} \to \mathbb{C}$ είναι όλες επεκτάσεις σωμάτων.*

Παράδειγμα 2.1.2 *Αν K είναι ένα σώμα τότε το $K(t)$ είναι το σώμα όλων των ρητών εκφράσεων του t με συντελεστές από το K. Δηλαδή το $K(t)$ αποτελείται από όλα τα πολυώνυμα της μορφής:*

$$\frac{a_0 + a_1 t + \ldots + a_n t^n}{b_0 + b_1 t + \ldots + b_m t^m}$$

όταν $a_i \in K$ $(i = 0, 1, \ldots, n)$ και $b_j \in K$ $(j = 0, 1, \ldots, m)$. Υπάρχει ένας φυσικός μονομορφισμός $i : K \to K(t)$ έτσι ώστε κάθε στοιχείο του K πηγαίνει στο αντίστοιχο σταθερό πολυώνυμο. Είναι και αυτή μια επέκταση σώματος.

Παράδειγμα 2.1.3 *Έστω P το σύνολο όλων των πραγματικών αριθμών της μορφής $p + q\sqrt{2}$ όταν p, $q \in \mathbb{Q}$. Το P είναι ένα υπόσωμα του $\mathbb{R}$. Διότι:*

- $0 = 0 + 0\sqrt{2} \in P$
- $1 = 1 + 0\sqrt{2} \in P$

Για κάθε $p + q\sqrt{2},\ r + s\sqrt{2} \in P$

- $p + q\sqrt{2} + r + s\sqrt{2} = (p + q) + (r + s)\sqrt{2} \in P$
- $-(p + q\sqrt{2}) = -p - q\sqrt{2} \in P$
- $(p + q\sqrt{2})(r + s\sqrt{2}) = (pr + 2qs) + (ps + qr)\sqrt{2} \in P$
- $(p + q\sqrt{2})^{-1} = \frac{p}{p^2 - 2q^2} - \frac{q}{p^2 - 2q^2}\sqrt{2} \in P,\ (p, q \neq 0)$

Ο μονομορφισμός $i : \mathbb{Q} \to P$ είναι μια επέκταση σώματος.

Αν $i : K \to L$ είναι μια επέκταση σώματος μπορούμε συνήθως να ταυτήσουμε το K με την εικόνα του $i(K)$ οπότε ο i μπορεί να θεωρηθεί ένα προς ένα και το K μπορεί να θεωρηθεί ως υπόσωμα του L. Κάτω από αυτές τις προυποθέσεις χρησιμοποιούμε τον συμβολισμό

$$L : K$$

για την επέκταση και λέμε ότι το L είναι μια επέκταση του K.

Ορισμός 2.1.2 *Έστω K ένα σώμα και X ένα μη κενό υποσύνολο του K. Τότε το υπόσωμα του K που παράγεται από το X είναι η τόμη όλων των υποσωμάτων του K που περιέχουν το X.*

Μπορούμε επίσης να πούμε ότι το υπόσωμα του K που παράγεται από το X είναι το μικρότερο υπόσωμα του K που περιέχει το X ή ότι το σύνολο όλων των στοιχείων του K μπορούν να δημιουργηθούν απο τα στοιχεία του X με πεπερασμένο πλήθος πράξεων μέσα στο σώμα εφόσον το $X \neq \{0\}$.

Παράδειγμα 2.1.4 *Θα βρούμε το υπόσωμα του $\mathbb{C}$ που παράγεται από το $X = \{1, i\}$. Έστω L αυτό το υπόσωμα. Τότε το L θα πρέπει να περιέχει το πρώτο υπόσωμα του $\mathbb{C}$, δηλαδή το $\mathbb{Q}$. Αυτό συμβαίνει διότι το πρώτο υπόσωμα ενός σώματος είναι το μικρότερο υπόσωμα του σώματος και επομένως περιέχεται σε κάθε άλλο υπόσωμα. Εφόσον το L είναι κλειστό με τις πράξεις του σώματος θα πρέπει να περιέχει κάθε στοιχείο της μορφής*

$$p + qi$$

όταν $p, q \in \mathbb{Q}$. Θα ονομάσουμε M το σύνολο όλων αυτών των στοιχείων. Θα αποδείξουμε ότι το M είναι σώμα. Το M είναι κλειστό κάτω από την πρόσθεση και τον πολλαπλασιασμό και επίσης για κάθε $p + qi \neq 0$ έχουμε:

$$(p + qi)^{-1} = \frac{p}{p^2 + q^2} - \frac{q}{p^2 + q^2} i,$$

άρα το M είναι σώμα και περιέχει το X. Εφόσον το L είναι το μικρότερο υπόσωμα που περιέχει το X, ισχύει $L \subseteq M$. Όμως από την υπόθεση έχουμε ότι $M \subseteq L$ άρα τελικα $M = L$ και το υπόσωμα του $\mathbb{C}$ που παράγεται από το X είναι της μορφής

$$M = \{p + qi : p, q \in \mathbb{Q}\}.$$

Στην περίπτωση μιας επέκτασης $K : L$ μας ενδιαφέρουν περισσότερο τα σώματα που υπάρχουν μεταξύ των L και K. Αυτό σημαίνει ότι μπορούμε να περιορίσουμε το ενδιαφέρον μας σε υποσώματα του L που περιέχουν το K ή ισοδύναμα σε σώματα της μορφής $K \cup Y$ όταν $Y \subseteq L$.

Ορισμός 2.1.3 *Αν $L : K$ είναι μια επέκταση και Y ένα υποσύνολο του L τότε το υπόσωμα του L που παράγεται από το $K \cup Y$ γράφεται $K(Y)$ και λέμε ότι δημιουργείται από το K προσθέτοντας το Y.*

Παράδειγμα 2.1.5 *Έστω $K = \mathbb{Q}$ και $Y = \{i, -i, \sqrt{5}, -\sqrt{5}\}$. Τότε το $K(Y)$ θα πρέπει να περιέχει το K και το Y. Δηλαδή θα πρέπει να περιέχει κάθε στοιχείο της μορφης*

$$a = p + qi + r\sqrt{5} + si\sqrt{5} \quad (p, q, r, s \in \mathbb{Q}).$$

Έστω $L \subseteq \mathbb{C}$ το σύνολο όλων αυτών των στοιχείων. Θα αποδείξουμε ότι το L είναι σώμα. Το L είναι κλειστό κάτω από την πρόσθεση και τον πολλαπλασιασμο και αρκεί να δείξουμε ότι για $(p,q,r,s) \neq (0,0,0,0)$ ισχύει

$$(p + qi + r\sqrt{5} + si\sqrt{5})^{-1} \in L$$

Έστω M το υπόσωμα του L που περιέχει όλα τα στοιχεία της μορφής $p + qi$ $(p, q \in \mathbb{Q})$. Τότε μπορούμε να γράψουμε

$$a = x + y\sqrt{5}$$

όταν $x = p + qi$ και $y = r + si \in M$. Έστω

$$b = x - y\sqrt{5} \in L.$$

Τότε

$$ab = (x + y\sqrt{5})(x - y\sqrt{5}) = x^2 - 5y^2 = z$$

όταν το $z \in M$. Τότε $a^{-1} = bz^{-1}$. Θέτω $z = u + vi$ $(u, v \in \mathbb{Q})$ και έστω $w = u - vi$. Τότε

$$zw = (u + vi)(u - vi) = u^2 - (vi)^2 = u^2 + v^2$$

άρα έχουμε

$$z^{-1} = (u^2 + v^2)^{-1} w \in M$$

οπότε το $a^{-1} = bz^{-1} \in L$. Εφόσον το L είναι σώμα τότε το $K(Y) = L$.

Παρατηρούμε ότι το $K(Y)$ είναι μεγαλύτερο από το $K \cup Y$. Γενικότερα αν το Y έχει μόνο ένα στοιχείο αντί για $K(\{y\})$ θα γράφουμε $K(y)$ και γενικότερα αντί για $K(\{y_1, \ldots, y_n\})$ θα γράφουμε $K(y_1, \ldots, y_n)$.

Παράδειγμα 2.1.6 *Το υπόσωμα $\mathbb{R}(i)$ του $\mathbb{C}$ θα πρέπει να περιέχει όλα τα στοιχεία της μορφής $x + yi$ όταν $x, y \in \mathbb{R}$. Άρα $\mathbb{C} = \mathbb{R}(i)$.*

Παράδειγμα 2.1.7 *Έστω K ένα σώμα και $K(t)$ το σύνολο όλων των ρητών εκφράσεων του t με συντελεστές από το K. Το $K(t)$ θα μπορούσε να θεωρηθεί ως μια διφορούμενη έννοια εφόσον με $K(t)$ επίσης συμβολίζουμε το υπόσωμα που παράγεται από το $K \cup t$. Όμως αυτό το σώμα εφόσον είναι κλειστό κάτω από τις πράξεις θα πρέπει να περιέχει όλες τις ρητές εκφράσεις του t. Οπότε είναι ολόκληρο το σώμα των ρητών εκφράσεων και οι δύο έννοιες που θα μπορούσε να έχει ο συμβολισμος $K(t)$ ταυτίζονται.*

Παράδειγμα 2.1.8 *Το υπόσωμα του $\mathbb{R}$ που αποτελείται από όλα τα στοιχεία $p+q\sqrt{2}$ όταν $p,\ q \in \mathbb{Q}$ είναι προφανώς το $\mathbb{Q}(\sqrt{2})$.*

Παράδειγμα 2.1.9 *Είδαμε ότι το $\mathbb{R}(i)$ περιέχει όλα τα στοιχεία της μορφής $x+yi$ όταν $x,\ y \in \mathbb{R}$. Το $\mathbb{Q}(\sqrt{2})$ αποτελείται από όλα τα στοιχεία της μορφής $p+q\sqrt{2}$ όταν $p,\ q \in \mathbb{Q}$. Γενικά δεν ισχύει ότι ένα σώμα της μορφής $K(a)$ αποτελείται από όλα τα στοιχεία της μορφής $j+ka$ όταν $j,\ k \in K$. Σε ορισμένες περιπτώσεις τα στοιχεία αυτά και μόνο δεν αποτελούν ένα σώμα. Για παράδειγμα έστω ότι έχουμε την επέκταση $\mathbb{R} : \mathbb{Q}$ και έστω ότι $a = \sqrt[3]{2}$. Το σώμα $\mathbb{Q}(a)$ αποτελείται από όλα τα στοιχεία του $\mathbb{R}$ της μορφής $p+qa+ra^2$ όταν $p,\ q,\ r \in \mathbb{Q}$. Το σύνολο αυτών των στοιχείων αποτελούν ένα σώμα διότι:*

- $0 = 0 + 0\sqrt[3]{2} + 0\sqrt[3]{4} \ \in \mathbb{Q}(\sqrt[3]{2})$
- $1 = 1 + 0\sqrt[3]{2} + 0\sqrt[3]{4} \ \in \mathbb{Q}(\sqrt[3]{2})$

$\forall p+q\sqrt[3]{2}+r\sqrt[3]{4},\ k+l\sqrt[3]{2}+m\sqrt[3]{4} \ \in \mathbb{Q}(\sqrt[3]{2})$

- $p+q\sqrt[3]{2}+r\sqrt[3]{4}+k+l\sqrt[3]{2}+m\sqrt[3]{4} = (p+k)+(q+l)\sqrt[3]{2}+(r+m)\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$
- $-(p+q\sqrt[3]{2}+r\sqrt[3]{4}) = -p+(-q)\sqrt[3]{2}+(-r)\sqrt[3]{4} \ \in \mathbb{Q}(\sqrt[3]{2})$
- $(p+q\sqrt[3]{2}+r\sqrt[3]{4})(k+l\sqrt[3]{2}+m\sqrt[3]{4}) = pk+2(qm+lr)+(pl+qk+2mr)\sqrt[3]{2}+(pm+ql+kr)\sqrt[3]{4} \ \in \mathbb{Q}(\sqrt[3]{2})$
- $(p+q\sqrt[3]{2}+r\sqrt[3]{4})^{-1} = \frac{p^2-2qr}{p^3+2q^3+4r^3-6pqr}+\frac{3r^2-pq}{p^3+2q^3+4r^3-6pqr}\sqrt[3]{2}+\frac{q^2-pr}{p^3+2q^3+4r^3-6pqr}\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$

2.2 Απλές επεκτάσεις

Οι πιο απλές επεκτάσεις είναι αυτές που δημιουργούνται από την προσθήκη ενός στοιχείου.

Ορισμός 2.2.1 *Μία απλή επέκταση είναι μία επέκταση $L : K$ έχοντας την ιδιότητα $L = K(\alpha)$ για κάποιο $\alpha \in L$.*

Παράδειγμα 2.2.1 *Οι επεκτάσεις $\mathbb{R}(i), K(t), \mathbb{Q}(\sqrt{2})$ είναι απλές επεκτάσεις.*

Παράδειγμα 2.2.2 *Μια επέκταση μπορει να είναι απλή χωρίς αυτό να φαίνεται. Για παράδειγμα έστω $L = \mathbb{Q}(i, -i, \sqrt{5}, -\sqrt{5})$ μια επέκταση του $\mathbb{Q}$. Όπως είναι γράμμένη μοιάζει με μια επέκταση που δημιουργείται από 4 στοιχεία. Θα*

αποδείξουμε όμως πως είναι ίδια με την απλή επέκταση $L' = \mathbb{Q}(i+\sqrt{5})$ *του* $\mathbb{Q}$. *Αρκεί να δείξουμε ότι* $i \in L'$ *και* $\sqrt{5} \in L'$ *γιατί τότε θα έχουμε* $L \subseteq L'$ *και* $L' \subseteq L$ *οπότε θα ισχύει* $L' = L$. *Το* $(i+\sqrt{5}) \in L'$ *επομένως το* L' *περιέχει και το*

$$(i+\sqrt{5})^2 = 4 + 2i\sqrt{5}.$$

Άρα το L' *θα περιέχει και το*

$$(i+\sqrt{5})(4+2i\sqrt{5}) = 14i - 2\sqrt{5}.$$

Άρα θα περιέχει και το

$$14i - 2\sqrt{5} + 2(i+\sqrt{5}) = 16i.$$

Το σώμα περιέχει το 1 άρα περιέχει και το

$$\underbrace{1+1+\ldots+1}_{16} = 16$$

συνεπώς θα περιέχει και το 16^{-1}. *Επομένως περιέχει το*

$$(16^{-1})(16i) = i$$

άρα θα περιέχει το i *και θα περιέχει και το* $(i+\sqrt{5}) - i = \sqrt{5}$. *Άρα τελικά* $L' = L$ *και η επέκταση* $\mathbb{Q}(i, -i, \sqrt{5}, -\sqrt{5}) : \mathbb{Q}$ *είναι απλή.*

Από την άλλη πλευρά η επέκταση $\mathbb{R} : \mathbb{Q}$ δεν είναι απλή κι αυτο γιατί το $\mathbb{Q}$ είναι αριθμήσιμο ενώ το $\mathbb{R}$ δεν είναι αριθμήσιμο.

Ορισμός 2.2.2 *Ένας ισομορφισμός μεταξύ δύο επεκτάσεων σωμάτων* $i : K \to K^*,\ j : L \to L^*$ *είναι ένα ζευγάρι* (λ, μ) *ισομορφισμών σωμάτων* $\lambda : K \to L,\ \mu : K^* \to L^*$, *έτσι ώστε* $\forall k \in K$ *να ισχύει:*

$$j(\lambda(k)) = \mu(i(k)).$$

Για να καταλάβουμε καλύτερα τον ορισμό μπορούμε να δούμε το παρακάτω σχημα.

$$\begin{array}{ccc} K & \stackrel{i}{\to} & K^* \\ \lambda \downarrow & & \downarrow \mu \\ L & \stackrel{\to}{j} & L^* \end{array}$$

Θα πρέπει τα δύο μονοπάτια από το K στο L^* να δινουν την ίδια συνάρτηση.

Ο λόγος που δώσαμε τον ορισμό με αυτό τον τρόπο είναι να καταλάβουμε πως όπως η δομή ενός σώματος διατηρείται κάτω από τον ισομορφισμό έτσι και η δημιουργία ενός σώματος από ένα μικρότερο σώμα γίνεται με τρόπο που να διατηρείται η δομή του μικρού σώματος. Αν ταυτήσουμε το K με το $i(K)$ και το L με το $j(L)$ τότε οι i, j είναι ένα προς ένα και η μεταθετική συνθήκη γίνεται

$$\mu|K = \lambda$$

όπου το $\mu|K$ συμβολίζει τον περιορισμό του μ στο K. Αν ταυτήσουμε το K με το L τότε ο λ γίνεται ο ταυτοτικός οπότε ο $\mu|K$ είναι ο ταυτοτικός.

2.3 Κατασκευή απλών επεκτάσεων

Έχουμε ήδη δει κάποιες απλές επεκτάσεις. Η επέκταση $\mathbb{C} = \mathbb{R}(i)$ δημιουργείται από το $\mathbb{R}$ προσθέτοντας ένα στοιχείο i το οποίο ικανοποιεί την πολυωνυμική σχέση $i^2 + 1 = 0$. Η επέκταση $\mathbb{Q}(t) : \mathbb{Q}$ δημιουργείται από το $\mathbb{Q}$ προσθέτοντας ένα στοιχείο t το οποίο δεν ικανοποιεί καμία πολυωνυμική σχέση αφού αν $p \in K[t]$ τότε $p(t) = 0$ αν και μόνο αν το p είναι το μηδενικο πολυώνυμο.

Ορισμός 2.3.1 *Έστω K(a):K μία απλή επέκταση. Αν υπάρχει ένα μη μηδενικό πολυώνυμο στο K έτσι ώστε να ισχύει $p(a) = 0$ τότε λέμε ότι το a είναι ένα αλγεβρικό στοιχείο στο K και η επέκταση $K(a) : K$ είναι μια απλή αλγεβρική επέκταση. Διαφορετικά λέμε ότι το a είναι υπερβατικό στο K και η K(a):K είναι μια απλή υπερβατική επέκταση.*

Στην περίπτωση της υπερβατικής επέκτασης η $K(t) : K$ είναι η μοναδική μέχρι ισομορφισμού απλή υπερβατική επέκταση του K. Αν K(α):K είναι αλγεβρική θα δείξουμε στη συνέχεια ότι υπάρχει ένα μοναδικό μονικό ανάγωγο πολυώνυμο m με συντελεστές από το K έτσι ώστε $m(a) = 0$ και αυτό το m καθορίζει την επέκταση μοναδικά στον ισομορφισμό. Θα δούμε στη συνέχεια πως κατασκευάζουμε απλές επεκτάσεις.

Θεώρημα 2.3.1 *Το σώμα των ρητών εκφρασεων $K(t)$ είναι μια απλή υπερβατική επέκταση του σώματος K.*

Απόδειξη: Είναι φανερά μια απλή επέκταση εφόσον δημιουργείται από ένα στοιχείο, το t. Αν p είναι ένα πολυώνυμο πάνω από το K έτσι ώστε $p(t) = 0$ τότε $p = 0$ από τον ορισμό του $K(t)$.□

Ορισμός 2.3.2 *Ένα πολυώνυμο*

$$a_0 + a_1 t + \ldots + a_n t^n$$

με συντελεστές από ένα σώμα K λέγεται μονικό αν $a_n = 1$.

Κάθε πολυώνυμο μπορεί να γραφεί σαν γινόμενο μονικών πολυωνύμων. Έστω $a_0 + a_1 t + \ldots + a_n t^n$ ένα πολυώνυμο με συντελεστές από ένα σώμα K. Μπορούμε να το γράψουμε ως εξής:

$$a_n(a_n^{-1}a_0 + a_n^{-1}a_1 t + \ldots + a_n^{-1}a_n t^n)$$

δηλαδή

$$a_n(a_n^{-1}a_0 + a_n^{-1}a_1 t + \ldots + t^n).$$

Εφόσον το K είναι σώμα για κάθε $a_i \in K$ υπάρχει ο αντίστροφός του $a_i^{-1} \in K$. Σε αυτή την περίπτωση θεωρούμε το a_n ως ένα σταθερό πολυώνυμο. Για ένα μη μηδενικό πολυώνυμο αυτά τα μονικά πολυώνυμα είναι μοναδικά, αφού για κάθε στοιχείο a_i υπάρχει μοναδικός αντίστροφος. Επιπλέον το γινόμενο δύο μονικών πολυωνύμων είναι μονικο αφού αν $f_1(t) = a_0 + a_1 t + \ldots + t^n$ και $f_2(t) = b_0 + b_1 t + \ldots + t^m$ είναι δυο μονικά πολυώνυμα τότε

$$f_1(t)f_2(t) = a_0 b_0 + \ldots + t^{n+m}$$

που είναι μονικό πολυώνυμο.
Θα αποδείξουμε ότι για κάθε απλή αλγεβρική επέκταση $K(a) : K$ υπάρχει ένα μοναδικό μονικό πολυώνυμο ελαχίστου βαθμού έτσι ώστε $p(a) = 0$. Έστω ότι $K(a) : K$ είναι μια απλή αλγεβρική επέκταση. Τότε υπάρχει ένα πολυώνυμο p με συντελεστές από το K έτσι ώστε $p(a) = 0$. Υποθέτουμε ότι αυτό το πολυώνυμο είναι μονικό. Από τα μονικά πολυώνυμα των οποίων είναι ρίζα το a επιλέγουμε εκείνο που είναι ελαχίστου βαθμού. Υποθέτουμε τώρα ότι υπάρχουν δύο τέτοια πολυώνυμα έστω p, q. Τότε θα πρέπει να ισχύει
$p(a) - q(a) = 0$. Αν $p \neq q$ τότε κάποιο πολλαπλάσιο του $p - q$ είναι μονικό πολυώνυμο. Αυτό όμως είναι άτοπο αφού υποθέσαμε ότι τα p, q είναι τα ελαχίστου βαθμού πολυώνυμα έτσι ώστε να ισχύει $p(a) = q(a) = 0$. Επομένως υπάρχει ένα μοναδικό μονικό πολυώνυμο p ελαχίστου βαθμού έτσι ώστε $p(a) = 0$.

Ορισμός 2.3.3 *Έστω $L : K$ μία επέκταση σώματος και υποθέτουμε ότι το $a \in L$ είναι αλγεβρικό στο σώμα K. Τότε το ελάχιστο πολυώνυμο του a με συντελεστές από το K είναι το μοναδικό μονικό πολυώνυμο m με συντελεστές από το K ελαχίστου βαθμού έτσι ώστε να ισχύει $m(a) = 0$.*

Παράδειγμα 2.3.1 *Έστω ότι έχουμε την επέκταση $\mathbb{R}(i) : \mathbb{R}$. Το $i \in \mathbb{C}$ είναι αλγεβρικό στο $\mathbb{R}$. Έστω $m(t) = t^2 + 1$, τότε $m(i) = 0$. Το m είναι μονικό πολυώνυμο. Τα μοναδικά μονικά πολυώνυμα με συντελεστές από το*

$\mathbb{R}$ μικρότερου βαθμού από το m είναι αυτά της μορφής $t + r$ $(r \in \mathbb{R})$ ή το 1. Όμως το i δεν μπορεί να είναι ρίζα κάποιου από αυτά γιατί τότε θα είχαμε $i \in \mathbb{R}$. Οπότε το ελάχιστο πολυώνυμο του i στο $\mathbb{R}$ είναι το $m(t) = t^2 + 1$.

Λήμμα 2.3.1 *Αν a είναι ένα αλγεβρικό στοιχείο σε ένα σώμα K, τότε το ελάχιστο πολυώνυμο του a στο K είναι ανάγωγο στο K. Επίσης διαιρεί κάθε πολυώνυμο του οποίου το a είναι ρίζα.*

Απόδειξη: Έστω ότι το ελάχιστο πολυώνυμο m του a στο K είναι παραγοντοποιήσιμο. Άρα μπορουμε να το γράψουμε $m = fg$ όταν f, g είναι πολυώνυμα μικρότερου βαθμού. Υποθέτουμε ότι τα f, g είναι μονικά. Εφόσον $m(a) = 0$ τότε $f(a)g(a) = 0$ και επομένως είτε $f(a) = 0$ είτε $g(a) = 0$. Αυτό είναι άτοπο γιατί τότε το m δεν είναι το ελάχιστο πολυώνυμο. Άρα το m είναι ανάγωγο στο K. Έστω τώρα ότι το p είναι ένα πολυώνυμο με συντελεστές από το K έτσι ώστε $p(a) = 0$. Το m είναι το ελάχιστο πολυώνυμο του a άρα $\partial m < \partial p$. Επομένως απο τον αλγόριθμο της διαίρεσης υπάρχουν πολυώνυμα q, r έτσι ώστε $p = mq + r$ και $\partial r < \partial m$. Άρα $0 = p(a) = m(a)q(a) + r(a)$, δηλαδή $r(a) = 0$. Αν $r \neq 0$ τότε είτε το r είτε κάποιος παράγοντάς του είναι μονικο πολυώνυμο και αυτό είναι άτοπο αφού ορίσαμε το m ως το ελάχιστο μονικό πολυώνυμο με ρίζα το a. Άρα $r = 0$ και επομένως το $m|p$.□

Στην συνέχεια θα δείξουμε ότι για κάθε σώμα K και κάθε ανάγωγο μονικό πολυώνυμο m με συντελεστές από το K μπορούμε να κατασκευάσουμε μια επέκταση $K(a) : K$ έτσι ώστε το a να έχει ελάχιστο πολυώνυμο το m στο K.

Έστω R και S δακτύλιοι και $\phi : R \to S$ ένας ομομορφισμός δακτυλίων. Ο πυρήνας του ϕ $(ker\phi)$ είναι

$$ker\phi = \{r \in R : \phi(r) = 0\}.$$

Ο $ker\phi$ είναι ένα ιδεώδες του R διότι αν $r_1, r_2 \in ker\phi$ και $a \in R$

- $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) = 0 + 0 = 0$ άρα $r_1 + r_2 \in ker\phi$
- $\phi(ar) = a\phi(r) = 0$ άρα $ar \in ker\phi$
- $\phi(ra) = \phi(r)a = 0$ άρα $ra \in ker\phi$

Επομένως ορίζεται ο δακτύλιος πηλίκο $R/ker\phi$ που είναι ισομορφικός με την εικόνα του ϕ. Λέμε ότι ο ϕ είναι μονομορφισμός αν είναι ένα προς ένα. Αυτό είναι ισοδύναμο με την σχέση $ker(\phi) = \{0\}$.

Λήμμα 2.3.2 *Αν ϕ είναι ένας ομομορφισμός δακτυλίων από ένα σώμα K σε ένα δακτύλιο R και $\phi \neq 0$ τότε ο ϕ είναι ένας μονομορφισμός.*

Απόδειξη: Ο πυρήνας του ϕ είναι ένα ιδεώδες του K. Όμως το K είναι ένα σώμα επομένως δεν έχει άλλα ιδεώδη εκτός από το 0 και τον εαυτό του K. Υποθέτουμε ότι $H \subseteq K$ είναι ένα ιδεώδες του K. Τότε ισχύει

$$kh \in H \qquad \forall h \in H,\ \forall k \in K$$

Όμως το $h \in H$ και το $h \in K$ και επειδή το K είναι σώμα και το $h^{-1} \in K$. Άρα αν πάρω $k = h^{-1}$ τότε

$$hh^{-1} \in H$$

δηλαδή

$$1 \in H.$$

Επειδή $1 \in H$ ισχύει

$$1k \in H \qquad \forall k \in K.$$

Άρα $H = K$. Επειδή $\phi \neq 0$ ο πυρήνας δεν είναι το K άρα θα πρέπει να είναι το 0. Εφόσον $ker\phi = \{0\}$ τότε ο ϕ είναι μονομορφισμός. □

Πρέπει να πούμε ότι αν το K είναι δακτύλιος το παραπάνω λήμμα δεν ισχύει. Για τον ομομορφισμό $\phi : \mathbb{Z} \to \mathbb{Z}_2$ ισχύει $\phi \neq 0$ αλλά δεν είναι μονομορφισμός.

Λήμμα 2.3.3 *Αν m είναι ένα ανάγωγο πολυώνυμο με συντελεστές από ένα σώμα K με $\partial m > 0$ και I είναι το ιδεώδες του $K[t]$ που αποτελείται από όλα τα πολλαπλάσια του m τότε ο δακτύλιος πηλίκο $K[t]/I$ είναι ένα σώμα.*

Απόδειξη: Έστω ότι το σύμπλοκο $I + f$ είναι ένα μη μηδενικό στοιχείο του $S = K[t]/I$. Εφόσον το m είναι ανάγωγο, τα m και f είναι πρώτα μεταξύ τους. Διαφορετικά θα είχαμε $f = km$ $(k \in K)$ οπότε $I + f = I + km = I$ που είναι άτοπο αφού υποθέσαμε ότι το $I + f$ είναι μη μηδενικό. Επομένως υπάρχουν a, b στο K έτσι ώστε να ισχύει:

$$af + bm = 1.$$

Τότε θα έχουμε:

$$(I + a)(I + f) + (I + b)(I + m) = I + 1.$$

Όμως ισχύει $I + m = I$ άρα το $I + m$ είναι το μηδενικό στοιχείο του S και το $I + 1$ είναι το ταυτοτικό στοιχείο του S. Άρα έχουμε

$$(I + a)(I + f) = I + 1.$$

Επομένως το αντίστροφο του $I + f$ είναι το $I + a$ και καταλήγουμε ότι το S είναι σώμα.□

Θεώρημα 2.3.2 *Αν K είναι ένα σώμα και m ένα ανάγωγο μονικό πολυώνυμο με συντελεστές από το K τότε υπάρχει μία επέκταση $K(a) : K$ έτσι ώστε το a να έχει ελάχιστο πολυώνυμο το m στο K.*

Απόδειξη: Υπάρχει ένας φυσικός μονομορφισμός $i : K \to K[t]$. Έστω I το ιδεώδες του $K[t]$ που αποτελείται από όλα τα πολλαπλάσια του m και $S = K[t]/I$. Έστω v ο φυσικός ομομορφισμός $K[t] \to S$. Από το λήμμα 2.3.3 το S είναι ένα σώμα και από το λήμμα 2.3.2 η σύνθετη σχέση vi είναι ένας μονομορφισμός. Ταυτίζουμε το K με την εικόνα του $v(i(K))$ και έστω $a = I + t$. Τότε παρατηρούμε ότι $S = K(a)$. Εφόσον το $m \in I$ έχουμε ότι $m(a) = I$ και το I είναι το μηδενικό στοιχείο του S. Εφόσον το m είναι ανάγωγο και μονικό θα πρέπει να είναι το ελάχιστο πολυώνυμο του α. Αν το p είναι το ελάχιστο πολυώνυμο τότε από το λήμμα 2.3.1 το $p|m$ άρα $p = m$.□

2.4 Κατηγοριοποίηση απλών επεκτάσεων

Θεώρημα 2.4.1 *Κάθε απλή υπερβατική επέκταση $K(a) : K$ είναι ισομορφική με την επέκταση $K(t) : K$ των ρητών εκφράσεων ενός απροσδιορίστου t στο K. Ο ισομορφισμός μπορεί να επιλεχθεί έτσι ώστε το t να πηγαίνει στο a.*

Απόδειξη: Ορίζουμε μία συνάρτηση $\phi : K(t) \to K(a)$ έτσι ώστε να ισχύει:

$$\phi(f(t)/g(t)) = f(a)/g(a).$$

Για να ορίζεται η συνάρτηση θα πρέπει η $g \neq 0$. Όμως το α είναι υπερβατικό άρα και $g(a) \neq 0$ οπότε ο παραπάνω ορισμός ισχύει. Ο ϕ είναι ομομορφισμός αφού

$$\phi(f_1(t)/g_1(t) + f_2(t)/g_2(t)) = \phi(f_1(t)/g_1(t)) + \phi(f_2(t)/g_2(t))$$

και

$$\phi((f_1(t)/g_1(t))(f_2(t)/g_2(t))) = \phi(f_1(t)/g_1(t))\phi(f_2(t)/g_2(t)).$$

Επίσης $f \neq 0$ οπότε $\phi \neq 0$ διότι $\phi(f(t)/g(t)) = f(a)/g(a)$ και από το λήμμα 2.3.2 ο ϕ είναι μονομορφισμός. Παρατηρούμε ότι ο ϕ είναι και επί άρα είναι ισομορφισμός. Επιπλέον ο $\phi|K$ είναι ο ταυτοτικός άρα ο ϕ ορίζει έναν ισομορφισμό επεκτάσεων. Άρα θα πρέπει το t να πηγαίνει στο α, δηλαδη $\phi(t) = a$.□

Λήμμα 2.4.1 *Έστω $K(a) : K$ μια απλή αλγεβρική επέκταση όπου το a έχει ελάχιστο πολυώνυμο το m στο K. Τότε κάθε στοιχείο του $K(a)$ έχει μία μοναδική έκφραση της μορφής $p(a)$ όπου p είναι ένα πολυώνυμο με συντελεστές από το K και $\partial p < \partial m$.*

Απόδειξη: Κάθε στοιχείο του $K(a)$ μπορεί να εκφραστεί στη μορφή $f(a)/g(a)$ όταν τα $f, g \in K[t]$ και $g(a) \neq 0$. Αυτό συμβαίνει γιατί το σύνολο όλων των στοιχείων της μορφής $f(a)/g(a)$ αποτελούν ένα σώμα που περιέχει το K και το a και υπάρχει μέσα στο $K(a)$. Εφόσον $g(a) \neq 0$ το m δεν διαιρεί το g και αφού το g είναι ανάγωγο τα m, g είναι πρώτα μεταξύ τους. Άρα υπάρχουν πολυώνυμα b, c πάνω από το K έτσι ώστε να ισχύει

$$bg + cm = 1.$$

Επειδή $m(a) = 0$ η σχέση γίνεται

$$b(a)g(a) = 1 \Leftrightarrow 1/g(a) = b(a).$$

Άρα έχουμε:

$$f(a)/g(a) = f(a)b(a) = h(a)$$

για κάποιο πολυώνυμο h πάνω από το K. Έστω r το υπόλοιπο της διαίρεσης του h με το m. Δηλαδή

$$h = mq + r$$

όπου r είναι ένα πολυώνυμο με συντελεστές από το K. Όμως $m(a) = 0$ άρα έχουμε $h(a) = r(a)$. Επειδή $\partial r < \partial m$ υπαρχει ένα τέτοιο πολυώνυμο. Θα αποδείξουμε τώρα την μοναδικότητα ενός τέτοιου πολυωνύμου για κάθε στοιχείο του $K(a)$. Έστω $f(a) = g(a)$ όταν $\partial f, \partial g < \partial m$. Αν $e = f - g$ τότε $e(a) = 0$ και $\partial e < \partial m$ που είναι άτοπο αφού υποθέσαμε ότι το m είναι το ελάχιστο πολυώνυμο του a.□

Παράδειγμα 2.4.1 *Έστω $K = \mathbb{R}$ και $m(t) = t^2 + t + 1$. Σύμφωνα με το προηγούμενο λήμμα αν το a έχει ελάχιστο πολυώνυμο το m στο K, τότε καθε στοιχείο του $K(a)$ είναι ένα πολυώνυμο του a βαθμού< 2. Έστω το στοιχείο $(3a^2+2)/(a+4)$. Θα το γράψουμε σε μορφή $p(a)$ όπου p είναι ένα πολυώνυμο με συντελεστές από το K. Αρχικά θα βρούμε πολυώνυμα p, q έτσι ώστε*

$$p(t + 4) + q(t^2 + t + 1) = 1.$$

$$t^2 + t + 1 = (t + 4)(t - 3) + 13$$

άρα

$$\frac{1}{13}(t^2 + t + 1) - (t - 3)/13(t + 4) = 1.$$

Δηλαδή

$$p = -\frac{1}{13}(t-3)$$

και

$$q = \frac{1}{13}.$$

Επειδή $a^2 + a + 1 = 0$ *θα έχουμε*

$$-\frac{1}{13}(a+4)(a-3) = 1$$

δηλαδή

$$1/(a+4) = -(a-3)/(13).$$

Άρα έχουμε

$$\begin{aligned}(3a^2+2)/(a+4) &= -\frac{1}{13}(3a^2+2)(a-3)\\ &= -\frac{1}{13}(3(-a-1)+2)(a-3)\\ &= -\frac{1}{13}(-3a^2+8a+3)\\ &= -\frac{1}{13}(11a+6)\\ &= -\frac{11}{13}a - \frac{6}{13}.\end{aligned}$$

Θεώρημα 2.4.2 *Έστω K(a):K και K(β):K απλές αλγεβρικές επεκτάσεις έτσι ώστε τα a και β έχουν το ίδιο ελάχιστο πολυώνυμο m στο K. Τότε οι δύο επεκτάσεις είναι ισομορφικές και ο ισομορφισμός των μεγάλων σωμάτων είναι τέτοιος ώστε να πηγαίνει το a στο β.*

Απόδειξη: Από το λήμμα 2.4.1 κάθε στοιχείο $x \in K(a)$ μπορεί να εκφραστεί μοναδικά στη μορφή

$$x = x_0 + x_1 a + \ldots + x_n a^n \qquad (x_1, \ldots, x_n \in K)$$

όταν $n = \partial m - 1$. Ορίζουμε μια συνάρτηση $\phi : K(a) \to K(\beta)$ έτσι ώστε

$$\phi(x) = x_0 + x_1\beta + \ldots + x_n\beta^n.$$

Από το λήμμα 2.4.1 η ϕ είναι ένα προς ένα και επί. Επίσης ισχύει

$$\begin{aligned}\phi(x+y) &= x_0 + y_0 + (x_1+y_1)\beta + \ldots + (x_n+y_n)\beta^n\\ &= x_0 + x_1\beta + \ldots + x_n\beta^n + y_0 + y_1\beta + \ldots + y_n\beta^n\\ &= \phi(x) + \phi(y)\end{aligned}$$

Θα δείξουμε ότι

$$\phi(xy) = \phi(x)\phi(y)$$

για κάθε $x, y \in K(a)$. Έστω $x = f(a)$, $y = g(a)$, $xy = h(a)$ όταν f, g, h είναι πολυώνυμα με συντελεστές από το K βαθμού $< \partial m$. Τότε

$$f(a)g(a) - h(a) = xy - xy = 0.$$

Από το λήμμα 2.3.1, το m διαιρεί το $fg - h$ άρα υπάρχει ένα πολυώνυμο q στο K έτσι ώστε $fg = mq + h$. Εφόσον $\partial h < \partial m$ προκύπτει ότι το h είναι το υπόλοιπο της διαίρεσης του fg με το m. Επομένως έχουμε

$$f(\beta)g(\beta) = h(\beta)$$

οπότε

$$\phi(xy) = h(\beta) = f(\beta)g(\beta) = \phi(x)\phi(y)$$

και άρα ο ϕ είναι ένας ισομορφισμός. Εφόσον ο ϕ είναι ο ταυτοτικός στο K οι δύο επεκτάσεις είναι ισομορφικές. Άρα θα πρέπει το a να πηγαίνει στο β, δηλαδή $\phi(a) = \beta$.□

Ορισμός 2.4.1 *Έστω $i : K \to L$ ένας μονομορφισμός σωμάτων. Υπάρχει ένας μονομορφισμός $\hat{\imath} : K[t] \to L[t]$ έτσι ώστε*

$$\hat{\imath}(k_0 + k_1 t + \ldots + k_n t^n) = i(k_0) + i(k_1)t + \ldots + i(k_n)t^n$$

όταν $k_0, \ldots, k_n \in K$. Αν ο i είναι ένας ισομορφισμός τότε και ο $\hat{\imath}$ είναι ισομορφισμός.

Στην συνέχεια θα χρησιμοποιούμε το ίδιο σύμβολο i για την συνάρτηση μεταξύ των σωμάτων και μεταξύ των επεκτάσεων στους δακτύλιους πολυωνύμων τους. Δηλαδη ισχύει $\hat{\imath}(k) = i(k) \ \ \forall k \in K$.

Θεώρημα 2.4.3 *Έστω ότι K και L είναι σώματα και $i : K \to L$ είναι ένας ισομορφισμός. Έστω $K(a)$ και $L(\beta)$ απλές επεκτάσεις των K και L έτσι ώστε το a να έχει ελάχιστο πολυώνυμο το $m_a(t)$ στο K και το β να έχει ελάχιστο πολυώνυμο το $m_\beta(t)$ στο L. Υποθέτουμε επιπλέον ότι $m_\beta(t) = i(m_a(t))$. Τότε υπάρχει ένας ισομορφισμός $j : K(a) \to L(\beta)$ έτσι ώστε $j|K = i$ και $j(a) = \beta$.*

Απόδειξη: Από το λήμμα 2.4.1 κάθε στοιχείο $x \in K(a)$ μπορεί να εκφραστεί μοναδικά στη μορφή

$$x = x_0 + x_1 a + \ldots + x_n a^n \qquad (x_1, \ldots, x_n \in K)$$

και κάθε στοιχείο $y \in L(\beta)$ μπορεί να εκφραστεί μοναδικά στη μορφή

$$y = y_0 + y_1\beta + \ldots + y_r\beta^r \qquad (y_1, \ldots, y_r \in L)$$

όταν $n = \partial m_a - 1$ και $r = \partial m_\beta - 1$. Από τον ορισμό 2.4.1 υπάρχει ένας μονομορφισμός $i : K(a) \to L(a)$ έτσι ώστε

$$i(x_0 + x_1a + \ldots + x_na^n) = i(x_0) + i(x_1)a + \ldots + i(x_n)a^n.$$

Ορίζουμε μια συνάρτηση $j : K(a) \to L(\beta)$ έτσι ώστε

$$j(x) = i(x_0) + i(x_1)\beta + \ldots + i(x_n)\beta^n.$$

Από το λήμμα 2.4.1 κάθε στοιχείο του $L(\beta)$ έχει μοναδική έκφραση της μορφής $p(\beta)$ όπου p είναι ένα πολυώνυμο με συντελεστές από το L. Άρα ο j είναι ένα προς ένα και επί. Επίσης
$\forall z = z_0 + z_1\beta + \ldots + z_r\beta^r,\ y = y_0 + y_1\beta + \ldots + y_r\beta^r \in L(\beta)$ ισχύει

$$\begin{aligned} j(z+y) &= z_0 + y_0 + (z_1 + y_1)\beta + \ldots + (z_r + y_r)\beta^r \\ &= z_0 + z_1\beta + \ldots + z_r\beta^r + y_0 + y_1\beta + \ldots + y_r\beta^r \\ &= j(z) + j(y) \end{aligned}$$

Θα δείξουμε ότι

$$j(zy) = j(z)j(y)$$

για κάθε $z, y \in L(\beta)$. Έστω $z = f(\beta)$, $y = g(\beta)$, $zy = h(\beta)$ όταν f, g, h είναι πολυώνυμα με συντελεστές από το L βαθμού $< \partial m_\beta$. Τότε

$$f(\beta)g(\beta) - h(\beta) = zy - zy = 0.$$

Από το λήμμα 2.3.1, το m_β διαιρεί το $fg - h$ άρα υπάρχει ένα πολυώνυμο q με συντελεστές από το L έτσι ώστε $fg = m_\beta q + h$. Εφόσον $\partial h < \partial m_\beta$ προκύπτει ότι το h είναι το υπόλοιπο της διαίρεσης του fg με το m_β. Επομένως έχουμε

$$f(\beta)g(\beta) = h(\beta)$$

οπότε

$$j(zy) = h(\beta) = f(\beta)g(\beta) = j(z)j(y)$$

και άρα ο j είναι ένας ισομορφισμός. Εφόσον ο j είναι ο ταυτοτικός στο K οι δύο επεκτάσεις είναι ισομορφικές. Άρα θα πρέπει το a να πηγαίνει στο β, δηλαδή $j(a) = \beta$. Το παραπάνω θεώρημα μας δείχνει ότι κάτω από τις δεδομένες συνθήκες οι επεκτάσεις $K(a) : K$ και $L(\beta) : L$ είναι ισομορφικές. Αυτό

μας επιτρέπει να ταυτήσουμε το K με το L και το $K(a)$ με το $L(\beta)$ μέσω των συναρτήσεων i και j.□

Παράδειγμα 2.4.2 *Βρείτε τα υποσώματα του* $\mathbb{C}$ *που παράγονται από*
(a) $\{0,\ 1\}$
(b) $\{0\}$
(c) $\{0,\ 1,\ i\}$
(d) $\{i,\ \sqrt{2}\}$
(e) $\{\sqrt{2},\ \sqrt{3}\}$
(f) $\mathbb{R}$
(g) $\mathbb{R} \cup \{i\}$

Απάντηση:
(a) $\mathbb{Q}$
(b) $\{0\}$
(c) $\{p + qi : p,\ q \in \mathbb{Q}\}$
(d) $\{p + q\sqrt{2} + ri + si\sqrt{2} : p,\ q,\ r,\ s \in \mathbb{Q}\}$
(e) $\{p + q\sqrt{2} + r\sqrt{3} + s\sqrt{6} : p,\ q,\ r,\ s \in \mathbb{Q}\}$
(f) $\mathbb{R}$
(g) $\mathbb{C}$

Παράδειγμα 2.4.3 *Περιγράψτε τα υποσώματα του* $\mathbb{C}$ *της μορφής*
(a) $\mathbb{Q}(\sqrt{2})$
(b) $\mathbb{Q}(i)$
(c) $\mathbb{Q}(a)$ *όταν το* a *είναι η κυβική ρίζα του 2* $(\sqrt[3]{2})$
(d) $\mathbb{Q}(\sqrt{5},\ \sqrt{7})$
(e) $\mathbb{Q}(i\sqrt{11})$

Απάντηση:
(a) $\{p + q\sqrt{2} : p,\ q \in \mathbb{Q}\}$
(b) $\{p + qi : p,\ q \in \mathbb{Q}\}$
(c) $\{p + qa + ra^2 : p,\ q,\ r \in \mathbb{Q}\}$
(d) $\{p + q\sqrt{5} + r\sqrt{7} + s\sqrt{35} : p,\ q,\ r,\ s \in \mathbb{Q}\}$
(e) $\{p + qi\sqrt{11} : p,\ q \in \mathbb{Q}\}$

Παράδειγμα 2.4.4 *Έστω* $K = \mathbb{Z}_2$. *Περιγράψτε τα υποσώματα του* $K(t)$ *της μορφής:*
(a) $K(t^2)$
(b) $K(t + 1)$

(c) $K(t^5)$
(d) $K(t^2+1)$

Απάντηση:
(a) $\frac{a_0+a_1t^2+...+a_nt^{2n}}{b_0+b_1t^2+...+b_mt^{2m}}$ όπου $a_i,\ b_i \in \{0,\ 1\}$ και $m,\ n \in \{0,\ 1,\ 2, \ldots\}$

(b) $\frac{a_0+a_1t+...+a_nt^n}{b_0+b_1t+...+b_mt^m}$ όπου $a_i,\ b_i \in \{0,\ 1\}$ και $m,\ n \in \{0,\ 1,\ 2, \ldots\}$

(c) $\frac{a_0+a_1t^5+...+a_nt^{5n}}{b_0+b_1t^5+...+b_mt^{5m}}$ όπου $a_i,\ b_i \in \{0,\ 1\}$ και $m,\ n \in \{0,\ 1,\ 2, \ldots\}$

(d) $\frac{a_0+a_1t^2+...+a_nt^{2n}}{b_0+b_1t^2+...+b_mt^{2m}}$ όπου $a_i,\ b_i \in \{0,\ 1\}$ και $m,\ n \in \{0,\ 1,\ 2, \ldots\}$

Παράδειγμα 2.4.5 *Δείξτε ότι η επέκταση* $\mathbb{Q}(i,\ \sqrt{2})$ *είναι απλή.*

Απάντηση:
$(i+\sqrt{2})^2 = 1+2i\sqrt{2}\ \in \mathbb{Q}(i+\sqrt{2})$
$(1+2i\sqrt{2})(i+\sqrt{2}) = 5i-\sqrt{2}\ \in \mathbb{Q}(i+\sqrt{2})$
Άρα $i \in \mathbb{Q}(i+\sqrt{2})$
$i+\sqrt{2}-i = \sqrt{2}\ \in \mathbb{Q}(i+\sqrt{2})$
Άρα τα $i,\ \sqrt{2}\ \in \mathbb{Q}(i+\sqrt{2})$
Επομένως $\mathbb{Q}(i,\ \sqrt{2}) = \mathbb{Q}(i+\sqrt{2})$ και άρα η $\mathbb{Q}(i,\ \sqrt{2})$ είναι απλή.

Κεφάλαιο 3

Ο βαθμός μιας επέκτασης

Σε αυτό το κεφάλαιο θα αξιοποιήσουμε την τεχνική κατα την οποία συσχετίζουμε με κάθε επέκταση σωμάτων ένα διανυσματικό χώρο.

3.1 Ο νόμος του πύργου

Στο παρακάτω θεώρημα θα ορίσουμε τη δομή ενός διανυσματικού χώρου σε μιά επέκταση σωμάτων.

Θεώρημα 3.1.1 *Αν $L : K$ είναι μια επέκταση σωμάτων οι πράξεις*

$$\begin{aligned} (\lambda,\ u) &\rightarrow \lambda u \qquad (\lambda \in K,\ u \in L) \\ (u,\ v) &\rightarrow u + v \qquad (u,\ v \in L) \end{aligned}$$

ορίζουν στο L την δομή ενός διανυσματικού χώρου με βαθμωτό πολλαπλασιασμό από το σώμα το K.

Απόδειξη: Το σώμα L με τις παραπάνω πράξεις είναι διανυσματικός χώρος με σώμα το K διότι ισχύουν τα παρακάτω αξιώματα:

1. $\forall\ u, v, z \in L \quad u + (v + z) = (u + v) + z.$
2. $\forall\ u, v \in L \quad u + v = v + u.$
3. $\exists\ 0 \in L : \forall\ u \in L \quad u + 0 = 0 + u = u.$
4. $\forall\ u \in L,\ \exists\ u' = -u \in L : u + u' = u' + u = 0.$
5. $\forall\ k \in K,\ \forall\ u, v \in L \quad k(u + v) = ku + kv.$

6. $\forall\ k, \lambda \in K,\ \forall\ u \in L \quad (k+\lambda)u = ku + \lambda u.$

7. $\forall\ k, \lambda \in K,\ \forall\ u \in L \quad k(\lambda u) = (k\lambda)u.$

8. $\forall\ u \in L,\ \exists\ 1 \in L : 1u = u1 = u.$ □

Ένας διανυσματικός χώρος με ένα σώμα ορίζεται μοναδικά ως προς τον ισομορφισμό από την διάστασή του.

Ορισμός 3.1.1 *Ο βαθμός $[L : K]$ μιας επέκτασης σώματος $L : K$ είναι η διάσταση του L αν θεωρηθεί ως ένας διανυσματικός χώρος με σώμα το K.*

Παράδειγμα 3.1.1 *Το σύνολο των μιγαδικών αριθμών $\mathbb{C}$ είναι διάστασης δύο με σώμα το σώμα των πραγματικών αριθμών $\mathbb{R}$ αφού το $\{1,\ i\}$ είναι μια βάση του $\mathbb{C}$. Επομένως $[\mathbb{C} : \mathbb{R}] = 2$.*

Παράδειγμα 3.1.2 *Ο $[\mathbb{C}(t) : \mathbb{C}]$ είναι άπειρος διότι η διάσταση του $\mathbb{C}(t)$ με σώμα το $\mathbb{C}$ είναι άπειρη αφού τα $1, t, t^2, \ldots$ είναι μια βάση του $\mathbb{C}(t)$.*

Παράδειγμα 3.1.3 *Έστω K το σώμα που ορίζεται από τους παρακάτω πίνακες και έστω $P = \{0, 1\}$ το πρώτο του υπόσωμα το οποίο είναι ισομορφικό με το $\mathbb{Z}_2$.*

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$.$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Τα στοιχεία $\{1, a\}$ αποτελούν μια βάση για το K με σώμα το P, άρα $[K : P] = 2$.

Είναι φανερό ότι ισομορφικές επεκτάσεις σωμάτων έχουν τον ίδιο βαθμό.

Το επόμενο θεώρημα είναι γνωστό ώς νόμος του πύργου και μας επιτρέπει να υπολογίζουμε τον βαθμό σύνθετων επεκτάσεων αν γνωρίζουμε τους βαθμούς κάποιων απλούστερων από αυτές.

Θεώρημα 3.1.2 *Αν K, L, M είναι σώματα και $K \subseteq L \subseteq M$ τότε*

$$[M : K] = [M : L][L : K].$$

Στην περίπτωση που κάποιος από τους βαθμούς είναι άπειρος τότε έχουμε: Αν $[M : L] = \infty$ ή $[L : K] = \infty$ τότε $[M : K] = \infty$ και αν $[M : K] = \infty$ τότε $[M : L] = \infty$ ή $[L : K] = \infty$.

Απόδειξη: Έστω $(x_i)_{i\in I}$ είναι μια βάση του L ως διάνυσματικού χώρου με σώμα το K και έστω $(y_j)_{j\in J}$ μια βάση για το M με σώμα το L. Αρκεί να δείξουμε ότι η $(x_i y_j)_{i\in I, j\in J}$ είναι μια βάση για το M με σώμα το K ($x_i y_j$ είναι γινόμενο μέσα στο σώμα M). Θα πρέπει να δείξουμε ότι τα στοιχεία της βάσης είναι γραμμικά ανεξάρτητα. Έστω ότι για κάποια πεπερασμένα στοιχεία x_i, y_j ισχύει

$$\sum_{i,j} k_{ij} x_i y_j = 0 \quad (k_{ij} \in K).$$

Αυτό μπορούμε να το γράψουμε ως

$$\sum_j \left(\sum_i k_{ij} x_i \right) y_j = 0.$$

Εφόσον οι συντελεστές $\sum_i k_{ij} x_i$ είναι μέσα στο L και τα y_j είναι γραμμικά ανεξάρτητα θα πρέπει να ισχύει

$$\sum_i k_{ij} x_i = 0.$$

Εφόσον τα x_i είναι γραμμικά ανεξάρτητα θα πρέπει να ισχύει

$$k_{ij} = 0.$$

Επαναλαμβάνοντας την ίδια διαδικασία για όλα τα x_i, y_j καταλήγουμε ότι $k_{ij} = 0 \quad \forall i \in I$ και $\forall j \in J$. Άρα τελικά τα $x_i y_j$ είναι γραμμικά ανεξάρτητα στο K.

Στη συνέχεια θα πρέπει να δείξουμε ότι τα $x_i y_j$ παράγουν τον M με σώμα το K. Κάθε στοιχείο $x \in M$ μπορεί να γραφεί στη μορφή

$$x = \sum_j \lambda_j y_j$$

για κάποια $\lambda_j \in L$, εφόσον τα y_j παράγουν τον M με σώμα το L. Επίσης για κάθε $j \in J$

$$\lambda_j = \sum_i \lambda_{ij} x_i$$

για κάποια $\lambda_{ij} \in K$ διότι τα x_i παράγουν τον L με σώμα το K. Από τις δύο παραπάνω σχέσεις παίρνουμε την εξής

$$x = \sum_{i,j} k_{ij} x_i y_j$$

και άρα τα $x_i y_j$ παράγουν τον M με σώμα το K.□

Παράδειγμα 3.1.4 *Έστω ότι θέλουμε να βρούμε τον βαθμό* $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}]$. *Κάθε στοιχείο του* $\mathbb{Q}(\sqrt{2})$ *γράφεται στη μορφη* $p+q\sqrt{2}$ *όπου* $p, q \in \mathbb{Q}$. *Άρα το σύνολο* $\{1, \sqrt{2}\}$ *παράγει τον* $\mathbb{Q}(\sqrt{2})$. *Θα πρέπει επίσης να δείξουμε ότι τα* $1, \sqrt{2}$ *είναι γραμμικά ανεξάρτητα στο* $\mathbb{Q}$. *Έστω* $p+q\sqrt{2} = 0$ *όπου* $p, q \in \mathbb{Q}$. *Αν* $q \neq 0$ *τότε θα πρέπει* $p/q = -\sqrt{2}$, *που είναι άτοπο αφού το* $-\sqrt{2} \notin \mathbb{Q}$. *Άρα* $q = 0$ *συνεπώς* $p = 0$, *δηλαδή τα* $1, \sqrt{2}$ *είναι γραμμικά ανεξάρτητα. Άρα τα* $\{1, \sqrt{2}\}$ *είναι μια βάση του* $\mathbb{Q}(\sqrt{2})$ *με σώμα το* $\mathbb{Q}$. *Επομένως η διάσταση του* $\mathbb{Q}(\sqrt{2})$ *ως διανυσματικός χώρος με σώμα το* $\mathbb{Q}$ *είναι 2 και άρα* $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. *Με τον ίδιο τρόπο μπορούμε να δείξουμε ότι τα* $\{1, \sqrt{3}\}$ *είναι μια βάση για τον* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ *με σώμα το* $\mathbb{Q}(\sqrt{2})$. *Κάθε στοιχείο του* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ *μπορεί να γραφεί στη μορφή*

$$p + q\sqrt{2} + r\sqrt{3} + s\sqrt{6}$$

όπου τα $p,\ q,\ r,\ s \in \mathbb{Q}$. *Μπορούμε να γράψουμε την παραπάνω σχέση ως εξής*

$$(p + q\sqrt{2}) + (r + s\sqrt{2})\sqrt{3}.$$

Παρατηρούμε ότι τα $\{1, \sqrt{3}\}$ *παράγουν τον* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ *με σώμα το* $\mathbb{Q}(\sqrt{2})$. *Μένει να δείξουμε την γραμμική ανεξαρτησία των* $\{1, \sqrt{3}\}$. *Έστω*

$$(p + q\sqrt{2}) + (r + s\sqrt{2})\sqrt{3} = 0$$

τότε

$$p + q\sqrt{2} = 0 \ \textit{και}\ r + s\sqrt{2} = 0$$

ή

$$-\sqrt{3} = (p + q\sqrt{2})/(r + s\sqrt{2}) \ \in \mathbb{Q}(\sqrt{2}).$$

Αν $-\sqrt{3} = (p + q\sqrt{2})/(r + s\sqrt{2})$ *τότε*

$$-\sqrt{3} = a + b\sqrt{2}$$

όπου τα $a, b \in \mathbb{Q}$. *Αν υψώσουμε στο τετράγωνο την τελευταία σχέση έχουμε*

$$3 = a^2 + 2b^2 + 2\sqrt{2}ab$$

άρα θα πρέπει το $\sqrt{2}ab$ *να είναι ρητός που συμβαίνει μόνο όταν* $a = b = 0$. *Επομένως ισχύει* $p + q\sqrt{2} = 0$ *και* $r + s\sqrt{2} = 0$ *και άρα τα* $\{1, \sqrt{3}\}$ *είναι γραμμικά ανεξάρτητα. Τελικά αποδείξαμε ότι τα* $\{1, \sqrt{3}\}$ *είναι μια βάση του* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ *με σώμα το* $\mathbb{Q}(\sqrt{2})$. *Άρα* $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. *Τελικά έχουμε*

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4.$$

Πρόταση 3.1.1 *Έστω* $K(a) : K$ *μια απλή επέκταση. Αν είναι υπερβατική τότε* $[K(a) : K] = \infty$. *Αν είναι αλγεβρική τότε* $[K(a) : K] = \partial m$ *όπου* m *είναι το ελάχιστο πολυώνυμο του* a *στο* K.

Απόδειξη: Για την υπερβατικη περίπτωση αρκεί να πούμε ότι τα στοιχεία $1,\ a,\ a^2,\ \ldots$ είναι γραμμικά αναξάρτητα στο K. Για την αλγεβρική περίπτωση αρκεί να βρούμε μια βάση. Έστω $\partial m = n$ και έστω τα στοιχεία $1,\ a,\ a^2,\ \ldots,\ a^{n-1}$. Από το λήμμα 2.4.1 συμπεραίνουμε κάθε στοιχείο του K(α) μπορεί να γραφεί ως γραμμικός συνδυασμός αυτών των στοιχείων. Επομένως τα στοιχεία παράγουν τον K(α) με σώμα το K. Επίσης από το λήμμα 2.4.1 γνώρίζουμε πως κάθε στοιχείο του K(α) μπορεί να γραφεί ως γραμμικός συνδυασμός αυτών των στοιχείων με μοναδικό τρόπο. Δηλαδή αν $x = x_0 + x_1 a + \ldots + x_{n-1}a^{n-1}$ και $x = y_0 + y_1 a + y_{n-1}a^{n-1}$ τότε θα πρέπει $x_i = y_i\ \forall i$.

$$x - x = x_0 - y_0 + (x_1 - y_1)a + \ldots + (x_{n-1} - y_{n-1})a^{n-1}$$

δηλαδή

$$0 = x_0 - y_0 + (x_1 - y_1)a + \ldots + (x_{n-1} - y_{n-1})a^{n-1}.$$

Επειδη $x_i = y_i\ \forall i$ έχουμε ότι $x_i - y_i = 0\ \forall i$ άρα τα $1,\ a,\ a^2,\ \ldots,\ a^{n-1}$ είναι γραμμικά ανεξάρτητα.□

Παράδειγμα 3.1.5 *Έστω* $\mathbb{C} = \mathbb{R}(i)$. *Το ελάχιστο πολυώνυμο του* i *με σώμα το* $\mathbb{R}$ *είναι το* $t^2 + 1$ *που είναι βαθμού 2. Άρα* $[\mathbb{C} : \mathbb{R}] = 2$ *όπως είχαμε βρει και σε προηγούμενο παράδειγμα με διαφορετικό τρόπο.*

Ορισμός 3.1.2 *Πεπερασμένη επέκταση λέγεται μια επέκταση της οποίας ο βαθμός είναι πεπερασμένος.*

Ορισμός 3.1.3 *Μία επέκταση* $L : K$ *είναι αλγεβρική αν κάθε στοιχείο του* L *είναι αλγεβρικό στο* K.

Οι αλγεβρικές επεκτάσεις δεν είναι πάντα πεπερασμένες. Όμως κάθε πεπερασμένη επέκταση είναι αλγεβρική.

Λήμμα 3.1.1 *Η $L : K$ είναι μια πεπερασμένη επέκταση αν και μόνο αν το L είναι αλγεβρικό στο K και υπάρχουν πεπερασμένα στοιχεία $a_1, \ldots, a_s \in L$ έτσι ώστε να ισχύει $L = K(a_1, \ldots, a_s)$.*

Απόδειξη: Έστω η επέκταση $L = K(a_1, \ldots, a_s)$. Τότε

$$\begin{aligned} [L : K] &= [K(a_1, \ldots, a_s) : K(a_1, \ldots, a_{s-1})] \\ & \quad [K(a_1, \ldots, a_{s-1}) : K(a_1, \ldots, a_{s-2})] \\ &\ldots \quad [K(a_1, a_2) : K(a_1)][K(a_1) : K] \\ &= \partial m_s \partial m_{s-1} \ldots \partial m_2 \partial m_1 \end{aligned}$$

όπου ∂m_i είναι το ελάχιστο πολυώνυμο του a_i στο $K(a_1, \ldots, a_{i-1})$ για $i = 2, 3, \ldots, s$ και m_1 είναι το ελάχιστο πολυώνυμο του a_1 στο K. Άρα η επέκταση είναι πεπερασμένη.
Αντίστροφα, έστω $L : K$ μια πεπερασμένη επάκταση. Εφόσον είναι πεπερασμένη υπάρχει μια βάση $\{a_1, \ldots, a_s\}$ για το L έτσι ώστε $L = K(a_1, \ldots, a_s)$. Μένει να δείξουμε ότι η επέκταση είναι αλγεβρική. Έστω x κάποιο στοιχείο του L και έστω $n = [L : K]$. Το σύνολο $\{1, x, \ldots, x^n\}$ περιέχει $n + 1$ στοιχεία τα οποία θα πρέπει να είναι γραμμικά εξαρτημένα στο K. Άρα

$$k_0 + k_1 x + \ldots + k_n x^n = 0$$

για κάποια $k_0, k_1, \ldots, k_n \in K$ άρα το x είναι αλγεβρικό στο K.□

3.2 Αλγεβρικοί αριθμοί

Έστω A το σύνολο όλων των μιγαδικών αριθμών που είναι αλγεβρικοί στο $\mathbb{Q}$. Τα στοιχεία του A ονομάζονται αλγεβρικοί αριθμοί. Στη συνέχεια θα δείξουμε ότι το σύνολο αυτών των στοιχείων αποτελεί ένα σώμα. Από το λήμμα 4.1.1 γνωρίζουμε ότι ένα στοιχείο a που ανήκει στο A είναι αλγεβρικό αν και μόνο αν $[\mathbb{Q}(a) : \mathbb{Q}] < \infty$. Έστω a, β δύο στοιχεία του A. Τότε

$$[\mathbb{Q}(a, \beta) : \mathbb{Q}] = [\mathbb{Q}(a, \beta) : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}] < \infty.$$

Επίσης έχουμε

- $[\mathbb{Q}(a + \beta) : \mathbb{Q}] = [\mathbb{Q}(a, \beta) : \mathbb{Q}] < \infty$
- $[\mathbb{Q}(-a) : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}] < \infty$
- $[\mathbb{Q}(a\beta) : \mathbb{Q}] = [\mathbb{Q}(a, \beta) : \mathbb{Q}] < \infty$

- $[\mathbb{Q}(a^{-1}) : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}] < \infty \quad a \neq 0$

Επομένως τα $a + \beta$, $-a$, $a\beta$, a^{-1} ανήκουν στο Α και άρα το Α είναι σώμα.

Το Α είναι μια αλγεβρική επέκταση του $\mathbb{Q}$ αφού κάθε στοιχείο του είναι αλγεβρικό στο $\mathbb{Q}$. Όμως δεν μπορούμε να δείξουμε ότι ο βαθμός αυτής της επέκτασης είναι πεπερασμένος. Άρα μια αλγεβρική επέκταση δεν είναι απαραίτητα πεπερασμένη.

Παράδειγμα 3.2.1 *Βρείτε τους βαθμούς των παρακάτω επεκτάσεων*
(a) $\mathbb{C} : \mathbb{Q}$
(b) $\mathbb{Z}_5(t) : \mathbb{Z}_5$
(c) $\mathbb{R}(\sqrt{5}) : \mathbb{R}$
(d) $\mathbb{Q}(a) : \mathbb{Q}$ *όπου* $a = \sqrt[3]{2}$
(e) $\mathbb{Q}(3,\ \sqrt{5},\ \sqrt{11}) : \mathbb{Q}$
(f) $\mathbb{Q}(\sqrt{6}) : \mathbb{Q}$
(g) $\mathbb{Q}(a) : \mathbb{Q}$ *όπου* $a^7 = 3$

Απάντηση:
(a) $[\mathbb{C} : \mathbb{Q}] = [\mathbb{C} : \mathbb{R}][\mathbb{R} : \mathbb{Q}] = 2 \cdot \infty = \infty$. Διότι είδαμε ότι η επέκταση $[\mathbb{R} : \mathbb{Q}]$ είναι υπερβατική.

(b) $[\mathbb{Z}_5(t) : \mathbb{Z}_5] = \infty$. Διότι τα $\{1, t, t^2, \ldots\}$ είναι μια βάση του $\mathbb{Z}_5[t]$ με σώμα το $\mathbb{Z}_5$.

(c) $[\mathbb{R}(\sqrt{5}) : \mathbb{R} = 1]$. Διότι $\sqrt{5} \in \mathbb{R}$.

(d) $[\mathbb{Q}(a) : \mathbb{Q}] = 3$. Διότι τα $\{1, a, a^2\}$ είναι μια βάση του $\mathbb{Q}(a)$ με σώμα το $\mathbb{Q}$.

(e) $[\mathbb{Q}(3,\ \sqrt{5},\ \sqrt{11}) : \mathbb{Q}] = 4$. Διότι τα $\{1, \sqrt{5}, \sqrt{11}, \sqrt{55}\}$ είναι μια βάση του $\mathbb{Q}(3,\ \sqrt{5},\ \sqrt{11})$ με σώμα το $\mathbb{Q}$.

(f) $[\mathbb{Q}(\sqrt{6}) : \mathbb{Q}] = 2$. Διότι τα $\{1, \sqrt{6}\}$ είναι μια βάση του $\mathbb{Q}(\sqrt{6})$ με σώμα το $\mathbb{Q}$.

(g) $[\mathbb{Q}(a) : \mathbb{Q}] = 7$. Διότι τα $\{1, a, a^2, a^3, a^4, a^5, a^6\}$ είναι μια βάση του $\mathbb{Q}(a)$ με σώμα το $\mathbb{Q}$.

Παράδειγμα 3.2.2 *Δείξτε ότι κάθε στοιχείο του* $\mathbb{Q}(\sqrt{5},\ \sqrt{7})$ *μπορεί να εκφραστεί μοναδικά στη μορφη*

$$p + q\sqrt{5} + r\sqrt{7} + s\sqrt{35}$$

όπου $p,\ q,\ r,\ s \in \mathbb{Q}$. *Υπολογίστε τον αντίστροφο ενός τέτοιου στοιχείου.*

Απάντηση:
Αρχικά θα δείξουμε ότι τα $\{1,\ \sqrt{5}\}$ αποτελούν βάση του $\mathbb{Q}(\sqrt{5})$ με σώμα το $\mathbb{Q}$. Έστω $p+q\sqrt{5}=0$ όπου $p,q\in\mathbb{Q}$. Αν $q\neq 0$ τότε θα πρέπει $p/q=-\sqrt{5}$, που είναι άτοπο αφού το $-\sqrt{5}\notin\mathbb{Q}$. Άρα $q=0$ συνεπώς $p=0$, δηλαδή τα $1,\sqrt{5}$ είναι γραμμικά ανεξάρτητα. Επίσης κάθε στοιχείο του $\mathbb{Q}(\sqrt{5})$ γράφεται στη μορφη $p+q\sqrt{5}$ όπου $p,q\in\mathbb{Q}$. Άρα το σύνολο $\{1,\sqrt{5}\}$ παράγει τον $\mathbb{Q}(\sqrt{5})$. Άρα τα $\{1,\sqrt{5}\}$ είναι μια βάση του $\mathbb{Q}(\sqrt{5})$ με σώμα το $\mathbb{Q}$. Με τον ίδιο τρόπο μπορούμε να δείξουμε ότι τα $\{1,\ \sqrt{7}\}$ είναι μια βάση για τον $\mathbb{Q}(\sqrt{5},\ \sqrt{7})$ με σώμα το $\mathbb{Q}(\sqrt{5})$. Κάθε στοιχείο του $\mathbb{Q}(\sqrt{5},\ \sqrt{7})$ μπορεί να γραφεί στη μορφή

$$p+q\sqrt{5}+r\sqrt{7}+s\sqrt{35}$$

όπου τα $p,\ q,\ r,\ s\in\mathbb{Q}$. Μπορούμε να γράψουμε την παραπάνω σχέση ως εξής

$$(p+q\sqrt{5})+(r+s\sqrt{5})\sqrt{7}.$$

Παρατηρούμε ότι τα $\{1,\ \sqrt{7}\}$ παράγουν τον $\mathbb{Q}(\sqrt{5},\ \sqrt{7})$ με σώμα το $\mathbb{Q}(\sqrt{5})$. Μένει να δείξουμε την γραμμική ανεξαρτησία των $\{1,\ \sqrt{7}\}$.Έστω

$$(p+q\sqrt{5})+(r+s\sqrt{5})\sqrt{7}=0$$

τότε

$$p+q\sqrt{5}=0\ \kappa\alpha\iota\ r+s\sqrt{5}=0$$

ή

$$\sqrt{7}=(p+q\sqrt{5})/(r+s\sqrt{5})\ \in\mathbb{Q}(\sqrt{5}).$$

Αν $\sqrt{7}=(p+q\sqrt{5})/(r+s\sqrt{5})$ τότε

$$\sqrt{7}=a+b\sqrt{5}$$

όπου τα $a,b\in\mathbb{Q}$. Αν υψώσουμε στο τετράγωνο την τελευταία σχέση έχουμε

$$7=a^2+5b^2+5\sqrt{5}ab$$

άρα θα πρέπει το $\sqrt{5}ab$ να είναι ρητός που συμβαίνει μόνο όταν $a=b=0$. Επομένως ισχύει $p+q\sqrt{5}=0$ και $r+s\sqrt{5}=0$ και άρα τα $\{1,\ \sqrt{7}\}$ είναι γραμμικά ανεξάρτητα. Τελικά αποδείξαμε ότι τα $\{1,\ \sqrt{7}\}$ είναι μια βάση του $\mathbb{Q}(\sqrt{5},\ \sqrt{7})$ με σώμα το $\mathbb{Q}(\sqrt{5})$. Τελικά καταλήγουμε ότι κάθε στοιχείο του $\mathbb{Q}(\sqrt{5},\ \sqrt{7})$ μπορεί να εκφραστεί μοναδικά στη μορφη

$$p+q\sqrt{5}+r\sqrt{7}+s\sqrt{35}$$

όπου $p,\ q,\ r,\ s \in \mathbb{Q}$.

Έστω

$$p + q\sqrt{5} + r\sqrt{7} + s\sqrt{35} \quad p,\ q,\ r,\ s \in \mathbb{Q}$$

ένα στοιχείο του $\mathbb{Q}(\sqrt{5},\ \sqrt{7})$. Μπορούμε να το γράψουμε στη μορφή:

$$(p + q\sqrt{5}) + (r + s\sqrt{5})\sqrt{7} = 0.$$

Θέτουμε

$$k = p + q\sqrt{5}\ \in \mathbb{Q}(\sqrt{5})\ \ \kappa\alpha\iota\ \ l = r + s\sqrt{5}\ \in \mathbb{Q}(\sqrt{5})$$

Ο αντίστροφος θα είναι ένα στοιχείο $a + \beta\sqrt{7}$ έτσι ώστε να ισχύει

$$(k + l\sqrt{7})(a + \beta\sqrt{7}) = 1$$

Από την παραπάνω εξίσωση παίρνω τις σχέσεις

$$a = \frac{k}{k^2 - 7l^2}\ \ \kappa\alpha\iota\ \ \beta = -\frac{l}{k^2 - 7l^2}$$

Άρα ο αντίστροφος του $p + q\sqrt{5} + r\sqrt{7} + s\sqrt{35}$ είναι ένα στοιχείο της μορφής

$$\frac{k}{k^2 - 7l^2} - \frac{l}{k^2 - 7l^2}\sqrt{7}.$$

Παράδειγμα 3.2.3 *Αν $[L : K] = 1$ δείξτε ότι $K = L$.*

Απάντηση:
Η βάση του L με σώμα το Κ αποτελείται από ένα στοιχείο έστω $a \in L$. Δηλαδή $L = \{xa : x \in K\}$. Θα δείξουμε ότι το $a \in K$. Έστω ότι $a \notin K$. Το $1 \in L$ άρα θα πρέπει να υπάρχει $x \in K$ έτσι ώστε $1 = xa$ ή $a^{-1} = x$. Όμως $x \in K$ και $a^{-1} \notin K$ που είναι άτοπο. Άρα $a \in K$. Έστω $y \in L$. Τότε $y = xa$ $(x \in K,\ a \in K)$ δηλαδή $y \in K$ οπότε $L \subset K$. Όμως $K \subset L$ άρα $K = L$.

Παράδειγμα 3.2.4 *Αν $[L : K]$ είναι πρώτος αριθμός δείξτε ότι τα μόνα σώματα έτσι ώστε να ισχύει $K \subseteq M \subseteq L$ είναι το K και το L.*

Απάντηση:
$[L : K] = [L : M][M : K]$. Επειδη $[L : K]$ είναι πρώτος αριθμός θα πρέπει να ισχύει

$$[L : M] = [L : K],\ [M : K] = 1$$

ή

$$[L : M] = 1,\ [M : K] = [L : K].$$

Βασιζόμενοι στην προηγούμενη άσκηση από την πρώτη περίπτωση έχουμε M=K και από την δεύτερη έχουμε M=L.

Κεφάλαιο 4

Κατασκευές με κανόνα και διαβήτη

4.1 Αλγεβρική διατύπωση

Έστω P_0 ένα γνωστό σύνολο σημείων στον ευκλείδειο χώρο $\mathbb{R}^2$ και θεωρούμε τις παρακάτω πράξεις:
(α) πράξη 1(με κανόνα): Μεταξύ δύο σημείων του P_0 σχεδιάζουμε μια ευθεία γραμμή.
(β) πράξη 2(με διαβήτη): Σχεδιάζουμε ένα κύκλο του οποίου το κέντρο είναι κάποιο σημείο του P_0 και η ακτίνα του είναι ίση με την απόσταση μεταξύ δύο σημείων του P_0.

Ορισμός 4.1.1 *Τα σημεία της τομής οποιονδήποτε διακεκριμένων ευθειών ή κύκλων που έχουν σχεδιαστεί με τις πράξεις 1 και 2 λέμε ότι είναι κατασκευάσιμα σε ένα βήμα από το P_0.*

Ένα σημείο $r \in \mathbb{R}^2$ είναι κατασκευάσιμο από το P_0 αν υπάρχει μία πεπερασμένη σειρά

$$r_1, \ \ldots, \ r_n = r$$

σημείων του $\mathbb{R}^2$ έτσι ώστε για κάθε $i = 1, \ \ldots, \ n$ το σημείο r_i να είναι κατασκευάσιμο σε ένα βήμα από το σύνολο

$$P_0 \cup \{r_1, \ \ldots, \ r_{i-1}\}.$$

Παράδειγμα 4.1.1 *Θα δείξουμε πως η κατασκευή του μέσου μιας δεδομένης ευθείας μπορεί να πραγματοποιηθεί σύμφωνα με όσα ορίσαμε παραπάνω. Έστω ότι μας δίνουν δύο σημεία $p_1, \ p_2 \in \mathbb{R}^2$. Έστω $P_0 = \{p_1, p_2\}$.*

1. *Σχεδιάζουμε την ευθεία* p_1p_2.
2. *Σχεδιάζουμε τον κύκλο με κέντρο* p_1 *και ακτίνα* p_1p_2.
3. *Σχεδιάζουμε τον κύκλο με κέντρο* p_2 *και ακτίνα* p_1p_2.
4. *Έστω* r_1 *και* r_2 *τα σημεία τομής των δύο κύκλων.*
5. *Σχεδιάζουμε την ευθεία* r_1r_2.
6. *Έστω* r_3 *η τομή των ευθειών* p_1p_2 *και* r_1r_2.

Τότε η σειρά των σημείων $r_1,\ r_2,\ r_3$ *ορίζει την κατασκευή του μέσου της ευθείας* p_1p_2.

Εφόσον μια ευθεία ορίζεται από δυο σημεία της και ένας κύκλος ορίζεται από το κέντρο του και ένα σημείο της περιφέρειάς του όλες οι γνωστές γεωμετρικές κατασκευές της ευκλείδειας γεωμετρίας προκύπτουν με τον τρόπο που περιγράψαμε παραπάνω.

Θα δούμε τώρα πως συνδυάζουμε την θεωρία σωμάτων με τα παραπάνω. Με κάθε στάδιο στην κατασκευή αντιστοιχίζουμε το υπόσωμα του $\mathbb{R}$ που παράγεται από τις συντεταγμένες των σημείων που έχουμε κατασκευάσει. Έστω K_0 το υπόσωμα του $\mathbb{R}$ που παράγεται από τις x και y συντεταγμένες των σημείων του P_0. Αν το r_i έχει συντεταγμένες $(x_i,\ y_i)$ τότε ορίζουμε το K_i να είναι το σώμα που δημιουργείται από το K_{i-1} προσθέτωντας τα x_i, y_i, δηλαδή

$$K_i = K_{i-1}(x_i,\ y_i).$$

Παρατηρούμε ότι

$$K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n \subseteq \mathbb{R}.$$

Λήμμα 4.1.1 *Σύμφωνα με τα παραπάνω τα* $x_i,\ y_i$ *είναι ρίζες στο* K_i *δευτεροβάθμιων πολυωνύμων με συντελεστές από το* K_{i-1}.

Απόδειξη: Υπάρχουν τρεις περιπτώσεις: **α)** Μια ευθεία να τέμνει ευθεία, **β)** μια ευθεία να τέμνει κύκλο και **γ)** κύκλος να τέμνει κύκλο.

α) Έστω A, B, C, D σημεία με συντεταγμένες $(p,\ q)$, $(r,\ s)$, $(t,\ u)$, $(v,\ w)$ αντίστοιχα που ανήκουν στον K_{i-1}. Σχεδιάζουμε τις ευθείες AB και CD. Η εξίσωση που περιγράφει την ευθεία AB είναι η εξής:

$$\frac{x-p}{r-p} = \frac{y-q}{s-q} \tag{4.1}$$

και η εξίσωση που περιγράφει την ευθεία CD είναι η εξής:

$$\frac{x-t}{v-t} = \frac{y-u}{w-u}. \tag{4.2}$$

Έστω X, Y τα σημεία τομής των δύο ευθειών. Λύνοντας τις εξισώσεις (4.1) και (4.2) ως προς x έχουμε:

$$x[(s-q)(v-t)-(w-u)(r-p)]-p(s-q)(v-t)+t(w-u)(r-p)+(q-u)(v-t) = 0$$

συνεπώς οι x-συντεταγμένες των X, Y είναι οι ρίζες της παραπάνω εξίσωσης με συντελεστές από τον K_{i-1}. Λύνοντας τις εξισώσεις (4.1) και (4.2) ως προς y έχουμε:

$$y[(r-p)(w-u)-(s-q)(v-t)]+u(s-q)(v-t)-q(r-p)(w-u)+(p-t)(w-u) = 0$$

συνεπώς οι y-συντεταγμένες των X, Y είναι οι ρίζες της παραπάνω εξίσωσης με συντελεστές από τον K_{i-1}.

β) Έστω A, B, C σημεία με συντεταγμένες $(p,\ q)$, $(r,\ s)$, $(t,\ u)$ αντίστοιχα που ανήκουν στον K_{i-1}. Σχεδιάζουμε την ευθεία AB και τον κύκλο με κέντρο C και ακτίνα w, όπου το $w^2 \in K_{i-1}$. Το w^2 ανήκει στον K_{i-1} διότι το w είναι η απόσταση μεταξύ δύο σημείων που ανήκουν στον K_{i-1}. Η εξίσωση που περιγράφει την ευθεία AB είναι η εξής:

$$\frac{x-p}{r-p} = \frac{y-q}{s-q} \tag{4.3}$$

και η εξίσωση που περιγράφει τον κύκλο είναι η εξής:

$$(x-t)^2 + (y-u)^2 = w^2. \tag{4.4}$$

Έστω X, Y τα σημεία τομής του κύκλου με την ευθεία. Λύνοντας τις εξισώσεις (4.3) και (4.4) ως προς x έχουμε:

$$(x-t)^2 + \left(\frac{s-q}{r-p}\ (x-p) + q - u\right)^2 = w^2$$

συνεπώς οι x-συντεταγμένες των X, Y είναι οι ρίζες του παραπάνω δευτεροβάθμιου πολυωνύμου με συντελεστές από τον K_{i-1}. Λύνοντας τις εξισώσεις (4.3) και (4.4) ως προς y έχουμε:

$$\left(\frac{r-p}{s-q}\ (y-q) + p - t\right)^2 + (y-u)^2 = w^2$$

και άρα οι y-συντεταγμένες των X, Y είναι οι ρίζες αυτού του δευτεροβάθμιου πολυωνύμου με συντελεστές από τον K_{i-1}.

γ) Έστω A, B σημεία με συντεταγμένες $(p,\ q)$, $(r,\ s)$, αντίστοιχα που ανήκουν στον K_{i-1}. Σχεδιάζουμε τον κύκλο με κέντρο A και ακτίνα w, όπου το $w^2 \in K_{i-1}$. Το w^2 ανήκει στον K_{i-1} διότι το w είναι η απόσταση μεταξύ δύο σημείων που ανήκουν στον K_{i-1}. Σχεδιάζουμε τον κύκλο με κέντρο B και ακτίνα z, όπου το $z^2 \in K_{i-1}$. Το z^2 ανήκει στον K_{i-1} διότι το z είναι η απόσταση μεταξύ δύο σημείων που ανήκουν στον K_{i-1}. Η εξίσωση που περιγράφει τον κύκλο με κέντρο το A και ακτίνα w είναι η εξής:

$$(x-p)^2 + (y-q)^2 = w^2. \tag{4.5}$$

και εξίσωση που περιγράφει τον κύκλο με κέντρο το B και ακτίνα z είναι η εξής:

$$(x-r)^2 + (y-s)^2 = z^2. \tag{4.6}$$

Έστω X, Y τα σημεία τομής των δύο κύκλων.Λύνοντας τις εξισώσεις (4.5) και (4.6) ως προς x έχουμε:

Για $y = \sqrt{w^2-(x-p)^2} + q$

$$\begin{aligned}
&4 \quad \Big((q-s)^2+(r-p)^2\Big)x^2 + \\
&+ \quad \Big(4\Big(p^2-r^2\Big)\Big(r-p\Big)+4\Big(z^2-w^2-(q-s)^2\Big)\Big(r-p\Big)-8q\Big(q-s\Big)^2\Big)x \\
&+ \quad (p^2-r^2)^2+\Big(z^2-w^2-(q-s)^2\Big)^2+2\Big(z^2-w^2-(q-s)^2\Big)(p^2-r^2) \\
&+ \quad 4(q-s)^2(p^2-w^2)= 0
\end{aligned}$$

και για $y = -\sqrt{w^2+(x-p)^2} + q$

$$\begin{aligned}
&4 \quad \Big((q-s)^2+(p-r)^2\Big)x^2 + \\
&+ \quad \Big(4\Big(r^2-p^2\Big)\Big(p-r\Big)+4\Big(z^2-w^2-(q-s)^2\Big)\Big(p-r\Big)-8p\Big(q-s\Big)^2\Big)x \\
&+ \quad (r^2-p^2)^2+\Big(z^2-w^2-(q-s)^2\Big)^2+2\Big(z^2-w^2-(p-r)^2\Big)(r^2-p^2) \\
&+ \quad 4(q-s)^2(p^2-w^2)= 0
\end{aligned}$$

συνεπώς οι x-συντεταγμένες των X, Y είναι οι ρίζες ενός δευτεροβάθμιου πολυωνύμου με συντελεστές από τον K_{i-1}. Διακρίνοντας περιπτώσεις θα βρούμε

δύο τιμές για το x σε περίπτωση που οι κύκλοι τέμνονται ενώ αν εφάπτονται θα βρούμε μία τιμή για το x.

Λύνοντας τις εξισώσεις (4.5) και (4.6) ως προς y έχουμε:
Για $x = \sqrt{w^2 + (y-q)^2} + p$

$$\begin{aligned} 4 \quad & \Big((s-q)^2+(p-r)^2\Big)y^2 + \\ + \quad & \Big(4\Big(q^2-s^2\Big)\Big(s-q\Big)+4\Big(z^2-w^2-(p-r)^2\Big)\Big(s-q\Big)-8q\Big(p-r\Big)^2\Big)y \\ + \quad & q^2-s^2+\Big(z^2-w^2-(p-r)^2\Big)^2+2\Big(z^2-w^2-(p-r)^2\Big)(q^2-s^2) \\ + \quad & 4(p-r)^2(q^2-w^2)=0 \end{aligned}$$

και για $x = -\sqrt{w^2 + (y-q)^2} + p$

$$\begin{aligned} 4 \quad & \Big((q-s)^2+(p-r)^2\Big)y^2 + \\ + \quad & \Big(4\Big(s^2-q^2\Big)\Big(q-s\Big)+4\Big((p-r)^2+w^2-z^2\Big)\Big(q-s\Big)-8q\Big(p-r\Big)^2\Big)y \\ + \quad & s^2-q^2+\Big((p-r)^2+w^2-z^2\Big)^2+2\Big((p-r)^2+w^2-z^2\Big)(s^2-q^2) \\ + \quad & 4(p-r)^2(q^2-w^2)=0 \end{aligned}$$

συνεπώς οι y-συντεταγμένες των X, Y είναι οι ρίζες ενός δευτεροβάθμιου πολυωνύμου με συντελεστές από τον K_{i-1}. Διακρίνοντας περιπτώσεις θα βρούμε δύο τιμές για το y σε περίπτωση που οι κύκλοι τέμνονται ενώ αν εφάπτονται θα βρούμε μία τιμή για το y.□

Θεώρημα 4.1.1 *Αν το $r = (x,\ y)$ είναι κατασκευάσιμο από ένα υποσύνολο P_0 του $\mathbb{R}^2$ και αν K_0 είναι το υπόσωμα του $\mathbb{R}$ που παράγεται από τις συντεταγμένες των σημείων του P_0, τότε οι βαθμοί*

$$[K_0(x) : K_0] \quad \text{και} \quad [K_0(y) : K_0]$$

είναι δυνάμεις του 2.

Απόδειξη:
$[K_{i-1}(x_i) : K_{i-1}] = 1$ ή 2
διότι το x_i είναι ρίζα ενός πολυωνύμου δευτέρου βαθμού με συντελεστές από το K_{i-1}. Η τιμή 2 είναι για την περίπτωση κατα την οποία το πολυώνυμο είναι

είναι ανάγωγο, διαφορετικά είναι 1. Με τον ίδιο τρόπο παίρνουμε την σχέση: $[K_{i-1}(y_i) : K_{i-1}] = 1$ ή 2.
Επίσης έχουμε:
$[K_{i-1}(x_i,\ y_i) : K_{i-1}] = [K_{i-1}(x_i,\ y_i) : K_{i-1}(x_i)][K_{i-1}(x_i) : K_{i-1}] = 1,\ 2$ ή 4. Εφόσον ο βαθμός $[K_i : K_{i-1}]$ είναι δύναμη του 2 επαγωγικά παρατηρούμε ότι ο βαθμος $[K_n : K_0]$ είναι δύναμη του 2. Εφόσον ισχύει

$$[K_n : K_0(x)][K_0(x) : K_0] = [K_n : K_0]$$

προκύπτει ότι ο βαθμός $[K_0(x) : K_0]$ είναι δύναμη του 2. Με όμοιο τρόπο καταλήγουμε ότι ο βαθμός $[K_0(y) : K_0]$ είναι δύναμη του 2.□

4.2 Αδύνατες αποδείξεις

Θα χρησιμοποιήσουμε την παραπάνω θεωρία για να αποδείξουμε ότι δεν υπάρχει κατασκευή με κανόνα και διαβήτη για τα τρία παρακάτω προβλήματα.

Θεώρημα 4.2.1 *Ο κύβος δεν μπορεί να διπλασιαστεί χρησιμοποιώντας κανόνα και διαβήτη.*

Απόδειξη: Έστω ότι μας δίνεται ένας κύβος έτσι ώστε η μία πλευρά του να είναι το μοναδιαίο τμήμα του x-άξονα. Επομένως το $P_0 = \{(0,0),\ (1,0)\}$ και άρα $K_0 = \mathbb{Q}$. Για να διπλασιάσουμε τον κύβο θα πρέπει να κατασκευάσουμε το σημείο (α,0) όπου $a^3 = 2$. Συνεπώς από το θεώρημα 4.1.1 έχουμε ότι ο βαθμός $[\mathbb{Q}(a) : \mathbb{Q}]$ θα πρέπει να είναι μια δύναμη του 2. Όμως το a είναι μια ρίζα του πολυωνύμου $t^3 - 2$ στο $\mathbb{Q}$ το οποίο σύμφωνα με το κριτήριο του *Eisenstein* και για $p = 2$ είναι ανάγωγο στο $\mathbb{Q}$. Άρα από την πρόταση 3.1.1 ισχύει $[\mathbb{Q}(a) : \mathbb{Q}] = 3$ που δεν είναι δύναμη του 2. Άρα ο κύβος δεν μπορεί να διπλασιαστεί με κανόνα και διαβήτη.□

Θεώρημα 4.2.2 *Η γωνία $\pi/3$ δεν μπορεί να τριχοτομηθεί χρησιμοποιώντας κανόνα και διαβήτη.*

Απόδειξη: Έστω ότι μας δίνονται τα σημεία (0,0) και (1,0) στον τριγωνομετρικό κύκλο. Δηλαδή $P_0 = \{(0,0),(1,0)\}$ οπότε $K_0 = \mathbb{Q}$. Για να κατασκευάσουμε μια γωνία που να τριχοτομεί την γωνία $\pi/3$ θα πρέπει να κατασκευάσουμε το σημείο (α,0) όπου $a = \cos(\pi/9)$. Από αυτό θα μπορούσε να κατασκευαστεί το $\beta = 2\cos(\pi/9)$. Από την τριγωνομετρία γνωρίζουμε ότι

$$(\cos\theta + i\sin\theta)^3 = \cos 3\theta + i\sin 3\theta.$$

$$(\cos\theta + i\sin\theta)^3 = \cos^3\theta - 3\cos\theta\sin^2\theta + i(\cos^2\theta\sin\theta - \sin^3\theta).$$

Επομένως θα πρέπει να ισχύει

$$\cos 3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta$$

δηλαδή θα πρέπει να ισχύει

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

Για $\theta = \pi/9$ έχουμε

$$\cos\frac{\pi}{3} = 4\cos^3\frac{\pi}{9} - 3\cos\frac{\pi}{9}.$$

Επειδή $\cos\pi/3 = 1/2$ έχουμε τη σχέση

$$\frac{1}{2} = 4\cos^3\frac{\pi}{9} - 3\cos\frac{\pi}{9}$$

ή

$$1 = 8\cos^3\frac{\pi}{9} - 6\cos\frac{\pi}{9}$$

ή

$$\beta^3 - 3\beta - 1 = 0.$$

Έστω $f(\beta) = \beta^3 - 3\beta - 1 = 0$. Τότε,

$$f(\beta+1) = 8\beta^3 + 3\beta^2 - 3.$$

Το $f(\beta+1)$ από το κριτήριο του *Eisenstein* και για $p = 3$ είναι ανάγωγο στο $\mathbb{Q}$ επομένως και το $f(\beta)$ είναι ανάγωγο στο $\mathbb{Q}$ άρα $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$ που δεν είναι δύναμη του 2, άρα το σημείο β δεν είναι κατασκευάσιμο με κανόνα και διαβήτη.□

Θεώρημα 4.2.3 *Ο κύκλος δεν μπορεί να τετραγωνισθεί χρησιμοποιώντας κανόνα και διαβήτη.*

Απόδειξη: Έστω ότι έχουμε ένα κύκλο με κέντρο (0,0) και ακτίνα την ευθεία p_1p_2 όπου $p_1 = (0,0)$ και $p_2 = (1,0)$. Δήλαδή $P_0 = \{(0,0),(1,0)\}$ οπότε $K_0 = \mathbb{Q}$. Για να τετραγωνίσουμε τον κύκλο θα πρέπει να κατασκευάσουμε ένα τετράγωνο με πλευρά ίση με $\sqrt{\pi}$, δηλαδή θα πρέπει να κατασκευάσουμε το σημείο $(0,\sqrt{\pi})$. Ισοδύναμα θα πρέπει να κατασκευάσουμε το σημείο $(0,\pi)$. Αν μια τέτοια κατασκευή γίνεται θα πρέπει ο βαθμός $[\mathbb{Q}(\pi) : \mathbb{Q}]$ να είναι μια δύναμη του 2. Για να συμβαίνει αυτό θα πρέπει επίσης το π να είναι αλγεβρικό στο $\mathbb{Q}$. Όμως γνωρίζουμε από το θεώρημα του *Lindemann* ότι το π δέν είναι αλγεβρικό στο $\mathbb{Q}$. Συνεπώς η κατασκευή δεν είναι δυνατή.□

Κεφάλαιο 5

Η ιδέα της θεωρίας του Galois

5.1 Εισαγωγή

Ορισμός 5.1.1 *Έστω K ένα υπόσωμα του σώματος L. Ένας αυτομορφισμός a του L είναι ένας K-αυτομορφισμός του L αν*

$$a(k) = k \quad \forall k \in K.$$

Θεώρημα 5.1.1 *Αν $L : K$ είναι μια επέκταση τότε το σύνολο όλων των K-αυτομορφισμών του L αποτελεί μια ομάδα με πράξη την σύνθεση συναρτήσεων.*

Απόδειξη: Έστω ότι a και β είναι K-αυτομορφισμοί του L. Τότε αν $k \in K$

$$a(\beta(k)) = a(k) = k$$

άρα ο $a\beta$ είναι ένας K-αυτομορφισμός. Επίσης η ταυτοτική συνάρτηση $a(k) = k$ $\forall k \in K$ είναι ένας K-αυτομορφισμός. Τέλος $\forall k \in K$ έχουμε

$$k = a^{-1}(a(k)) = a^{-1}(k)$$

άρα και ο a^{-1} είναι ένας K-αυτομορφισμός. Άρα το σύνολο όλων των K-αυτομορφισμών του L αποτελεί μια ομάδα.□

Ορισμός 5.1.2 *Η ομάδα Galois $\Gamma(L : K)$ της επέκτασης $L : K$ είναι η ομάδα όλων των K-αυτομορφισμών του L με πράξη την σύνθεση συναρτήσεων.*

Παράδειγμα 5.1.1 *Έστω η επέκταση $\mathbb{C} : \mathbb{R}$. Υποθέτουμε ότι ο a είναι ένας $\mathbb{R}$-αυτομορφισμός του $\mathbb{C}$. Έστω $j = a(i)$ όπου $i = \sqrt{-1}$. Τότε*

$$j^2 = (a(i))^2 = a(i^2) = a(-1) = -1.$$

Τότε θα έχουμε $j = i$ *ή* $j = -i$. *Για καθε* $x,\ y \in \mathbb{R}$ *έχουμε*

$$a(x + iy) = a(x) + a(i)a(y) = x + jy.$$

Επομένως έχουμε δύο επιλογές για τους $\mathbb{R}$*-αυτομορφισμούς:*

$$\begin{aligned} a_1 &: x + iy \to x + iy \\ a_2 &: x + iy \to x - iy. \end{aligned}$$

Ο a_1 *είναι η ταυτοτική απεικόνιση και άρα είναι ένας* $\mathbb{R}$*-αυτομορφισμός του* $\mathbb{C}$. *Θα δείξουμε στην συνέχεια ότι και ο* a_2 *είναι ένας* $\mathbb{R}$*-αυτομορφισμός του* $\mathbb{C}$.

$$\begin{aligned} a_2((x + iy) + (u + iv)) &= (x + u) - (y + v)i \\ &= a_2(x + iy) + a_2(u + iv). \\ a_2((x + iy)(u + iv)) &= a_2(xu - yv - i(xv + yu)) \\ &= xu - yv - i(xv + yu) \\ &= (x - iy)(u - iv) \\ &= a_2(x + iy)a_2(u + iv). \end{aligned}$$

Επομένως ο a_2 *είναι ένας ομομορφισμός. Έστω* $x \in \mathbb{R}$. *Τότε*

$$a_2(x + 0i) = x - 0i = x$$

άρα ο a_2 *είναι ένας* $\mathbb{R}$*-αυτομορφισμός. Παρατηρούμε ότι*

$$a_2^2 = a_2(a_2(x + iy)) = a_2(x - iy) = x + iy$$

δηλαδή $a_2^2 = a_1$. *Άρα η ομάδα Galois είναι μια κυκλική ομάδα τάξης 2.*

Παράδειγμα 5.1.2 *Έστω* c *η τρίτη ρίζα του 2 και έστω η επέκταση* $\mathbb{Q}(c) : \mathbb{Q}$. *Έστω* a *ένας* $\mathbb{Q}$*-αυτομορφισμός του* $\mathbb{Q}(c)$. *τότε*

$$(a(c))^3 = a(c^3) = a(2) = 2.$$

Δηλαδή

$$a(c) = \sqrt[3]{2} = c.$$

Επομένως ο a *είναι η ταυτοτική απεικόνιση και επομένως η ομάδα Galois* $\Gamma(\mathbb{Q}(c) : \mathbb{Q})$ *έχει τάξη 1.*

Ο *Galois* ανακάλυψε ότι κάτω από κατάλληλες προϋποθέσεις υπάρχει μια 1-1 αντιστοιχία μεταξύ:

1. των υποομάδων της ομάδας *Galois* μιας επέκτασης $L : K$

2. των υποσωμάτων Μ του L τέτοια ώστε $K \subseteq M$.

Αν $L : K$ είναι μια επέκταση θα λέμε ένα σώμα Μ ενδιάμεσο σώμα αν ισχύει $K \subseteq M \subseteq L$. Για κάθε ενδιάμεσο σώμα Μ υπάρχει η ομάδα $M^* = \Gamma(L : M)$ όλων των Μ-αυτομορφισμών του L. $K^* = \Gamma(L : K)$ είναι ολόκληρη η ομάδα *Galois* της επέκτασης $L : K$ και $L^* = \Gamma(L : L) = 1$. Αν $M \subseteq N$ τότε $M^* \supseteq N^*$ γιατί αν $a \in N^*$ τότε $a(x) = x \ \forall x \in M$ άρα και $\forall x \in N$ αφού $M \subseteq N$, άρα $a \in M^*$, δηλαδή $N^* \subseteq M^*$.

Για κάθε υποομάδα Η της ομάδας $\Gamma(L : K)$ υπάρχει το σύνολο $H^\dagger$ όλων των στοιχείων $x \in L$ έτσι ώστε $a(x) = x \ \ \forall a \in H$. Αυτό είναι ένα ενδιάμεσο σώμα και θα το εξηγήσουμε στη συνέχεια.

Λήμμα 5.1.1 *Αν H είναι μια υποομάδα της ομάδας $\Gamma(L : K)$ τότε το σύνολο $H^\dagger$ είναι ένα υπόσωμα του L που περιέχει το K.*

Απόδειξη: Έστω $x, y \in H^\dagger$ και $a \in H$. Τότε

$$a(x + y) = a(x) + a(y) = x + y$$

δηλαδή $x + y \in H^\dagger$.

$$a(xy) = a(x)a(y) = xy$$

δηλαδή $xy \in H^\dagger$. Άρα το $H^\dagger$ είναι κλειστό κάτω από τις πράξεις και επομένως είναι υπόσωμα του L. Επιπλέον $\forall a \in \Gamma(L : K)$ έχουμε $a(k) = k \ \ \forall k \in K$ άρα $K \subseteq H^\dagger$ □

Ορισμός 5.1.3 *Σύμφωνα με τα παραπάνω το $H^\dagger$ είναι το σώμα που καθορίζεται από το H.*

Αν $H \subseteq G$ τότε $H^\dagger \supseteq G^\dagger$ διότι αν $x \in G^\dagger$ τότε $a(x) = x \ \ \forall a \in G$ και για κάθε $a \in H$ αφού $H \subseteq G$. Συνεπώς $x \in H^\dagger$ δηλαδή $H^\dagger \supseteq G^\dagger$.

Έστω η επέκταση $L : K$. Αν το Μ είναι ένα ενδιάμεσο σώμα και η Η είναι μια υποομάδα της ομάδας *Galois*, $\Gamma(L : K)$ τότε ισχύει:

$$M \subseteq M^{*\dagger} \tag{5.1}$$

$$H \subseteq H^{\dagger *} \tag{5.2}$$

Έστω $x \in M$. Τότε $a(x) = x$, $\forall a \in M^*$ αφού $M^* = \Gamma(L : M)$ είναι όλοι οι Μ-αυτομορφισμοί του L. Όμως $x \in L$ αφού $M \subseteq L$ και $a(x) = x \ \ \forall a \in M^*$

άρα $x \in M^{*\dagger}$. Άρα $M \subseteq M^{*\dagger}$.
$H^\dagger = \{x \in L : a(x) = x \ \forall a \in H\}$. Δηλαδή αποτελείται από τα στοιχεία του L που όλοι οι αυτομορφισμοί του Η τα στέλνουν στον εαυτό τους.
$H^{\dagger *} = \Gamma(L : H^\dagger)$. Δηλαδή αποτελείται από τους $H^\dagger$-αυτομορφισμούς του L. Όμως ένας $H^\dagger$-αυτομορφισμός είναι και ένας Η-αυτομορφισμός. Συνεπώς $H \subseteq H^{\dagger *}$.
Το παράδειγμα 5.1.2 μας δείχνει ότι οι σχέσεις (5.1), (5.2) δεν είναι πάντα ισότητες. Στο συγκεκριμένο παράδειγμα ισχύει

$$\mathbb{Q}^{*\dagger} = \mathbb{Q}(c).$$

$\mathbb{Q}^* = \Gamma(\mathbb{Q}(c) : \mathbb{Q})$. Επειδή όπως δείξαμε το $c \to c$ υπάρχει ένας μοναδικός $\mathbb{Q}$-αυτομορφισμός, ο ταυτοτικός έστω a. $\mathbb{Q}^{*\dagger} = \{x \in \mathbb{Q}(c) : a(x) = x, \ a \in \mathbb{Q}^*\}$ και επειδή ο a είναι ο ταυτοτικός έχουμε ότι $\forall x \in \mathbb{Q}(c)$ ισχύει $a(x) = x$. Συνεπώς $\mathbb{Q}^{*\dagger} = \mathbb{Q}(c)$.
Αν συμβολίσουμε με $\mathcal{F}$ το σύνολο των ενδιάμεσων σωμάτων και με $\mathcal{G}$ το σύνολο όλων των υποομάδων της ομάδας $Galois$, τότε έχουμε δύο συναρτήσεις

$$\begin{aligned} {}^* : \mathcal{F} &\to \mathcal{G} \\ {}^\dagger : \mathcal{G} &\to \mathcal{F} \end{aligned}$$

οι οποίες ικανοποιούν τις σχέσεις (5.1) και (5.2).

Παράδειγμα 5.1.3 *Έστω ότι έχουμε το πολυώνυμο*

$$f(t) = t^4 - 4t^2 - 5 = 0$$

το οποίο παραγοντοποιείται ως εξής:

$$(t^2 + 1)(t^2 - 5) = 0$$

και οι ρίζες του είναι $a = i, \ \beta = -i, \ \gamma = \sqrt{5}, \ \delta = -\sqrt{5}$. *Η επέκταση που αντιστοιχεί στο παραπάνω πολυώνυμο είναι η* $L : \mathbb{Q}$ *όπου* $L = \mathbb{Q}(i, \sqrt{5})$. *Θα βρούμε στη συνέχεια τους* $\mathbb{Q}$*-αυτομορφισμούς του* L. *Έστω ο* a *είναι ένας* $\mathbb{Q}$*-αυτομορφισμός του* L. *Έστω* $j = a(i)$ *όπου* $i = \sqrt{-1}$. *Τότε*

$$j^2 = (a(i))^2 = a(i^2) = a(-1) = -1.$$

Τότε θα έχουμε $j = i$ *ή* $j = -i$. *Έστω ότι ο* β *είναι ένας* $\mathbb{Q}$*-αυτομορφισμός του* L. *Έστω* $k = \beta(\sqrt{5})$. *Τότε*

$$k^2 = (\beta(\sqrt{5}))^2 = \beta(\sqrt{5}^2) = \beta(5) = 5.$$

Τότε θα έχουμε $k = \sqrt{5}$ *ή* $k = -\sqrt{5}$. *Τελικά θα έχουμε τέσσερις* $\mathbb{Q}$-*αυτομορφισμούς του* L, *τους εξής:*

$$\begin{aligned} a_1 &: p+qi+r\sqrt{5}+si\sqrt{5} \to p+qi+r\sqrt{5}+si\sqrt{5} \\ a_2 &: p+qi+r\sqrt{5}+si\sqrt{5} \to p-qi+r\sqrt{5}+si\sqrt{5} \\ a_3 &: p+qi+r\sqrt{5}+si\sqrt{5} \to p+qi-r\sqrt{5}+si\sqrt{5} \\ a_4 &: p+qi+r\sqrt{5}+si\sqrt{5} \to p-qi-r\sqrt{5}+si\sqrt{5} \end{aligned}$$

Επομένως η ομάδα Galois είναι

$$G = \{a_1, a_2, a_3, a_4\}.$$

Οι υποομάδες της G *είναι:*

$$1,\ \{a_1, a_2\},\ \{a_1, a_3\},\ \{a_1, a_4\}$$

όπου $1 = \{a_1\}$. *Τα αντίστοιχα σώματα που καθορίζονται από αυτές είναι:*

$$L,\ \mathbb{Q}(\sqrt{5}),\ \mathbb{Q}(i),\ \mathbb{Q}(i\sqrt{5}).$$

Τα παραπάνω σώματα μαζί με το K *είναι τα μόνα υποσώματα του* L, *επομένως σε αυτή την περίπτωση η αντιστοιχία Galois είναι ένα προς ένα.*

Παράδειγμα 5.1.4 *Βρείτε τους* K-*αυτομορφισμούς του* L *των παρακάτω επεκτάσεων* $L : K$
(*a*) $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$
(*b*) $\mathbb{Q}(a) : \mathbb{Q}$ *όπου* $a = \sqrt[5]{7}$
(*c*) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$.

Απάντηση:
(*a*) $I : \sqrt{2} \to \sqrt{2}$ και $R : \sqrt{2} \to -\sqrt{2}$
(*b*) Έστω γ ένας $\mathbb{Q}$-αυτομορφισμός του $\mathbb{Q}(a)$. Έστω $j = \gamma(a)$ όπου $a = \sqrt[5]{7}$. Τότε $j^5 = (\gamma(a))^5 = \gamma(a^5) = \gamma(a) = a$. Άρα υπάρχει ένας $\mathbb{Q}$-αυτομορφισμός, ο ταυτοτικός $I : a \to a$.
(*c*) $I : \sqrt{2} \to \sqrt{2}$, $R : \sqrt{2} \to -\sqrt{2}$, $S : \sqrt{3} \to -\sqrt{3}$ και $T : \sqrt{2} \to -\sqrt{2}$ και $\sqrt{3} \to -\sqrt{3}$.

Παράδειγμα 5.1.5 *Βρείτε τις αντίστοιχες ομάδες Galois για τις παραπάνω επεκτάσεις.*

Απάντηση:
(*a*) $G = \{I, R\}$
(*b*) $G = \{I\}$
(*c*) $G = \{I, R, S, T\}$

Παράδειγμα 5.1.6 *Σε ποιές από τις παραπάνω περιπτώσεις η αντιστοιχία του Galois μεταξύ $\mathcal{F}$ και $\mathcal{G}$ είναι ένα προς ένα;*

Απάντηση:
(a) $\mathcal{F} = \{\mathbb{Q},\ \mathbb{Q}(\sqrt{2})\}$ και $\mathcal{G} = \{I,\ \{I, R\}\}$ επομένως η αντιστοιχία *Galois* είναι ένα προς ένα.
(b) $\mathcal{F} = \{\mathbb{Q},\ \mathbb{Q}(a),\ \mathbb{Q}(a^2)\}$ και $\mathcal{G} = \{I\}$ επομένως η αντιστοιχία *Galois* δεν είναι ένα προς ένα.
(c) $\mathcal{F} = \{\mathbb{Q},\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{3}),\ \mathbb{Q}(\sqrt{2}\sqrt{3}),\ \mathbb{Q}(\sqrt{2}, \sqrt{3})\}$
και $\mathcal{G} = \{I,\ \{I, R\},\ \{I, S\},\ \{I, T\},\ \{I, R, S, T\}\}$ επομένως η αντιστοιχία *Galois* είναι ένα προς ένα.

Παράδειγμα 5.1.7 *Έστω K το σώμα που είδαμε στο ερώτημα (h) του παραδείγματος 1.4.3 και έστω P το πρώτο του υπόσωμα. Ποια είναι η ομάδα Galois της επέκτασης $K : P$; Είναι η αντιστοιχία Galois ένα προς ένα;*

Απάντηση: Το πρώτο υπόσωμα του σώματος Κ είναι το $P = \{1, 0\}$ και η επέκταση γράφεται $P(\alpha, \beta) : P$. Έχουμε δύο P-αυτομορφισμούς:

$$\begin{aligned} a_1 &: \alpha \to \alpha,\ \beta \to \beta \\ a_2 &: \alpha \to \beta \\ &\quad\ \beta \to \alpha \end{aligned}$$

Άρα $G = \{a_1, a_2\}$. $\mathcal{F} = \{P, K\}$ και $\mathcal{G} = \{a_1,\ \{a_1, a_2\}\}$ επομένως η αντιστοιχία *Galois* είναι ένα προς ένα.

Παράδειγμα 5.1.8 *Έστω $K(a)$:K μια απλή αλγεβρική επέκταση και έστω γ είναι ένα στοιχείο της ομάδας Galois. Δείξτε ότι το $\gamma(a)$ έχει το ίδιο ελάχιστο πολυώνυμο με το a στο K.*

Απάντηση: Έστω ότι το $b_0 + b_1 t + \ldots + b_n t^n$ είναι το ελάχιστο πολυώνυμο του a, $(b_0, b_1, \ldots, b_n) \in K$. Δηλαδή ισχύει

$$b_0 + b_1 a + \ldots + b_n a^n = 0.$$

$$\gamma(b_0 + b_1 a + \ldots + b_n a^n) = \gamma(0)$$

δηλαδη

$$b_0 + b_1 \gamma(a) + \ldots + b_n \gamma(a^n) = 0$$

γιατί ο γ είναι Κ-αυτομορφισμός και επομένως $\gamma(b) = b \ \forall b \in K$. Τελικά έχουμε

$$b_o + b_1\gamma(a) + \ldots + b_n(\gamma(a))^n = 0.$$

Αν υπάρχει ένα πολυώνυμο $c_0 + c_1t + \ldots + c_mt^m$, $(c_o, c_1, \ldots, c_n \in K)$ με $m < n$ έτσι ώστε

$$c_0 + c_1\gamma(a) + \ldots + c_m\gamma(a)^n = 0$$

τότε

$$\gamma^{-1}(c_0 + c_1\gamma(a) + \ldots + c_m\gamma(a)^n) = \gamma^{-1}(0)$$

οπότε

$$c_0 + c_1a + \ldots + c_ma^m = 0$$

διότι ο γ^{-1} είναι και αυτός ένας Κ-αυτομορφισμός του $K(a)$. Όμως αυτό είναι άτοπο αφού υποθέσαμε ότι το $b_0+b_1t+\ldots+b_nt^n$ είναι το ελάχιστο πολυώνυμο του a στο Κ. Άρα το $b_0 + b_1t + \ldots + b_nt^n$ είναι το ελάχιστο πολυώνυμο και του $\gamma(a)$ στο Κ. Άρα το a έχει το ίδιο ελάχιστο πολυώνυμο με το $\gamma(a)$ στο Κ.

Παράδειγμα 5.1.9 *Βρείτε όλα τα ενδιάμεσα σώματα της επέκτασης* $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}$. *Βρείτε την ομάδα Galois. Συγκρίνετε.*

Απάντηση: Τα ενδιάμεσα σώματα είναι τα εξής:

- $\mathbb{Q}$
- $\mathbb{Q}(\sqrt{3}, \sqrt{5})$
- $\mathbb{Q}(\sqrt{2}, \sqrt{5})$
- $\mathbb{Q}(\sqrt{2}, \sqrt{3})$
- $\mathbb{Q}(\sqrt{5})$
- $\mathbb{Q}(\sqrt{3})$
- $\mathbb{Q}(\sqrt{2})$
- $\mathbb{Q}(\sqrt{2}\sqrt{3})$
- $\mathbb{Q}(\sqrt{2}\sqrt{5})$
- $\mathbb{Q}(\sqrt{3}\sqrt{5})$
- $\mathbb{Q}(\sqrt{2}\sqrt{3}\sqrt{5})$

Οι $\mathbb{Q}$-αυτομορφισμοί του $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ είναι οι εξής:

- $a_1 : \sqrt{2} \to \sqrt{2}$
- $a_2 : \sqrt{2} \to -\sqrt{2}$
- $a_3 : \sqrt{3} \to -\sqrt{3}$
- $a_4 : \sqrt{5} \to -\sqrt{5}$
- $a_5 : \sqrt{2} \to -\sqrt{2},\ \sqrt{3} \to -\sqrt{3}$
- $a_6 : \sqrt{2} \to -\sqrt{2},\ \sqrt{5} \to -\sqrt{5}$
- $a_7 : \sqrt{3} \to -\sqrt{3},\ \sqrt{5} \to -\sqrt{5}$
- $a_8 : \sqrt{2} \to -\sqrt{2},\ \sqrt{3} \to -\sqrt{3},\ \sqrt{5} \to -\sqrt{5}$

$$\mathcal{G} = \{\ a_1,\ \{a_1,a_2\},\ \{a_1,a_3\},\ \{a_1,a_4\},\ \{a_1,a_5\},\ \{a_1,a_6\},\ \{a_1,a_7\},\ \{a_1,a_8\},\ \{a_1,a_2,a_7,a_8\},\ \{a_1,a_3,a_6,a_8\},\ \{a_1,a_4,a_5,a_8\}\ \}$$

Επομένως η αντιστοιχία *Galois* είναι ένα προς ένα.

Παράδειγμα 5.1.10 *Βρείτε ποιες από τις παρακάτω προτάσεις είναι σωστές ή λανθασμένες.*
(a) Κάθε K-αυτομορφισμός του L είναι ένας αυτομορφισμός του L.
(b) Κάθε L-αυτομορφισμός του L είναι η ταυτοτική απεικόνιση.
(c) Η ομάδα Galois της επέκτασης $L : K$ είναι μια κυκλική ομάδα.
(d) Η ομάδα Galois της επέκτασης $\mathbb{C} : \mathbb{R}$ είναι αβελιανή.
(e) Οι συναρτήσεις * και † είναι πάντα μεταξύ τους αντίστροφες.
(f) Οι συναρτήσεις * και † διατηρούν τον ισομορφισμό.
(g) Αν $\Gamma(L : K) = 1$ τότε $L = K$.
(h) Αν $L = K$ τότε $\Gamma(L : K) = 1$.
(i) Ο $K(t)$ έχει μόνο έναν K-αυτομορφισμό.
(j) Η ομάδα Galois είναι ευκολότερο να οριστεί παρά να υπολογιστεί.

Απάντηση:
(a) Σωστο. $\forall x \in K$ ισχύει $a(x) = x$ και επειδή $K \subseteq L$, $x \in L$ και άρα ο a είναι ένας αυτομορφισμός του L.
(b) Σωστο. $\forall x \in L$ ισχύει $a(x) = x$ και άρα ο L-αυτομορφισμός είναι η

ταυτοτική απεικόνιση.
(c) Λάθος. Η ομάδα *Galois* που είδαμε στο παράδειγμα 5.1.3 δεν είναι κυκλική αφού όλες οι υποομάδες της είναι τάξης 2 και καμία δεν παράγει ολόκληρη την ομάδα.
(d) Σωστό. Στο παράδειγμα 5.1.1 έχουμε $a_2(a_1(x+iy)) = x - iy$ και $a_1(a_2(x+iy)) = x - iy$, $\forall x, y \in \mathbb{R}$.
(e) Λάθος.
(f) Λάθος. Δείξαμε ότι αν $M \subseteq N$ τότε $M^* \supseteq N^*$ και αν $H \subseteq G$ τότε $H^\dagger \supseteq G^\dagger$.
(g) Λάθος. Δείξαμε παραπάνω ότι $\Gamma(\mathbb{Q}(c) : \mathbb{Q}) = 1$ όταν $c = \sqrt[3]{2}$, αλλά $\mathbb{Q}(c) \neq \mathbb{Q}$.
(h) Σωστό. Αν $K = L$ υπάρχει μόνο ένας K-αυτομορφισμός του L και είναι ο ταυτοτικός.
(i) Λάθος. Υπάρχει σίγουρα ο ταυτοτικός K-αυτομορφισμός όπου όλα τα στοιχεία του $K(t)$ πηγαίνουν στον εαυτό τους μπορούν όμως να υπάρχουν και περιπτώσεις όπου το t για παράδειγμα να πηγαίνει στο t^2 ή το το t να πηγαίνει στο t^3 ενώ όλα τα στοιχεία του K πηγαίνουν στον εαυτό τους.
(j) Σωστό.

Κεφάλαιο 6

Κανονικότητα και διαχωρισιμότητα

6.1 Διασπόμενα σώματα

Ορισμός 6.1.1 *Αν K είναι ένα σώμα και f είναι ένα πολυώνυμο με συντελεστές από το K, τότε το f διασπάται στο K αν μπορεί να γραφεί ως γινόμενο γραμμικών παραγόντων*

$$f(t) = k(t - a_1) \dots (t - a_n)$$

όπου $k, a_1, \dots, a_n \in K$. Σε αυτήν την περίπτωση οι ρίζες του f στο K είναι οι $a_1, \dots, a_n$.

Παράδειγμα 6.1.1 *Το πολυώνυμο $t^3 - 1 \in \mathbb{Q}[t]$ δεν διασπάται στο $\mathbb{Q}$ αλλά διασπάται στο $\mathbb{C}$ αφού γράφεται στη μορφή*

$$(t - 1)(t - \omega)(t - \omega^2)$$

όπου $\omega = \exp(2\pi i/3)$.

Παράδειγμα 6.1.2 *Το πολυώνυμο $t^4 - 4t^2 - 5$ διασπάται στο $\mathbb{Q}(i, \sqrt{5})$ αφού γράφεται στη μορφή*

$$(t - i)(t + i)(t - \sqrt{5})(t + \sqrt{5}).$$

Όμως στο $\mathbb{Q}(i)$ το πολυώνυμο μπορεί να γραφεί ως

$$(t - i)(t + i)(t^2 - 5)$$

με έναν ανάγωγο παράγοντα $t^2 - 5$ βαθμού μεγαλύτερου από 1. Επομένως το πολυώνυμο δεν διασπάται στο $\mathbb{Q}(i)$. Αυτό μας δείχνει ότι αν ένα πολυώνυμο έχει κάποιους γραμμικούς παράγοντες σε μια επέκταση L δεν διασπάται απαραίτητα στο L.

Αν το f είναι ένα πολυώνυμο με συντελεστές από ένα σώμα K και L είναι μια επέκταση του K τότε το f είναι επίσης ένα πολυώνυμο στο L. Λέμε ότι το f διασπάται στο L αν είναι το γινόμενο γραμμικών παραγόντων με συντελεστές από το L. Θα δείξουμε στην συνέχεια ότι αν μας δοθεί ένα πολυώνυμο f με συντελεστές από ένα σώμα K, μπορούμε πάντα να κατασκευάσουμε μια επέκταση Σ του K έτσι ώστε το f να διασπάται στο Σ. Θα πρέπει επίσης το f να μην διασπάται σε κάποιο σώμα μικρότερο από το Σ οπότε το Σ να είναι το μικροτερο δυνατό σώμα που μπορούμε να βρούμε.

Ορισμός 6.1.2 *Το σώμα Σ είναι ένα σώμα διάσπασης για το πολυώνυμο f με συντελεστές από ένα σώμα K αν $K \subseteq \Sigma$ και*

1. *το f διασπάται στο Σ,*
2. *Αν $K \subseteq \Sigma' \subseteq \Sigma$ και το f διασπάται στο Σ' τότε $\Sigma' = \Sigma$.*

Η δεύτερη συνθήκη είναι ισοδύναμη με την:
2′. $\Sigma = K(\sigma_1, \ldots, \sigma_n)$ όπου $\sigma_1, \ldots, \sigma_n$ είναι ρίζες του f στο Σ.

Κατασκευάζουμε ένα σώμα διάσπασης προσθέτωντας στο K τα στοιχεία εκείνα που είναι οι ρίζες του f.

Θεώρημα 6.1.1 *Αν K είναι ένα σώμα και f είναι ένα πολυώνυμο με συντελεστές από το K τότε υπάρχει ένα σώμα διάσπασης για το f.*

Απόδειξη: Θα το αποδείξουμε με επαγωγή στο βαθμό του πολυωνύμου. Αν $\partial f = 1$ τότε το f είναι γραμικό πολυώνυμο οπότε διασπάται ήδη στο K. Αν το f δεν διασπάται στο K τότε έχει έναν ανάγωγο παράγοντα f_1 βαθμού μεγαλύτερου από 1. Χρησιμοποιώντας το θεώρημα 2.3.2 προσθέτουμε το σ_1 στο K, όπου $f(\sigma_1) = 0$. Έπειτα στο $K(\sigma_1)[t]$ έχουμε $f = (t - \sigma_1)g$ όπου $\partial g = \partial f - 1$. Επαγωγικά υπάρχει ένα σώμα διάσπασης Σ για το g στο $K(\sigma_1)$. Όμως τότε το Σ είναι ένα σώμα διάσπασης και για το f.□

Θα δείξουμε στη συνέχεια ότι τα σώματα διάσπασης που μπορούμε να κατασκευάσουμε για κάποιο πολυώνυμο f με συντελεστές από ένα σώμα K είναι μοναδικά ως προς τον ισομορφισμό.

Λήμμα 6.1.1 *Υποθέτουμε ότι $i : K \to K'$ είναι ένας ισομορφισμός σωμάτων. Έστω f ένα πολυώνυμο με συντελεστές από το K και έστω Σ ένα σώμα διάσπασης για το f. Έστω L μια επέκταση του K' έτσι ώστε το $i(f)$ να διασπάται στο L. Τότε υπάρχει ένας μονομορφισμός $j : \Sigma \to L$ έτσι ώστε $j \mid K = i$.*

Απόδειξη: Για να κατανοήσουμε καλύτερα το λήμμα θα κάνουμε το παρακάτω σχήμα

$$\begin{array}{ccccc} & K & \to & \Sigma & \\ i & \downarrow & & \downarrow & j \\ & K' & \to & L & \end{array}$$

όπου το j δεν έχει βρεθεί ακόμα.
Θα χρησιμοποιήσουμε επαγωγή στο βαθμό του f. Ως πολυώνυμο του Σ μπορούμε να το γράψουμε στη μορφή

$$f(t) = k(t - \sigma_1) \dots (t - \sigma_n).$$

όπου $\sigma_1, \dots, \sigma_n \in \Sigma$. Το ελαχιστο πολυώνυμο m του σ_1 στο K είναι ανάγωγος παράγοντας του f. Δηλαδή

$$f = mg$$

όπου g ανάγωγο πολυώνυμο με συντελεστές από το K και $\partial g, \partial m < \partial f$. Επόμένως ισχύει

$$i(f) = i(mg)$$

ή

$$i(f) = i(m)i(g).$$

Άρα το $i(m)$ διαιρεί το $i(f)$ το οποίο από την υπόθεση διασπάται στο L. Επομένως έχουμε

$$i(m) = (t - a_1) \dots (t - a_r)$$

για κάποια $a_1, \dots, a_r \in L$. Το $i(m)$ είναι ανάγωγος παράγοντας του $i(f)$ στο K'. Άρα θα πρέπει να είναι το ελάχιστο πολυώνυμο του a_1 στο K'. Επομένως από το θεώρημα 2.4.3 υπάρχει ένας ισομορφισμός

$$j_1 : K(\sigma_1) \to K'(a_1)$$

έτσι ώστε $j_1|K = i$ και $j_1(\sigma_1) = a_1$. Το Σ είναι ένα σώμα διάσπασης για το πολυώνυμο $h = f/(t - \sigma_1)$ με συντελεστές από το σώμα $K(\sigma_1)$. Αν συνεχίσουμε την ίδια διαδικασία θα καταλήξουμε επαγωγικά ότι υπάρχει ένας μονομορφισμός $j : \Sigma \to L$ έτσι ώστε $j|K(\sigma_1) = j_1$. Όμως τότε $j|K = i$.□

Θεώρημα 6.1.2 *Έστω $i : K \to K'$ ισομορφισμός σωμάτων. Έστω T ένα σώμα διάσπασης για το πολυώνυμο f με συντελεστές από το K και T' ένα σώμα διάσπασης για το πολυώνυμο $i(f)$ με συντελεστές από το K'. Τότε υπάρχει ένας ισομορφισμός $j : T \to T'$ έτσι ώστε $j|K = i$. Με άλλα λόγια οι επεκτάσεις $T : K$ και $T' : K'$ είναι ισομορφικές.*

Απόδειξη: Έχουμε το παρακάτω σχήμα

$$\begin{array}{ccccc} & K & \to & T & \\ i & \downarrow & & \downarrow & j \\ & K' & \to & T' & \end{array}$$

όπου το j δεν έχει βρεθει ακόμα. Από το λήμμα 6.1.1 υπάρχει ένας μονομορφισμός $j : T \to T'$ έτσι ώστε $j|K = i$. Όμως το $j(T)$ είναι ένα σώμα διάσπασης για το $i(f)$ στο K' και περιέχεται στο T'. Εφόσον το T' είναι επίσης ένα σώμα διάσπασης για το $i(f)$ στο K' έχουμε ότι $j(T) = T'$. Άρα ο j είναι επί. Τελικά ο j είναι ένας ισομορφισμός.□

Παράδειγμα 6.1.3 *Έστω $f(t) = (t^2-3)(t^3+1)$ ένα πολυώνυμο στο $\mathbb{Q}$. Θα κατασκευάσουμε ένα σώμα διάσπασης για το f. Το f διασπάται σε γραμμικούς παράγοντες στο $\mathbb{C}$ ως εξής:*

$$f(t) = (t+\sqrt{3})(t-\sqrt{3})(t+1)\left(t-\frac{1+i\sqrt{3}}{2}\right)\left(t-\frac{1-i\sqrt{3}}{2}\right).$$

Επομένως το σώμα διάσπασης του f είναι ένα υπόσωμα του $\mathbb{C}$ το

$$\mathbb{Q}\left(\sqrt{3}, \frac{1+i\sqrt{3}}{2}\right).$$

Το οποίο είναι το ίδιο με το $\mathbb{Q}(i, \sqrt{3})$.

Παράδειγμα 6.1.4 *Έστω $f(t) = (t^2-2t-2)(t^2+1)$ στο $\mathbb{Q}$. Οι ρίζες του f στο $\mathbb{C}$ είναι $1 \pm \sqrt{3}$, $\pm i$. Επομένως το σώμα διάσπασης του πολυωνύμου είναι το $\mathbb{Q}(1+\sqrt{3}, i)$ το οποίο είναι ίδιο με το $\mathbb{Q}(i, \sqrt{3})$.*

Παράδειγμα 6.1.5 *Είναι δυνατό να έχουμε δύο διαφορετικά πολυώνυμα τα οποία έχουν το ίδιο σώμα διάσπασης. Τα πολυώνυμα t^2-3 και t^2-2t-2 στο $\mathbb{Q}$ έχουν ως σώμα διάσπασης το $\mathbb{Q}(\sqrt{3})$. Το πρώτο πολυώνυμο έχει ρίζες τις $\pm\sqrt{3}$ και επομένως σώμα διάσπασης το $\mathbb{Q}(\sqrt{3})$ και το δεύτερο έχει ρίζες τις $1+\sqrt{3}$, $1+\sqrt{3}$ και σώμα διάσπασης το $\mathbb{Q}(1+\sqrt{3})$ που είναι ίδιο με το $\mathbb{Q}(\sqrt{3})$.*

Παράδειγμα 6.1.6 *Έστω το πολυώνυμο* $f(t) = t^2 + t + 1$ *στο* $\mathbb{Z}_2$. *Το* f *είναι ανάγωγο στο* $\mathbb{Z}_2$. *Για να κατασκευάσουμε το σώμα διάσπασης του* f *θα πρέπει να προσθέσουμε στο* $\mathbb{Z}_2$ *ένα στοιχείο* ζ *τέτοιο ώστε το* ζ *να έχει ελάχιστο πολυώνυμο το* f *στο* $\mathbb{Z}_2$. *Τότε θα ισχύει* $\zeta^2 + \zeta + 1 = 0$ *δηλαδή* $\zeta^2 = \zeta + 1$. *Επομένως το σώμα διάσπασης θα πρέπει να περιέχει τα στοιχεία* $0, 1, \zeta, 1 + \zeta$ *με τις εξής πράξεις:*

$+$	0	1	ζ	$1+\zeta$
0	0	1	ζ	$1+\zeta$
1	1	0	$1+\zeta$	ζ
ζ	ζ	$1+\zeta$	0	1
$1+\zeta$	$1+\zeta$	ζ	1	0

$\cdot$	0	1	ζ	$1+\zeta$
0	0	0	0	0
1	0	1	ζ	$1+\zeta$
ζ	0	ζ	$1+\zeta$	1
$1+\zeta$	0	$1+\zeta$	1	ζ

Για την διαμόρφωση των παραπάνω πινάκων έγιναν οι εξής υπολογισμοί:

- $\zeta + \zeta = 2\zeta = 0$.
- $\zeta\zeta = \zeta^2 = 1 + \zeta$.
- $\zeta(1 + \zeta) = \zeta + \zeta^2 = \zeta + \zeta + 1 = 2\zeta + 1 = 1$.

Επομένως το $\mathbb{Z}_2(\zeta)$ *είναι ένα σώμα με τέσσερα στοιχεία. Το* f *διασπάται στο* $\mathbb{Z}_2(\zeta)$ *ως:*

$$t^2 + t + 1 = (t - \zeta)(t - 1 - \zeta)$$

και δεν διασπάται σε κανένα μικρότερο σώμα. Άρα το $\mathbb{Z}_2(\zeta)$ *είναι ένα σώμα διάσπασης για το* f.

6.2 Κανονικότητα

Ορισμός 6.2.1 *Μία επέκταση* $L : K$ *είναι κανονική αν κάθε ανάγωγο πολυώνυμο στο* K, *το οποίο έχει μια τουλάχιστον ρίζα στο* L, *διασπάται στο* L.

Για παράδειγμα η επέκταση $\mathbb{C} : \mathbb{R}$ είναι κανονική διότι κάθε πολυώνυμο με συντελεστές από το $\mathbb{R}$ είτε είναι ανάγωγο είτε όχι διασπάται στο $\mathbb{C}$.
Η επέκταση $\mathbb{Q}(a) : \mathbb{Q}$ όπου $a = \sqrt[3]{2}$ δεν είναι κανονική. Το πολυώνυμο $t^3 - 2$

έχει μια ρίζα, το a, στο $\mathbb{Q}(a)$ όμως δεν διασπάται στο $\mathbb{Q}(a)$ αφού οι υπόλοιπες ρίζες του ανήκουν στο $\mathbb{C}$.
Για την κανονική επέκταση $\mathbb{C} : \mathbb{R}$ η αντιστοιχία *Galois* που είδαμε στο προηγούμενο κεφάλαιο είναι ένα προς ένα ενω για την μη-κανονική επέκταση $\mathbb{Q}(a) : \mathbb{Q}$ η αντιστοιχία *Galois* δεν είναι ένα προς ένα.

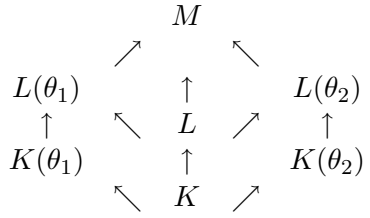
Θεώρημα 6.2.1 *Μία επέκταση $L : K$ είναι κανονική και πεπερασμένη αν και μόνο αν το L είναι ένα σώμα διάσπασης για κάποια πολυώνυμα στο K.*

Απόδειξη: Έστω ότι η επέκταση $L : K$ είναι κανονική και πεπερασμένη. Από το λήμμα 3.1.1 θα πρέπει να ισχύει $L = K(a_1, \ldots, a_s)$ για κάποια a_i αλγεβρικά στο K. Έστω m_i το ελάχιστο πολυώνυμο για το a_i στο K και έστω $f = m_1 \ldots m_s$. Κάθε m_i είναι ανάγωγο στο K και έχει μια ρίζα a_i στο L. Επομένως απο τον ορισμό της κανονικότητας το f διασπάται στο L. Εφόσον το L παράγεται από το K και τις ρίζες του f, είναι ένα σώμα διάσπασης για το πολυώνυμο f.

Έστω ότι το L είναι ένα σώμα διάσπασης για κάποια πολυώνυμα g στο K. Τότε η επέκταση είναι πεπερασμένη αφού $L = K(\beta_1, \ldots, \beta_r)$, όπου $\beta_1, \ldots, \beta_r$ είναι οι ρίζες των πολυωνύμων g. Μένει να δείξουμε ότι είναι κανονική. Έστω f ένα ανάγωγο πολυώνυμο στο K με μια ρίζα στο L. Θα πρέπει να δείξουμε ότι το f διασπάται στο L. Έστω $M \supseteq L$ ένα σώμα διάσπασης για το fg με συντελεστές από το K. Υποθέτουμε ότι θ_1 και θ_2 είναι ρίζες του f στο M. Ισχυριζόμαστε ότι

$$[L(\theta_1) : L] = [L(\theta_2) : L].$$

Θα το αποδείξουμε στη συνέχεια. Θα μελετήσουμε τα διάφορα υποσώματα του M, τα οποία περιγράφονται στο παρακάτω σχήμα:



όπου τα βέλη δηλώνουν ένα προς ένα σχέσεις. Για j=1 ή 2 έχουμε:

$$[L(\theta_j) : L][L : K] = [L(\theta_j) : K] = [L(\theta_j) : K(\theta_j)][K(\theta_j) : K].$$

Από την πρόταση 3.1.1 έχουμε ότι $[K(\theta_1) : K] = [K(\theta_2) : K]$. Το $L(\theta_j)$ είναι ένα σώμα διάσπασης για το g στο $K(\theta_j)$ και από το θεώρημα 2.4.2 η επέκταση $K(\theta_1)$ είναι ισομορφική με την $K(\theta_2)$. Άρα από το θεώρημα 6.1.2

οι επεκτάσεις $L(\theta_j) : K(\theta_j)$ είναι ισομορφικές για j=1, 2 και άρα έχουν τον ίδιο βαθμό. Άρα τελικά έχουμε:

$$[L(\theta_1) : L][L : K] = [L(\theta_1) : K] = xy$$

και

$$[L(\theta_2) : L][L : K] = [L(\theta_2) : K] = xy$$

όπου

$$x = [L(\theta_1) : K(\theta_1)] = [L(\theta_2) : K(\theta_2)]$$

και

$$y = [K(\theta_1) : K] = [K(\theta_2) : K].$$

Συνεπώς ισχύει

$$[L(\theta_1 : L] = [L(\theta_2) : L].$$

Όμως τότε αν $\theta_1 \in L$ έχουμε $[L(\theta_1) : L] = 1$ άρα και $[L(\theta_2) : L] = 1$ οπότε και $\theta_2 \in L$. Δηλαδή η επέκταση $L : K$ είναι κανονική.□

6.3 Διαχωρισιμότητα

Ορισμός 6.3.1 *Ένα ανάγωγο πολυώνυμο f με συντελεστές από ένα σώμα K είναι διαχωρίσιμο στο σώμα K αν δεν έχει πολλαπλές ρίζες σε ένα σώμα διάσπασης.*

Αυτό σημαίνει ότι σε οποιοδήποτε σώμα διάσπασης το f γράφεται ως εξής:

$$f(t) = k(t - \sigma_1) \dots (t - \sigma_n)$$

όπου τα σ_i είναι όλα διαφορετικά μεταξύ τους.

Ορισμός 6.3.2 *Ένα ανάγωγο πολυώνυμο σε ένα σώμα K είναι μη διαχωρίσιμο στο K αν δεν είναι διαχωρίσιμο στο K.*

Παράδειγμα 6.3.1 *Το πολυώνυμο $t^4+t^3+t^2+t+1$ είναι διαχωρίσιμο στο $\mathbb{Q}$ διότι έχει ένα σώμα διάσπασης μέσα στο $\mathbb{C}$ όπου οι ρίζες του είναι $\exp(2\pi i/5)$, $\exp(4\pi i/5)$, $\exp(6\pi i/5)$, $exp(8\pi i/5)$ και είναι όλες διαφορετικές μεταξύ τους.*

Παράδειγμα 6.3.2 *Έστω $K_0 = \mathbb{Z}_p$ όπου p είναι πρώτος αριθμός. Έστω $K = K_0(u)$ όπου το u είναι υπερβατικό στο K_0 και έστω*

$$f(t) = t^p - u \ \in K[t].$$

Έστω Σ ένα σώμα διάσπασης για το πολυώνυμο f και έστω τ μια ρίζα του f στο Σ. Τότε $\tau^p = u$. Έχουμε

$$(t-\tau)^p = t^p + \binom{p}{1} t^{p-1}(-\tau) + \ldots + (-\tau)^p$$

από το δυωνυμικό θεώρημα. Όμως όλοι οι δυωνυμικοί συντελεστές

$$\binom{p}{r}$$

όπου $0 < r < p$ διαιρούνται από το p διότι στην έκφραση $p!/[r!(p-r)!]$ ο παράγοντας p στον αριθμητή δεν υπάρχει στον παρονομαστή. Στο K όμως κάθε πολλαπλάσιο του p είναι 0, άρα τελικά παίρνουμε τη σχέση:

$$(t-\tau)^p = t^p - \tau^p = t^p - u = f(t).$$

Αν $\sigma^p - u = 0$ τότε $(\sigma - \tau)^p = 0$ και άρα $\sigma = \tau$. Συνεπώς όλες οι ρίζες του f στο Σ είναι ίσες.
Μένει να δείξουμε ότι το f είναι ανάγωγο στο K. Υποθέτουμε ότι $f = gh$, όπου $g, h \in K[t]$ και $\partial g, \partial h < \partial f$. Δηλαδή $gh = (t-\tau)^p$. Από μοναδικότητα της παραγοντοποίησης θα πρέπει να έχουμε $g(t) = (t-\tau)^s$ όπου $0 < s < p$. Δηλαδή $g(t) = t^s + \binom{s}{1} t^{s-1}(-\tau) + \ldots + (-\tau)^s$. Όμως ο σταθερός συντελεστής τ^s του g ανήκει στο K. Επειδή $0 < s < p$ και ο p είναι πρώτος, τα p, s είναι πρώτα μεταξύ τους. Άρα υπάρχουν a, b έτσι ώστε να ισχύει $as + bp = 1$. Όμως $\tau^s, \tau^p \in K$ άρα και $\tau^{as}, \tau^{bp} \in K$. Επομένως και $\tau^{as}\tau^{bp} \in K$, δηλαδή $\tau^{as+bp} \in K$ ή $\tau \in K$ αφού $as + bp = 1$. Επειδή $\tau \in K_0(u)$ θα πρέπει να ισχύει $\tau = v(u)/w(u)$ όπου $v, w \in K_0(u)$. Οπότε αν αντικαταστήσουμε στην σχέση $\tau^p = u$ έχουμε

$$(v(u)/w(u))^p = u$$

ή

$$v(u)^p = u(w(u))^p$$

δηλαδή

$$v(u)^p - u(w(u))^p = 0.$$

Όμως οι όροι των μεγιστοβάθμιων όρων δεν μπορούν να διαγραφούν και άρα το f είναι ανάγωγο. Επομένως το πολυώνυμο είναι μη διαχωρίσιμο.

6.4 Τυπική διαφόριση

Ορισμός 6.4.1 *Έστω ότι*

$$f(t) = a_0 + a_1 t + \ldots + a_n t^n \ \in K[t]$$

για κάποιο σώμα K. Τότε η τυπική παράγωγος του f είναι το πολυώνυμο:

$$Df = a_1 + 2a_2t + \ldots + na_nt^{n-1}.$$

Για $K = \mathbb{R}$ είναι η συνηθισμένη παράγωγος. Για όλα τα πολυώνυμα f και g με συντελεστές από ένα σώμα K και αν $\lambda \in K$ ισχύουν τα παρακάτω.

- $D(f+g) = Df + Dg$
- $D(fg) = Df \cdot g + f \cdot Dg$
- $D(\lambda) = 0$
- $D(\lambda f) = \lambda \cdot Df$.

Αυτές οι ιδιότητες μας επιτρέπουν να δώσουμε ένα κριτήριο για την ύπαρξη πολλαπλών ριζών χώρίς να γνωρίζουμε ποιες είναι οι ρίζες αυτές.

Λήμμα 6.4.1 *Ένα πολυώνυμο $f \neq 0$ με συντελεστές από ένα σώμα K έχει μια πολλαπλή ρίζα σε ένα σώμα διάσπασης αν και μόνο αν το f και το Df έχουν ένα κοινό παράγοντα βαθμού ≥ 1.*

Απόδειξη: Έστω ότι το f έχει μια πολλαπλή ρίζα σε ένα σώμα διάσπασης Σ, επομένως το πολυώνυμο στο Σ γράφεται:

$$f(t) = (t-a)^2 g(t)$$

όπου το $a \in \Sigma$. Τότε

$$Df = (t-a)\{(t-a)Dg + 2g\}$$

και άρα το f και το Df έχουν ένα κοινό παράγοντα το $(t-a) \in \Sigma[t]$. Επομένως το f και το Df έχουν ένα κοινό παράγοντα στο $K[t]$ που ονομάζεται το ελάχιστο πολυώνυμο του a στο K.

Υποθέτουμε ότι το f δεν έχει πολλαπλές ρίζες. Θα δείξουμε με επαγωγή στο βαθμό του f ότι τα f και Df είναι πρώτα μεταξύ τους στο $\Sigma[t]$ οπότε και πρώτα μεταξύ τους στο $K[t]$. Αν $\partial f = 1$ τότε φανερά τα δύο πολυώνυμα είναι πρώτα μεταξύ τους. Διαφορετικά $f(t) = (t-a)g(t)$ όπου το $(t-a) \not| g(t)$. Τότε

$$Df = (t-a)Dg + g.$$

Αν ένας παράγοντας του g διαιρεί το Df θα πρέπει επίσης να διαιρεί και το Dg εφόσον υποθέσαμε ότι το $(t-a)$ δεν είναι παράγοντας του g. Όμως τα g και Dg είναι πρώτα μεταξύ τους άρα και τα f και Df θα πρέπει να είναι πρώτα

μεταξύ τους.□

Μπορούμε τώρα να δώσουμε ικανές και αναγκαίες συνθήκες για την διαχωρισιμότητα ενός ανάγωγου πολυωνύμου.

Πρόταση 6.4.1 *Αν K είναι ένα σώμα χαρακτηριστικής 0 τότε κάθε ανάγωγο πολυώνυμο με συντελεστές από το K είναι διαχωρίσιμο στο K. Αν το K έχει χαρακτηριστική $p > 0$ τότε ένα ανάγωγο πολυώνυμο με συντελεστές από το K είναι μη διαχωρίσιμο αν και μόνο αν*

$$f(t) = k_0 + k_1 t^p + \ldots + k_r t^{rp} \tag{6.1}$$

όπου $k_0, k_1, \ldots, k_r \in K$.

Απόδειξη: Ένα ανάγωγο πολυώνυμο f με συντελεστές από το K είναι μη διαχωρίσιμο αν και μόνο αν το f και το Df έχουν ένα κοινό παράγοντα βαθμού ≥ 1. Αν ισχύει αυτό, επειδή το f είναι ανάγωγο και το Df έχει μικρότερο βαθμό από το f, θα πρέπει να έχουμε $Df = 0$. Δηλαδή αν

$$f(t) = a_0 + a_1 t + \ldots + a_n t^n$$

τότε

$$Df = a_1 + 2a_2 t + \ldots + n a_n t^{n-1}.$$

Για να ισχύει $Df = 0$ θα πρέπει $na_n = 0\ \forall n \in \mathbb{Z}$. Αν το σώμα έχει χαρακτηριστική μηδέν για να ισχύει αυτό θα πρέπει $a_n = 0\ \forall n \in \mathbb{Z}$. Δηλαδή σ'ενα σώμα χαρακτηριστικής 0 μόνο τα μηδενικά πολυώνυμα είναι μη διαχωρίσιμα και όλα τα πολυώνυμα βαθμου $\neq 0$ είναι διαχωρίσιμα. Αν το σώμα έχει χαρακτηριστική $p > 0$, για να ισχύει $na_n = 0\ \forall n \in \mathbb{Z}$, θα πρέπει $a_n = 0$ αν το p δεν διαιρεί το n. Θέτουμε $k_i = a_{pi}$ και παίρνουμε το τη σχέση (6.1).□

Σημείωση: Η συνθήκη για την διαχωρισιμότητα ενός πολυωνύμου σε σώματα χαρακτηριστικής $p > 0$ μπορεί να εκφραστεί λέγοντας ότι υπάρχουν μόνο δυνάμεις του t που είναι πολλαπλάσια του p. Έτσι ισχύει $f(t) = g(t^p)$ για κάποια πολυώνυμα g με συντελεστές από το σώμα K.

Ορισμός 6.4.2 *Ένα πολυώνυμο με συντελεστές από ένα σώμα K είναι διαχωρίσιμο στο K αν όλοι οι ανάγωγοι παράγοντές του είναι διαχωρίσιμοι στο K.*

Αν $L : K$ είναι μια επέκταση τότε ένα αλγεβρικό στοιχείο $a \in L$ είναι διαχωρίσιμο στο K αν το ελάχιστο πολυώνυμό του στο K είναι διαχωρίσιμο στο K.

Μια αλγεβρική επέκταση $L : K$ είναι διαχωρίσιμη επέκταση αν κάθε στοιχείο $a \in L$ είναι διαχωρίσιμο στο K.

Θα δείξουμε στη συνέχεια ότι η διαχωρισιμότητα των αλγεβρικών επεκτάσεων ισχύει και για τα ενδιάμεσα σώματα.

Λήμμα 6.4.2 *Αν $L : K$ είναι μια διαχωρίσιμη αλγεβρική επέκταση και M ένα ενδιάμεσο σώμα τότε οι επεκτάσεις $M : K$ και $L : M$ είναι διαχωρίσιμες.*

Απόδειξη: Η $L : K$ είναι μια διαχωρίσιμη αλγεβρική επέκταση και επομένως για κάθε στοιχείο που ανήκει στο L το ελάχιστο πολυώνυμό του είναι διαχωρίσιμο στο Κ. Επειδή $M \subseteq L$ σημαίνει ότι και για κάθε στοιχείο που ανήκει στο M το ελάχιστο πολυώνυμό του είναι διαχωρίσιμο στο Κ. Άρα η επέκταση $M : K$ είναι διαχωρίσιμη. Έστω ότι $a \in L$ και έστω m_K και m_M τα ελάχιστα πολυώνυμα του a στα σώματα Κ και Μ αντίστοιχα. Το $m_M | m_K$ στο $M[t]$. Όμως το a είναι διαχωρίσιμο στο Κ άρα και το m_K είναι διαχωρίσιμο στο Κ. Αφού το $m_M | m_K$, το m_M είναι ένας παράγοντας του m_K και μάλιστα ανάγωγος, επομένως και το m_M είναι διαχωρίσιμο στο Μ. Δηλαδή η επέκταση $L : M$ είναι διαχωρίσιμη.□

Παράδειγμα 6.4.1 *Να κατασκευάσετε τα υποσώματα του $\mathbb{C}$ τα οποία είναι σώματα διάσπασης στο $\mathbb{Q}$ για τα πολυώνυμα:*
(a) $t^3 - 1$
(b) $t^4 + 5t^2 + 6$
(c) $t^6 - 8$

Απάντηση:
(a) Οι ρίζες του πολυωνύμου είναι 1, $\exp(2\pi i/3)$, $\exp(4\pi i/3)$ και το σώμα διάσπασης $\mathbb{Q}(\exp(2\pi i/3))$.

(b) Οι ρίζες του πολυωνύμου είναι $\pm\sqrt{3}i$, $\pm\sqrt{2}i$ και το σώμα διάσπασης $\mathbb{Q}(\sqrt{3}i, \sqrt{2}i)$.

(c) Οι ρίζες του πολυωνύμου είναι $\sqrt{2}$, $-\sqrt{2}$, $\sqrt{2}\exp(2\pi i/6)$, $\sqrt{2}\exp(4\pi i/6)$, $\sqrt{2}\exp(8\pi i/6)$, $\sqrt{2}\exp(10\pi i/6)$ και το σώμα διάσπασης $\mathbb{Q}(\sqrt{2}, \exp(\pi i/3))$.

Παράδειγμα 6.4.2 *Βρείτε τους βαθμούς των παραπάνω επεκτάσεων του $\mathbb{Q}$.*

Απάντηση:
(a) $[\mathbb{Q}(\exp(2\pi i/3)) : \mathbb{Q}] = 3$ γιατί τα $\{1, \exp(2\pi i/3), \exp(4\pi i/3)\}$ είναι μια βάση του $\mathbb{Q}(\exp(2\pi i/3))$ με σώμα το $\mathbb{Q}$.

(b) $[\mathbb{Q}(\sqrt{3}i, \sqrt{2}i) : \mathbb{Q}] = 4$ γιατί τα $\{1, \sqrt{3}i, \sqrt{2}i, \sqrt{6}\}$ είναι μια βάση του

$\mathbb{Q}(\sqrt{3}i, \sqrt{2}i)$ με σώμα το $\mathbb{Q}$

(*c*) $[\mathbb{Q}(\sqrt{2}, \exp(\pi i/3)) : \mathbb{Q}] = 10$ γιατί τα $\{1, \sqrt{2}, \exp(2\pi i/6), \exp(4\pi i/6), \exp(8\pi i/6), \exp(10\pi i/6), \sqrt{2}\exp(2\pi i/6), \sqrt{2}\exp(4\pi i/6), \sqrt{2}\exp(8\pi i/6), \sqrt{2}\exp(10\pi i/6)\}$ είναι μια βάση του $\mathbb{Q}(\sqrt{2}, \exp(\pi i/3))$ με σώμα το $\mathbb{Q}$.