ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ

Θεωρία Σωμάτων

Όνομα Καθηγητή: **Ιωάννης Αντωνιάδης**

Τμήμα: **Μαθηματικών και Εφαρμοσμένων Μαθηματικών**

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται στην άδεια χρήσης **Creative Commons** και ειδικότερα

Αναφορά – Μη εμπορική Χρήση – Όχι Παράγωγο Έργο v.3.0

(Attribution – Non Commercial – Non-derivatives v.3.0)

- Εξαιρείται από την ως άνω άδεια υλικό που περιλαμβάνεται στις διαφάνειες του μαθήματος, και υπόκειται σε άλλου τύπου άδεια χρήσης. Η άδεια χρήσης στην οποία υπόκειται το υλικό αυτό αναφέρεται ρητώς.

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Κρήτης**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Θεωρία Σωμάτων

Ιωάννης Αντωνιάδης

18 Μαρτίου 2015

Περιεχόμενα

Κεφάλαιο 1

ΕΙΣΑΓΩΓΗ

Το πρόβλημα - κίνητρο δημιουργίας και ανάπτυξης της θεωρίας αποτέλεσε η λύση πολυωνυμικών εξισώσεων.

Από την ύπαρξη Βαβυλωνιακού κώδικα του 1600 π.Χ. στον οποίο αναφέρεται πρόβλημα αναγόμενο στην λύση δευτεροβάθμιας εξίσωσης συνάγουμε ότι οι Βαβυλώνιοι κατείχαν μέθοδο επίλυσης της.[Midonic, [1965], σελίδα 48, Bourbaki, [1969], σελίδα 92]

Κατά τους Bourbaki και πάλι [Bourbaki, 1969, σελίδα 102] οι αρχαίοι Έλληνες έλυσαν εξισώσεις δευτέρου βαθμού μέσω γεωμετρικών κατασκευών αλλά χωρίς αλγεβρική τυποποίηση, τουλάχιστον μέχρι το 100 μ.Χ.

Η γενική εξίσωση τρίτου βαθμού λύθηκε για πρώτη φορά από τον Nicolo Fontana (ο οποίος είχε το παρατσούκλι Tartagria) το 1535. Ειδικές περιπτώσεις αυτής είχαν μελετηθεί νωρίτερα από τον Scipio del Ferro. Ο Fontana κράτησε μυστικές τις λεπτομέριες της μεθόδου του τις οποίες αργότερα εμπιστεύθηκε στον Girolamo Gardano, αφού πρώτα απαίτησε από αυτόν να ορκιστεί ότι θα τις κρατήσει μυστικές. Η μέθοδος του Tartagria έγινε γνωστή όταν ο Cardano δημοσίευσε το 1545 την Ars Magna του. Η διατριβή αυτή του Cardano περιέχει και την μέθοδο επίλυσης της γενικής εξίσωσης τετάρτου βαθμού και αποδίδεται στον Loudovico Ferrari.

Οι τύποι ο οποίοι μας δίνουν τις λύσεις προκύπτουν από τις τέσσερις πράξεις της αριθμητικής μεταξύ των συντελεστών της εξίσωσης και εξαγωγή ριζών, λέγονται δε

ριζικές εκφράσεις.

Εντελώς φυσιολογικό ήταν να ακολουθήσει προσπάθεια επίλυσης της γενικής εξίσωσης πέμπτου βαθμού. Όλες αυτές οι προσπάθειες απέτυχαν.

Πρώτος ο J.-L. Lagrange σε δύο μνημόνια του (Memoirs) πρός την Ακαδημία Επιστημών του Βερολίνου, αφού συστηματοποίησε τις μεθόδους επίλυσης για εξισώσεις μέχρι και τετάρτου βαθμού, παρατήρησε ότι η προσέγγιση του αυτή δεν επεκτείνεται σε εξισώσεις πέμπτου βαθμού. Για πρώτη φορά οι αλγεβριστές της περιόδου αυτής υποψιάζονται ότι ίσως η γενική εξίσωση πέμπτου βαθμού δεν είναι επιλύσιμη με ριζικά. Αυτό αποδείχθηκε στα 1826 από τον Abel, έπειτα από αρκετές αλλά λανθασμένες, προηγούμενες απόπειρες του Ruffini. Ο Abel συνέχισε να εργάζεται στο ίδιο θέμα μέχρι το θάνατο του, το 1829.

Το επόμενο ερώτημα που προκύπτει απολύτως φυσιολογικά είναι η εύρεση ενός κριτηρίου για το πότε η (γενική) εξίσωση πέμπτου ή ανωτέρου βαθμού είναι επιλύσιμη με ριζικά και πότε όχι. Απάντηση στο ερώτημα αυτό έδωσε ο Evariste Galois το 1832 λίγο πριν τον θάνατό του. Η ιδέα του ήταν πράγματι μεγαλοφυής. Θα πρέπει κανείς να λάβει υπ΄ όψιν του ότι αυτό επιτεύχθηκε σε μία εποχή όπου η λεγόμενη μοντέρνα Άλγεβρα ουσιαστικά δεν υπήρχε.

Η επιτυχία αυτή του Galois έμελε να μείνει άγνωστη για τα επόμενα περίπου 10 χρόνια. Εργασίες που είχε υποβάλει για δημοσίευση στην Ακαδημία Επιστημών του Παρισιού δεν είχαν γίνει δεκτές και "χάθηκαν" μέχρι την 4η Ιουλίου 1843 όταν τα αποτελέσματά του ανακοινώθηκαν στην Ακαδημία από τον Joseph Liouville. Φαίνεται ότι οι ιδέες του προπορεύονταν κατά πολύ της εποχής του.

Αργότερα φάνηκε ότι η θεωρία του Galois μπορρεί να εφαρμοστεί και να δώσει απαντήσεις σε τέσσερα γεωμετρικά προβλήματα. Τα τρία από αυτά είναι τα ακόλουθα, γνωστά ως «Τα τρία άλυτα προβλήματα της Αρχαιότητας».

Με την βοήθεια μόνο κανόνα και διαβήτη,

1 Να τριχοτομηθεί δοθείσα, οποιαδήποτε γωνία.

2 Δίδεται κύβος ακμής α, να κατασκευαστεί κύβος με διπλάσιο όγκο.

3 Να κατασκευαστεί τετράγωνο το οποίο έχει εμβαδόν ίσο προς το εμβαδόν δοθέντος

κύκλου (τετραγωνισμός του κύκλου).

Στα 1796 ο δεκαεννιάχρονος Gauss απέδειξε το κατασκευάσιμο του κανονικού 17-γώνου. Λίγα χρόνια αργότερα διετύπωσε ικανή και αναγκαία συνθήκη για την κατασκευή κανονικού n-γώνου. Απέδειξε μόνο την μία κατεύθυνση της ισοδυναμίας. Η άλλη αποδείχθηκε από τον Wantzel το 1837:

4 Κατασκευή κανονικού η-γώνου.

Βρίσκει την λύση του στα πλαίσια της θεωρίας Galois. Απετέλεσε μάλιστα την αφορμή για να μελετηθούν και τα τρία παραπάνω προβλήματα με αλγεβρικές μεθόδους.

Η ιδέα του Galois ήταν στη λεγόμενη σήμερα επέκταση του Galois , να αντιστοιχίσει μια ομάδα συναρτήσεων (αυτομορφισμούς) αυτής, τη λεγόμενη ομάδα του Galois της δοθείσης επέκτασης.

Η ιδέα αυτή διατυπώθηκε γενικότερα στο ″Πρόγραμμα Erlangen″ του Felix Klein στα 1871.

Η θεωρία Galois θεωρείται σήμερα σαν ένας από τους πιο σημαντικούς και όμορφους κλάδους της Άλγεβρας. Έχει εφαρμογές στη Θεωρία Δακτυλίων, Αλγεβρική Θεωρία Αριθμών, Διαφορικές Εξισώσεις, Αλγεβρική Τοπολογία και Αλγεβρική Γεωμετρία.

Την οριστική μορφή παρουσίασης της θεωρίας χρωστούμε στον Emil Artin [δες, π.χ. έκδοση Notre Dame του Βιβλίου του].

Ηράκλειο 25/9/2005

Κεφάλαιο 2

ΠΡΟΛΕΓΟΜΕΝΑ

2.1 Δακτύλιοι και Σώματα

R αντιμεταθετικός δακτύλιος με μοναδιαίο $(1 \neq 0)$

R ακέραια περιοχή $\Leftrightarrow$ (επί πλέον *δεν* έχει διαιρέτες του μηδενός)

Ο **νόμος της διαγραφής** ισχύει στην R

Αν $a, b, c \in R, c \neq 0$ τότε $R' \leq R$ (υποδακτύλιος) $(R' \neq 0) \Leftrightarrow (\forall a, b \in R' \Rightarrow a - b \in R')$

Κ σώμα: Αντιμεταθετικός δακτύλιος με μοναδιαίο τ.ω. $(\forall a \in K, \exists b (= a^{-1}) \in K)$ τ.ω. $aa^{-1} = 1$

L σώμα, Ο υποδακτύλιος $K \leq L$ θα λέγεται υπόσωμα του $L \Leftrightarrow K$ σώμα.

Παραδείγματα:

$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}_p \forall p \in \mathbb{P}$

$\mathbb{Z}[i] = \{a + bi / a, b \in \mathbb{Z}\}$ ακέραια περιοχή με μοναδιαίο

ενώ το $\mathbb{Q}(i) = \{a + bi / a, b \in \mathbb{Q}\}$ σώμα.

Άσκηση:

$\mathbb{Z}[\sqrt{2}]$ ακέραια περιοχή με μοναδιαίο $\mathbb{Q}(\sqrt{2})$ σώμα.

Σώμα πηλίκων:

$\mathbb{Z}, \mathbb{Q} = \{\frac{a}{b}/a, b \in \mathbb{Z}, b \neq 0\}$

Συμβολισμός: $\mathbb{Q} = Quot(\mathbb{Z})$

Ιδεώδες:

$I \subseteq R, I \neq \emptyset$ και $\left\{ \begin{array}{l} (i)\forall a, b \in I \Rightarrow a - b \in I \\ (ii)\forall a \in I, \forall r \in R \Rightarrow ra \in I \end{array} \right\}$

Κάθε ιδεώδες είναι υποδακτύλιος του R.

Το αντίστροφο δεν ισχύει.

π.χ. $\mathbb{Z}$ = υποδακτύλιος του $\mathbb{Q}$ αλλά όχι ιδεώδες.

Συμβολισμός του ιδεώδους: $I \trianglelefteq R$

Πρόταση:

R αντιμεταθετικός δακτύλιος με $1 \in R$

R σώμα $\Leftrightarrow$ ο R έχει ακριβώς δύο ιδεώδη, τα $< 0 >$ και R

Ομομορφισμοί δακτυλίων:

$$\phi : R \to R' \Leftrightarrow \left\{ \begin{array}{ll} (i)\phi(a+b) = \phi(a) + \phi(b) & \forall a, b \in R \\ (ii)\phi(ab) = \phi(a)\phi(b) & \forall a, b \in R \\ (iii)\phi(1_R) = 1_{R'} & \end{array} \right\}$$

φ ομομορφισμός δακτυλίων τότε:

- φ μονομορφισμός $\Leftrightarrow$ φ είναι 1-1
- φ επιμορφισμός $\Leftrightarrow$ φ είναι επί
- φ ισομορφισμός $\Leftrightarrow$ φ είναι 1-1 και επί

Τότε λέμε ότι οι δακτύλιοι είναι ισόμορφοι $R \cong R'$

$\phi : R \to R$ Αν φ ισομορφισμός τότε θα λέγεται αυτομορφισμός του R

Ορισμός: Ομομορφισμός σωμάτων

$\phi : K \to L$ είναι ομομορφισμός σωμάτων όταν ο φ είναι ομομορφισμός δακτυλίων.

$Ker\phi = \{a \in K / \phi(a) = 0\} \trianglelefteq K$

$\Rightarrow Ker\phi =< 0 >$ ή $Ker\phi = K$

Όμως $\phi(1_K) = 1_L \neq 0 \Rightarrow 1_K \notin Ker\phi \Rightarrow Ker\phi =< 0 > \Rightarrow \phi$ μονομορφισμός.

Ώστε $\phi : K \to L \Rightarrow K \cong \phi(K) \leq L$

Ταυτίζουμε Κ με $\phi(K) \Rightarrow K \hookrightarrow L$

Πρόταση:

Τώρα, αν R ακέραια περιοχή και $K = Quot(R)$, το Κ είναι το ελάχιστο σώμα που περιέχει την R.

Δηλαδή, αν $R \leq L \Rightarrow K \leq L$

Απόδειξη:

Έστω $a, b \in R, b \neq 0$

L σώμα, $b \in L, b \neq 0 \Rightarrow b^{-1} \in L$

$a \in L$ και $b^{-1} \in L \Rightarrow ab^{-1} = \frac{a}{b} \in L$

Χαρακτηριστική δακτυλίου R (R αντιμεταθετικός δακτύλιος με 1_R)

Αν $a \in R$, τότε γράφουμε το $a + a$ σαν $2a$.

Αν $n \in N$, γράφουμε το άθροισμα $a + a + ... + a = n \cdot a$

Ορίζουμε $0 \cdot a := 0_R$ και $(-n)a = n(-a) = (-a) + (-a) + ... + (-a)$

Ξεχωρίζουμε δύο περιπτώσεις:

1. Τα στοιχεία $m \cdot 1_R (m = 1, 2, 3, ...)$ είναι όλα διαφορετικά (διακεκριμένα) μεταξύ τους.
2. $\exists m, n \in \mathbb{N}$ τ.ω. $m \cdot 1_R = (m + n) \cdot 1_R$

Στην πρώτη περίπτωση λέμε ότι η χαρακτηριστική του R είναι μηδέν. $chR = 0$.

Στην δεύτερη περίπτωση έχουμε $n \cdot 1_R = 0_R$, για κάποιο $n \in \mathbb{N}$.

Αρχή του ελαχίστου:

Κάθε μη-κενό υποσύνολο του $\mathbb{N}$ έχει ελάχιστο στοιχείο.

Επομένως, υπάρχει ελάχιστος φυσικός n, τ.ω. $n \cdot 1_R = 0_R$.

Ορισμός:

Ο n αυτός θα λέγεται *χαρακτηριστική* του R. $chR = n$. Στην ειδική περίπτωση που $R = K =$ σώμα ισχύει:

Πρόταση:

Η χαρακτηριστική σώματος είναι η 0 ή $p \in \mathbb{P}$

Απόδειξη:

Η απεικόνιση φ: $\left\{ \begin{array}{l} \mathbb{Z} \longrightarrow K \\ n \longmapsto n \cdot 1_K \end{array} \right\}$ είναι ομομορφισμός δακτυλίων. (άσκηση)

Ο $Ker\phi \trianglelefteq \mathbb{Z}$.

Ο $\mathbb{Z}$ είναι περιοχή κύριων ιδεωδών .

Ξεχωρίζουμε δύο περιπτώσεις:

1. $Ker\phi = 0$, δηλαδή [Αν $n \cdot 1_K = 0 \Rightarrow n = 0$] $\Rightarrow chK = 0$
2. $Ker\phi \neq 0$

Το ιδεώδες $Ker\phi$ παράγεται από τον ελάχιστο φυσικό n τ.ω. $n \cdot 1_K = 0$.

Αν ο n ήταν σύνθετος, έστω $n = n_1 \cdot n_2 (n_1 > 1, n_2 > 1)$ τότε θα είχαμε $n_1 \cdot 1_K \neq 0_K$ και $n_2 \cdot 1_K \neq 0_K$.

Αλλά τότε $(n_1 \cdot n_2) \cdot 1_K = (n_1 \cdot 1_K)(n_2 \cdot 1_K) \neq 0$, άτοπο

$\Rightarrow Ker\phi =< p >, p \in \mathbb{P}$ ο ελάχιστος φυσικός με την ιδιότητα $p \cdot 1_K = 0_K$.

Δηλαδή $chK = p \in \mathbb{P}$.

Τώρα αν $chK = 0$,όλα τα στοιχεία του R της μορφής $n \cdot 1_K / n \in \mathbb{Z}$ είναι μεταξύ τους διαφορετικά. $\Rightarrow$ η φ: $\left\{ \begin{array}{l} \mathbb{Z} \longrightarrow K \\ n \longmapsto n \cdot 1_K \end{array} \right\}$ είναι μονομορφισμός δακτυλίων.

$\Rightarrow \mathbb{Z} \leq K$, οπότε $\mathbb{Q} = Quot(\mathbb{Z}) \leq K$. Αν $chK = p$, τότε η απεικόνιση

$\phi : \mathbb{F}_p = [n] \to n \cdot 1_K \in K$ είναι ομομορφισμός (μονομορφισμός) σωμάτων. $\Rightarrow \mathbb{F}_p \leq K$

Μία χαρακτηριστική ιδιότητα όταν $chK = p \in \mathbb{P}$.

Η ταυτότητα του «άσχετου» $(a+b)^p = a^p + b^p$ (ισχύει και για δυνάμεις του p).

2.2 Ο δακτύλιος των πολυωνύμων

Στην παράγραφο αυτή R θα είναι μια ακέραια περιοχή και K ένα σώμα.

$R[X] := \{f(x)/f = \text{πολυώνυμο με συντελεστές στο } R\}$

$\oplus$ πρόσθεση πολυωνύμων

$\odot$ πολλαπλασιασμός πολυωνύμων

$(R[X], \oplus, \odot)$

Μάλιστα $R \leq R[X]$.

Τώρα, έστω $R = K$ σώμα.

Αλγόριθμος της διαίρεσης

Αν $f(X), g(X) \in K[X]$ και $g \neq 0 \Rightarrow \exists\,!\; q(X), r(X) \in K[X]$ τ.ω. $f = g \cdot q + r$ και $r = 0$ ή $deg(r) < deg(g), \Rightarrow (K[X] = \text{Ευκλείδεια περιοχή}) \Rightarrow (K[X] = \text{περιοχή μονοσήμαντης ανάλυσης})$.

Συνέπειες:

1. $(a \in K)$ Το a ρίζα του $f(X) \in K[X] \Leftrightarrow g(X) := X - a | f(X)$.
   Απόδειξη:
   $[a \text{ ρίζα του } f(X)] \Leftrightarrow [f(a) = 0] \Leftrightarrow [r = f(a) - (a - a)q = 0] \Leftrightarrow g(X)|f(X)$

2. Το $f(X)$ έχει το πολύ $deg\ f(X)-$ ρίζες στο Κ.
   (Διαιρώ κάθε φορά με $X - a$ και a ρίζα και χρησιμοποιώ την μονοσήμαντη ανάλυση)

Ορισμός:

Ένα $f(X) \in K[X]$ θα λέγεται ανάγωγο όταν δεν αναλύεται σε γινόμενο δύο πολυωνύμων $g(X), h(X) \in K[X]$ με $deg(g(X)) \geq 1,\ deg(h(X)) \geq 1$.

$K[X]$ περιοχή μονοσήμαντης ανάλυσης $\Rightarrow$ [Κάθε $f(X) \in K[X]$ αναλύεται μονοσήμαντα σε γινόμενο αναγώγων πολυωνύμων].

Όμως πότε ένα πολυώνυμο $f(X) \in K[X]$ είναι ανάγωγο;

Πρόταση:

Αν ο $a = \frac{b}{c} \in \mathbb{Q},\ b, c \in \mathbb{Z},\ c \neq 0\ \ \text{ΜΚΔ}(b, c) = 1$ είναι ρίζα του πολυωνύμου $f(X) = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0 \in \mathbb{Z}[X]$ τότε $b|a_0$ και $c|a_m$

Παράδειγμα:

Το $f(X) = x^3 - 3X - 1 \in \mathbb{Z}[X]$ δεν έχει ρίζα στο $\mathbb{Q}[X]$, αφού αν a ρίζα του $f(X)$ τότε $a = \frac{b}{c},\ c \neq 0,\ (b, c) = 1 \Rightarrow b|a_0 = -1 \Rightarrow b = \pm 1$ και $c|a_m = 1 \Rightarrow c = \pm 1 \Rightarrow a = \pm 1$ και $f(\pm 1) \neq 0$.
Τώρα αυτό συνδυαζόμενο με το γεγονός ότι $deg\ f(X) = 3 \leq 3 \Rightarrow f(X)$ ανάγωγο στον $\mathbb{Q}[X]$.

Πρόταση: (Λήμμα του Gauss)

Αν το $f(X) \in \mathbb{Z}[X]$ αναλύεται σε γινόμενο μη-τετριμμένων πολυωνύμων στο $\mathbb{Q}[X]$, τότε αναλύεται σε γινόμενο μη-τετριμμένων πολυωνύμων στο $\mathbb{Z}[X]$.
Ιδιαίτερα: Αν το $f(X)$ μονικό, τότε κάθε μονικός παράγοντας του $f(X)$ στον $\mathbb{Q}[X]$ ανήκει στον $\mathbb{Z}[X]$.

Πρόταση: (Κριτήριο Eisenstein)

$f(X) = a_m X^m + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$. Υποθέτουμε ότι $\exists\, p \in \mathbb{P}$ τ.ω.

- $p \nmid a_m$
- $p|a_{m-1},\ a_{m-2},\ a_1,\ a_0$
- $p^2 \nmid a_0$

Τότε το $f(X)$-ανάγωγο στο $\mathbb{Q}[X]$

Παρατήρηση:

Συχνά το πολυώνυμο έχει τέτοια μορφή που δεν είναι δυνατόν να εφαρμοστεί το κριτήριο *Eisenstein*, αλλά αυτό επιτυγχάνεται μετά από τη χρήση κάποιου «τρίκ».

Παράδειγμα:

Έστω $f(X) = 2X^5 - 4X^4 + 8X^3 + 14X^2 + 7 \in \mathbb{Z}[X]$.

Το πολυώνυμο αυτό είναι ανάγωγο $/_{\mathbb{Q}}$.

Πράγματι, αν δεν ήταν ανάγωγο και παραγοντοποιείται, ας πούμε, σε ένα γινόμενο δυο πολυωνύμων $f = g \cdot h$ με $deg\ g(X) = 2$ και $deg\ h(X) = 3$.

Τότε και το $X^5 f(\frac{1}{X}) = (X^2 g(\frac{1}{x}))(X^3 h(\frac{1}{X}))$ δεν είναι ανάγωγο ($Eisenstein$ για $p = 2$).

Συνεπώς και το αρχικό.

Παράδειγμα: (Ιδιαίτερα σημαντικό)

Το $f(X) = X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1 \in \mathbb{Z}[X]$ είναι ανάγωγο στο $\mathbb{Q}[X]$

Ένα ακόμη κριτήριο αναγωγισιμότητας

Αν $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ και $p \in \mathbb{P},\ p \nmid a_n$.

Θεωρούμε το πολυώνυμο $\bar{f}(X) = \bar{a}_0 + \bar{a}_1 X + \cdots + \bar{a}_n X^n \in \mathbb{Z}_p[X]$.

Αν $f = g \cdot h$ με $deg(g),\ deg(h) < deg(f)$ και $deg(g) + deg(h) = deg(f)$, τότε $\bar{f} = \bar{g} \cdot \bar{h}$.

Αν καταφέρουμε να αποδείξουμε ότι ($\bar{f}$ ανάγωγο στο $\mathbb{Z}_p[X]$), τότε θα έχουμε ($f =$ ανάγωγο στο $\mathbb{Z}$).

Ο έλεγχος αναγωγισιμότητας στον $\mathbb{Z}_p$ είναι πιο εύκολος του $\mathbb{Z}$.

Παράδειγμα:

Να αποδείξετε ότι το $f(X) = 7X^4 + 10X^3 - 2X^2 + 4X - 5 \in \mathbb{Z}[X]$ είναι ανάγωγο στον $\mathbb{Q}[X]$.

Απόδειξη:

Για $p = 3 \Rightarrow \bar{f}(X) = X^4 + X^3 + X^2 + X + 1 \in \mathbb{Z}_3[X]$.

Στο $\mathbb{Z}_3$ τα στοιχεία είναι $0, 1, -1$ και $1 + 1 = -1$, $\left\{ \begin{array}{l} \bar{f}(0) = 1 \neq 0 \\ \bar{f}(1) = -1 \neq 0 \\ \bar{f}(-1) = 1 \neq 0 \end{array} \right\}$

Άρα το $\bar{f}(X)$ δεν έχει γραμμικό παράγοντα στο $\mathbb{Z}_3[X]$.

Τώρα, ελέγχουμε την περίπτωση $X^4 + X^3 + X^2 + X + 1 = (X^2 + aX + b)(X^2 + cX + d)$

$$\Rightarrow \left\{ \begin{array}{l} a+c=1 \\ bd=1 \end{array} \right\} \text{ και } \left\{ \begin{array}{l} a+ac+d=1 \\ ad+bc=1 \end{array} \right\}$$

Από $bd=1 \Rightarrow$ (i) $b=d=1$ ή (ii) $b=d=-1$

Αν ισχύει η $(i) \Rightarrow ac=-1 \Rightarrow [a=+1 \text{ και } c=-1]$ ή $[a=-1 \text{ και } c=+1]$

Και στις δύο περιπτώσεις $a+c=0$, άτοπο, αφού $a+c=1$.

Αν ισχύει η $(ii) \Rightarrow ac=0$.

Αν $a=0 \Rightarrow c=1$ και συνεπώς $1=ad+bc=b$, άτοπο.

Ανάλογα, αν $c=0 \Rightarrow a=1$, οπότε $1=ad+bc=d$, άτοπο.

$\Rightarrow \bar{g}(X)$ ανάγωγο στον $\mathbb{Z}_3[X]$

$\Rightarrow g(X)$ ανάγωγο στον $\mathbb{Q}[X]$.

Παρατήρηση:

Αν $f(X) \in \mathbb{Z}[X]$ και $f(X)$ όχι ανάγωγο στο $\mathbb{Q}[X]$

$\Rightarrow$ $f(X)$ όχι ανάγωγο στο $\mathbb{Z}[X]$

$\Rightarrow (\tilde{f}(X)$ όχι ανάγωγο στο $\mathbb{F}_p[X]$ $\forall p \in \mathbb{P})$

Αν $\tilde{f}(X)$ όχι ανάγωγο στον $\mathbb{F}_p[X]$ για κάποιο πρώτο p, τότε αυτό δεν σημαίνει τίποτε !.

Ίσως για κάποιο άλλο πρώτο να είναι ανάγωγο.

Είναι όμως δυνατόν, το $\tilde{f}(X)$ να μην είναι ανάγωγο $\forall p \in \mathbb{P}$ και όμως το $f(X)$ να είναι ανάγωγο στο $\mathbb{Q}(X)$.

π.χ. Θα δούμε ότι αυτό ισχύει για το $f(X)=X^4+1$

Κεφάλαιο 3

ΕΠΕΚΤΑΣΕΙΣ ΣΩΜΑΤΩΝ

3.1 Βαθμός Επέκτασης

Αν $(K, +, \cdot)$ σώμα, υπόσωμα του $(L, +, \cdot)$ θα λέμε ότι το L είναι μία επέκταση του K.

Συμβολισμός: $\mathbf{L}/_{\mathbf{K}}$ (επέκταση σωμάτων)

Γενικότερα αν $\phi : K \hookrightarrow L$ μονομορφισμός σωμάτων, ταυτίζουμε πρότυπα με εικόνες και έχουμε $K \cong \phi(K) \leq L$.

Αν $L/_K$ και $M/_L$ επεκτάσεις σωμάτων, συχνά γράφουμε $M/_{L/_K}$.

Αν $L/_K$ επέκταση σωμάτων, τότε το L μπορεί να θεωρηθεί σαν K-διανυσματικός χώρος.

Παραδείγματα:

$\mathbb{Q}(\sqrt{2})/_{\mathbb{Q}}$, $\mathbb{R}/_{\mathbb{Q}}$, $\mathbb{C}/_{\mathbb{R}}$, $\mathbb{C}/_{\mathbb{Q}}$.

Ορισμός:

Έστω $L/_K$ επέκταση σωμάτων.

Βαθμός επέκτασης $L/_K$ θα λέγεται η διάσταση του K-διανυσματικού χώρου L.

Συμβολισμός: $[\mathbf{L} : \mathbf{K}] = \mathbf{dim_K L}$

Η επέκταση θα λέγεται πεπερασμένη όταν $[L : K] < \infty$.

Αλλιώς θα λέγεται άπειρη επέκταση.

Παράδειγμα (1):

Το $\mathbb{Q}$ είναι αριθμήσιμο.

Άρα και κάθε πεπερασμένη επέκταση του είναι σύνολο αριθμήσιμο.

Όμως, το R είναι υπεραριθμήσιμο.

Συνεπώς, η επέκταση ${}^{\mathbb{R}}/_{\mathbb{Q}}$ είναι άπειρη.

Παράδειγμα (2):

Η επέκταση ${}^{\mathbb{C}}/_{\mathbb{R}}$ είναι πεπερασμένη αφού μία βάση αυτής είναι το σύνολο $\mathfrak{B} := \{1, i\}$.

Επομένως ο βαθμός επέκτασης είναι δύο. $[\mathbb{C} : \mathbb{R}] = 2$.

Πρόταση 1η:

Έστω ότι ${}^{L}/_{K}$ επέκταση σωμάτων.

Ισχύει $[L : K] = 1 \Leftrightarrow L = K$

Απόδειξη:

" $\Leftarrow$ " Έστω $L = K$.

Το $\{1\}$ είναι μια βάση της ${}^{L}/_{K}$, αφού κάθε $a \in L = K$, γράφεται $a = a \cdot 1 \Rightarrow [L : K] = 1$.

" $\Rightarrow$ " Έστω $[L : K] = 1$ και $a,\ a \in L,\ a \neq 0$ μία βάση της επέκτασης ${}^{L}/_{K}$.

Επομένως το $1 \in L$, γράφεται $1 = b \cdot a\ (b \in K)\ (b \neq 0)$. Συνεπώς $a = \frac{1}{b} \in K$.

Για κάθε $c \in L$ υπάρχει $d \in K$ τ.ω. $c = da = d \cdot \frac{1}{b} = \frac{d}{b}\ \in K$.

Επομένως, $L \subseteq K$.

Αλλά και $K \subseteq L \Rightarrow L = K$

Πρόταση 2η:

Έστω ότι ${}^{L}/_{K}$ και ${}^{M}/_{L}$ επεκτάσεις σωμάτων.

Ισχύει: $[M : K] = [M : L] \cdot [L : K]$.

Σημείωση:

Η ισότητα έχει το ακόλουθο περιεχόμενο για άπειρες επεκτάσεις.

«Αν ${}^{L}/_{K}$ είναι άπειρη επέκταση είτε ${}^{M}/_{L}$ άπειρη επέκταση, τότε και η ${}^{M}/_{K}$ είναι άπειρη επέκταση».

Απόδειξη:

Έστω $r := [M : K] < \infty$ και $s := [L : K] < \infty$.

Αν $a_1, a_2, ..., a_r$ μία L-βάση του M και $b_1, b_2, ..., b_s$ μία K-βάση του L, τότε το σύνολο $A := \{a_i b_j \ / i = 1, 2, ..., r \text{ και } j = 1, 2, ..., s\}$ είναι μια K-βάση του M.

Πράγματι,

1. Το σύνολο A είναι K-γραμμικά ανεξάρτητο σύνολο του M.
   Έστω ότι $\sum_{i=1}^{r}\sum_{j=1}^{s} \lambda_{i,j} a_i b_j = 0 \ / \ \lambda_{i,j} \in K$
   $\Rightarrow \sum_{i=1}^{r}(\sum_{j=1}^{s} \lambda_{i,j} b_j) a_i = 0$
   Το σύνολο $\{a_i \ / \ i = 1, 2, ..., r\}$ είναι L-γραμμικά ανεξάρτητο σύνολο του M.
   $\Rightarrow \sum_{j=1}^{s} \lambda_{i,j} b_j = 0 \ \ (i = 1, 2, 3, ..., r)$.
   Το σύνολο $\{b_j \ / \ j = 1, 2, ..., s\}$ είναι K-γραμμικά ανεξάρτητο σύνολο του M.
   Συνεπώς, $\lambda_{i,j} = 0 \ \ \forall i = 1, 2, ..., r$ και $\forall j = 1, 2, ..., s$

2. Το A παράγει το σώμα M ως προς K.
   Πράγματι, αν $x \in M \Rightarrow x = \sum_{i=1}^{r} \lambda_i a_i \ \ \lambda_i \in L, \ \ \forall i = 1, 2, ..., r \ \ a_i \in L \ \ \forall i = 1, 2, ..., r$
   Συνεπώς $\exists \ \ \mu_{i,j} \in K$ τ.ω. $\lambda_i = \sum_{j=1}^{s} \mu_{i,j} b_j$
   Άρα, το $x = \sum_{i=1}^{r}\sum_{j=1}^{s} \mu_{i,j}(a_i b_j)$.
   Συνεπώς $[M : K] = r \cdot s = [M : L][L : K]$.
   Αν τώρα ${}^{L}/_{K}$ άπειρη, τότε και ${}^{M}/_{K}$ άπειρη επέκταση.
   Αν πάλι ${}^{M}/_{L}$ άπειρη, τότε και ${}^{M}/_{K}$ άπειρη.

Πόρισμα:

Αν $K_1, K_2, ..., K_n$ σώματα και ${}^{K_{i+1}}/_{K_i}$ επέκταση σωμάτων για κάθε $i = 1, 2, ..., n-1$, τότε $[K_n : K_1] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_3 : K_2][K_2 : K_1]$.

Απόδειξη:

Επαγωγικά (άσκηση)

3.2 Επισύναψη

Έστω $^L/_K$ επέκταση σωμάτων και $S \subseteq L$.

Προφανώς $K \cup S \subseteq L$.

Επιπλέον, αν M_1, M_2 υποσώματα του L τ.ω. $K \cup S \subseteq M_1$ και $K \cup S \subseteq M_2$, τότε και $K \cup S \subseteq M_1 \cap M_2$.

Έστω $K(S)$ η τομή όλων των υποσωμάτων του L, που περιέχουν το $K \cup S$.

Ορισμός:

Το σώμα $K(S)$ θα λέγεται το υπόσωμα του L που παράγεται από το σώμα K και το σύνολο S.

Συμβολισμός: Αν το S είναι πεπερασμένο, έστω $S = \{a_1, a_2, ..., a_n\}$ τότε γράφουμε $K(a_1, a_2, ..., a_n)$ αντί $K(\{a_1, a_2, ..., a_n\})$.

Επιθυμούμε να έχουμε μια πιο βολική έκφραση για το σώμα αυτό.

Πρόταση 3η:

Το $K(S)$ συμπίπτει με τι σύνολο E όλων των στοιχείων του L τα οποία εκφράζονται σαν πηλίκα γραμμικών συνδυασμών πεπερασμένων γινομένων στοιχείων του S.

Απόδειξη:

Έστω $P :=$ το σύνολο όλων των γραμμικών συνδυασμών πεπερασμένων γινομένων του S.

Αν $p, q \in P$, τότε $p \pm q$ και $p \cdot q \ \in P$.

Επομένως, αν $x = \frac{p}{q}$ και $y = \frac{r}{s} \in E$ με $p, q, r, s \in P$ $(q, s \neq 0)$,

τότε $x - y = \frac{ps-qr}{qs} \in E$ και, αν $y \neq 0$, $\frac{x}{y} = \frac{ps}{qr} \in E$.

Συνεπώς E υπόσωμα του L το οποίο περιέχει και το K και το S, δηλαδή $K(S) \leq E$.

Τώρα, κάθε υπόσωμα του L που περιέχει και τα K και S περιέχει και όλα τα πεπερασμένα γινόμενα στοιχείων του S και όλους τους γραμμικούς συνδυασμούς αυτών των γινομένων και όλα τα πηλίκα τέτοιων συνδυασμών.

Επομένως περιέχει και το E, δηλαδή $E \leq K(S)$.

Τελικά, $E = K(S)$.

Ειδικά, αν $S = \{a\}$ με $a \in K$, τότε $K(S) = K(a) = K$.

Αν, πάλι $S = \{a\}$ και $a \in L \setminus K$, τότε γραμμικοί συνδυασμοί πεπερασμένων γινομένων του a, σχηματίζουν πολυώνυμα του a και τα πηλίκα όλων αυτών δίνουν όλα τα πηλίκα πολυωνύμων του a.

Δηλαδή, $K(a) = \{\frac{f(a)}{g(a)} \ / \ f(X), g(X) \in K[X] \text{ και } g(a) \neq 0\}$.

Ορισμός:

Αν ${}^{L}/_{K}$ επέκταση σωμάτων, κάθε επέκταση της μορφής ${}^{K(a)}/_{K}$ για $a \in L$ θα λέγεται απλή επέκταση του K.

Παρατήρηση: Στην περίπτωση που το S είναι πεπερασμένο, έστω $S = \{a_1, a_2, ..., a_n\}$ το σώμα $K(a_1, a_2, ..., a_n) =$

$\left\{ \frac{f(a_1,a_2,...,a_n)}{g(a_1,a_2,...,a_n)} \ / \ f(a_1, a_2, ..., a_n), g(a_1, a_2, ..., a_n) \in K[X] \text{ και } g(a_1, a_2, ..., a_n) \neq 0 \right\}$

Αν K σώμα, ο δακτύλιος $R = K[X]$ είναι Ευκλείδεια περιοχή, συνεπώς (και) περιοχή κύριων ιδεωδών και άρα (και) περιοχή μονοσήμαντης ανάλυσης.

Το σώμα πηλίκων της ακέραιας περιοχής R είναι το

$K(X) = \left\{ \frac{f(X)}{g(X)} \ / \ f(X), g(X) \in K[X], \ g(X) \neq 0 \right\}$

και λέγεται σώμα των ρητών συναρτήσεων (μίας μεταβλητής) με συντελεστές από το σώμα K.

Πρόταση 4η:

Αν ${}^{L}/_{K}$ επέκταση σωμάτων και $a \in L$, τότε ισχύει ακριβώς μία από τις ακόλουθες δύο περιπτώσεις:

1. $K(a) \cong K(X)$
2. Υπάρχει μοναδικά ορισμένο μονικό, ανάγωγο πολυώνυμο $m(X) \in K[X]$ τ.ω. για κάθε $f(X) \in K[X]$ να ισχύουν:

   (α′) $f(a) = 0 \Leftrightarrow m(X) \mid f(X)$

   (β′) $K(a) \cong K[a] = \{f(a) \mid f(X) \in K[X]\}$ και

   (γ′) $[K(a) : K] = deg\ m(X)$

Απόδειξη:

1. Υποθέτουμε ότι δεν υπάρχει $f(X) \in K[X],\ f \neq 0$ τ.ω. $f(a) = 0$

   (Σημείωση: Αν $a \in K$, τότε το a είναι ρίζα του $f(X) = X - a\ \in K[X]$. Συνεπώς $a \notin K$)

   Η απεικόνιση $\phi := \left\{ \begin{array}{l} K(X) \longrightarrow K(a) \\ {}^{f}/_{g}\ (g \neq 0) \longmapsto \frac{f(a)}{g(a)} \end{array} \right\}$ είναι ομομορφισμός σωμάτων.

   (άσκηση)

   Είναι επιμορφισμός, αφού αν $\frac{f(a)}{g(a)} \in K(a)$, τότε υπάρχουν $f(X), g(X) \in K[X]$ τ.ω. $\phi(\frac{f}{g}) = \frac{f(a)}{g(a)}$.

   [Το $g(a) \neq 0\ \Rightarrow g(X) \neq 0$. Αφού υποθ. $g(a) = 0 \Leftrightarrow g = 0$]

   Τέλος είναι μονομορφισμός σωμάτων.

   Πράγματι, αν $\phi(\frac{f}{g}) = \phi(\frac{f'}{g'})$, με $f, f', g, g' \in K[X]$ και $g, g' \neq 0$, τότε θα έχουμε $f(a)g'(a) - f'(a)g(a) = 0$, στο $L\ \Rightarrow [f \cdot g' - f' \cdot g](a) = 0$

   Άμεση συνέπεια της υπόθεσης είναι ότι $f \cdot g' - f' \cdot g = 0$, στον $K[X]$, δηλαδή $\frac{f}{g} = \frac{f'}{g'}$.

   Συνεπώς η φ είναι ισομορφισμός σωμάτων, $K(X) \cong K(a)$.

2. Υποθέτουμε τώρα ότι υπάρχει $f(X) \in K[X],\ f \neq 0$ τ.ω. $f(a) = 0$.

   Από όλα αυτά τα πολυώνυμα υπάρχει κάποιο που έχει τον ελάχιστο βαθμό.

   Διαιρούμε τους συντελεστές του με τον συντελεστή της μεγαλύτερης δύναμης του X και έτσι το πολυώνυμο που προκύπτει είναι μονικό.

   Ας το ονομάσουμε $m(X)$.

   Επομένως το $m(X)$ είναι μονικό, έχει ρίζα του τον $a \in L$ και είναι ελάχιστου βαθμού.

   Θα αποδείξουμε ότι πληρεί τις ιδιότητες (α), (β) και (γ).

   (α′) " $\Rightarrow$ " Έστω $f(X) \in K[X]$ τ.ω. $f(a) = 0$.

   Ο δακτύλιος $K[X]$ είναι Ευκλείδεια περιοχή.

   Συνεπώς, υπάρχουν μοναδικά ορισμένα πολυώνυμα $q(X), r(X) \in K[X]$ τ.ω. $f(X) = m(X)q(X) + r(X)$ και $r(X) = 0$ ή $deg\ r(X) < deg\ m(X)$.

   Επομένως, $f(a) = m(a)q(a) + r(a) \Rightarrow r(a) = 0$ (αφού $f(a) = 0$ και $m(a) = 0$).

   Αν ίσχυε $r(X) \neq 0$, θα είχαμε $r(a) = 0$ και $deg\ r(X) < deg\ m(X)$, άτοπο.

   (Το $m(X)$ είναι πολυώνυμο ελαχίστου βαθμού με αυτή την ιδιότητα)

   Από τα παραπάνω προκύπτει ότι $r(X) = 0$, δηλαδή $f(X) = m(X)q(X)$ και

συνεπώς, $m(X) \mid f(X)$.

" $\Leftarrow$ " Αν $m(X) \mid_{K[X]} f(X) \Rightarrow \exists\, q(X) \in K[X]$ τ.ω. $f(X) = m(X)q(X)$, οπότε $f(a) = m(a)q(a) = 0 \cdot q(a) = 0$.

Το $m(X)$ είναι μοναδικό με τις παραπάνω ιδιότητες:

(Αν υπήρχε κάποιο άλλο $m'(X) \in K[X]$ τ.ω. $m'(X)$ μονικό, $m(a) = 0$ και $m'(X)$ επίσης ελαχίστου βαθμού, τότε $m(X) \mid_{K[X]} m'(X)$ και $m'(X) \mid_{K[X]} m(X)$ και επειδή και τα δυο είναι μονικά θα είχαμε $m(X) = m'(X)$.)

Τέλος το $m(X)$ είναι ανάγωγο στον $K[X]$.

Πράγματι, αν $m(X) = p(X) \cdot q(X)$ με $p(X), q(X) \in K[X]$ και $deg\ p(X) < m,\ \ deg\ q(X) < m$ θα έχουμε $m(a) = p(a) \cdot q(a) = 0 \Rightarrow [p(a) = 0$ είτε $q(a) = 0]$, άτοπο

(β′) Έστω $\frac{f(a)}{g(a)} \in K(a),\ g(a) \neq 0$

$g(a) \neq 0 \overset{(a)}{\Longrightarrow} m(X) \nmid g(X)$

$m(X)$ ανάγωγο $\Rightarrow$ ΜΚΔ $(m(X),\ g(X)) = 1$

Επομένως υπάρχουν $\alpha(x),\ b(X) \in K[X]$ τ.ω. $\alpha(X)g(X) + b(X)m(X) = 1$

Άρα, $\alpha(a)g(a) + b(a)m(a) = 1,\ \ (m(a) = 0) \Rightarrow \alpha(a)g(a) = 1$, δηλαδή

$\frac{f(a)}{g(a)} = f(a)\alpha(a) \in K[a]$

Από τα παραπάνω συμπεραίνουμε ότι $K(a) \leq K[a]$.

Πάντοτε ισχύει: $K[a] \leq K(a)$.

Τελικά προκύπτει ότι $K(a) = K[a]$.

(γ′) Έστω ότι $deg\ m(X) = m$ και $p(a) \in K[a] = K(a)$, με $p(X) \in K[X]$.

Σύμφωνα με τον ¨αλγόριθμο με διαίρεση¨, υπάρχουν μοναδικά ορισμένα πολυώνυμα $q(X), r(X) \in K[X]$ τ.ω. $p(X) = m(X) \cdot q(X) + r(X)$ και $r(X) = 0$ ή $deg\ r(X) < deg\ m(X) = n$

Συνεπώς, $p(a) = m(a)q(a) + r(a) = r(a),\ \ (m(a) = 0)$

Άρα $K(a) = \left\{\ r(a)\ /\ r(X) \in K[X], deg\ r(X) < n\ \right\}$

Επομένως το σύνολο $A := \left\{\ 1, a, a^2, ..., a^{n-1}\ \right\}$ παράγει τον K-διανυσματικό χώρο $K(a)$.

Είναι και γραμμικά ανεξάρτητο σύνολο.

(Αν ήταν γραμμικά εξαρτημένο θα υπήρχαν $\lambda_i \in K\ \ (i = 0, 1, ..., n-1)$ όχι όλα

μηδέν τ.ω. $\lambda_0 + \lambda_1 a + \lambda_2 a^2 + \cdots + \lambda_{n-1} a^{n-1} = 0$, οπότε το a θα ήταν ρίζα του πολυωνύμου $g(X) = \lambda_0 + \lambda_1 X + \lambda_2 X^2 + \cdots + \lambda_{n-1} X^{n-1}$, $g(X) \neq 0$ και $deg(g(x)) < deg\ m(X) = n$, άτοπο.)

Επομένως, $[K(a) : K] = n = deg\ m(X)$.

Παρατηρήσεις:

1. Μια βάση της επέκτασης ${}^{K(a)}/_{K}$ είναι το σύνολο $\mathfrak{B} := \{1, a, a^2, ..., a^{n-1}\}$
2. Αν $[K(a) : K] = n$ και $g(X) \in K[X]$, $g(X)$ μονικό τ.ω. $deg\ g(X) = n$ και $g(a) = 0$, τότε $g(X) = m(X)$.

Συμβολισμός: Το πολυώνυμο $m(X)$ θα το συμβολίζουμε και $\mathbf{Irr(a, K)}$.

Ερώτημα:

Πως θα γράψουμε το τυχαίο στοιχείο $\frac{f(a)}{g(a)}$ του $K(a)$ $(a = \text{αλγ}/K)$ σαν γραμμικό συνδυασμό των στοιχείων της βάσης $\mathfrak{B} = \{1, a, a^2, ..., a^{n-1}\}$;

Υπάρχουν δύο τρόποι:

1ος τρόπος: Εφαρμόζουμε τη διαδικασία της απόδειξης της πρότασης 4 (απόδειξη του (b)).

2ος τρόπος: Πιο απλός.

Παράδειγμα $1o$**:**

Έστω $f(X) = X^2 + X + 1 \in \mathbb{Q}[X]$

Το $f(X)$ είναι ανάγωγο στον $\mathbb{Q}[X]$ $(f(\pm 1) \neq 0)$. Έστω $a \in \mathbb{C}$, ρίζα του $f(X)$.

Ο βαθμός της επέκτασης $[\mathbb{Q}(a) : \mathbb{Q}] = 2$ και μία βάση αυτής $\mathfrak{B} := \{1, a\}$.

Από την $a^2 + a + 1 = 0$, έπεται ότι $a^2 - 1 = -a - 2 \neq 0$.

Θα εκφράσουμε το $\frac{a^2+1}{a^2-1} \in \mathbb{Q}(a)$ στη μορφή $a + ba$ / $a, b \in \mathbb{Q}$.

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

Διαιρούμε το πολυώνυμο $X^2 + X + 1$ με το $X + 2$,

$X^2 + X + 1 = (X + 2)(X - 1) + 3 \Rightarrow 0 = a^2 + a + 1 = (a + 2)(a - 1) + 3$

Συνεπώς, $(a + 2)(a - 1) = -3 \Rightarrow \frac{1}{a+2} = -\frac{1}{3}(a - 1)$ και τελικά έχουμε:

$\frac{a^2+1}{a^2-1} = 1 + \frac{2}{3}(a - 1) = \frac{1}{3} + \frac{2}{3}a$.

Παράδειγμα $2o$**:**

Στην πρώτη ματιά το σώμα $\mathbb{Q}(\sqrt{2},\sqrt{3})$ δεν φαίνεται να είναι απλή επέκταση του $\mathbb{Q}$.
Όμως μπορούμε να αποδείξουμε ότι $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ και ότι
$Irr(\sqrt{2}+\sqrt{3},\mathbb{Q}) = X^4 - 10X^2 + 1 \in \mathbb{Q}[X]$.

Ορισμός:

Έστω ${}^{L}/_{K}$ επέκταση σωμάτων και $a \in L$.
Το a θα λέγεται αλγεβρικό υπέρ το K $:\Leftrightarrow (\exists\ f(X) \in K[X]$ τ.ω. $f(a) = 0)$
Στην ειδική περίπτωση ${}^{\mathbb{C}}/_{\mathbb{Q}}$ αν ο $a \in \mathbb{C}$ είναι αλγεβρικός υπέρ το K, τότε ο a λέγεται *αλγεβρικός αριθμός*.
Αν ο $a \in L$ δεν είναι αλγεβρικός υπέρ το K, τότε θα λέγεται *υπερβατικός υπέρ το* K.
Είναι προφανές ότι σ΄ αυτή την περίπτωση $K(a) \cong K(X)$.
Στην ειδική περίπτωση της επέκτασης ${}^{\mathbb{C}}/_{\mathbb{Q}}$, αν ο $a \in \mathbb{C}$ είναι υπερβατικός υπέρ το $\mathbb{Q}$, θα λέγεται *υπερβατικός αριθμός*.
Γνωρίζουμε ότι υπάρχουν υπερβατικοί αριθμοί, π.χ. $e, \pi, 2^{\sqrt{2}}, ...$

3.3 Αλγεβρικές επεκτάσεις

Ορισμός:

${}^{L}/_{K}$ επέκταση σωμάτων.

Η επέκταση ${}^{L}/_{K}$ θα λέγεται **αλγεβρική**, όταν (κάθε $a \in L$ είναι αλγεβρικό ${}/_{K}$).

Αν η επέκταση ${}^{L}/_{K}$ δεν είναι αλγεβρική, τότε θα λέγεται **υπερβατική**.

(Επομένως, η ${}^{L}/_{K}$ θα είναι υπερβατική $\Leftrightarrow$ [$\exists a \in L$ τ.ω. $a =$ υπερβατικό ως προς το K.)

Πρόταση $5^{η}$:

Κάθε πεπερασμένη επέκταση σωμάτων ${}^{L}/_{K}$ είναι αλγεβρική.

Απόδειξη:

Έστω $[L : K] = n < \infty$ και a οποιοδήποτε στοιχείο του L.

(Αν $a \in K$, τότε το a αλγεβρικό υπέρ το K)

Αν $a \in {}^{L}/_{K}$ θεωρούμε το σύνολο $A := \{1, a, a^2, ..., a^n\}$.

Το σύνολο αυτό είναι γραμμικά εξαρτημένο.

Συνεπώς υπάρχουν $\lambda_0, \lambda_1, ..., \lambda_n \in K$, όχι όλα μηδέν, τ.ω. $\lambda_0 + \lambda_1 a, ..., \lambda_n a^n = 0$

δηλαδή, υπάρχει ένα πολυώνυμο $f(X) = \lambda_0 + \lambda_1 X, ..., \lambda_n X^n \neq 0$ τ.ω. $f(a) = 0$.

Άρα, το a είναι αλγεβρικό υπέρ το K και συνεπώς και η επέκταση ${}^{L}/_{K}$ είναι αλγεβρική.

Παρατηρήσεις:

1. Αν ${}^{L}/_{K}$ επέκταση σωμάτων και $a \in L$, a υπερβατικό υπέρ το K, τότε η επέκταση ${}^{K(a)}/_{K}$ είναι άπειρη.

   (Αν ήταν πεπερασμένη, θα ήταν αλγεβρική. Συνεπώς και το a θα ήταν αλγεβρικό υπέρ το K, άτοπο.)

2. Υπάρχουν επεκτάσεις σωμάτων ${}^{L}/_{K}$ άπειρου βαθμού οι οποίες είναι αλγεβρικές.

   Παραδείγματα θα αναφέρουμε στη συνέχεια.

Παραδείγματα:

- Αλγεβρικών επεκτάσεων:
  ${}^{\mathbb{Q}(\sqrt{5})}/_{\mathbb{Q}}$, ${}^{\mathbb{Q}(\sqrt[3]{2})}/_{\mathbb{Q}}$, ${}^{\mathbb{Q}(\pi)}/_{\mathbb{Q}(\pi^2)}$
- Υπερβατικών επεκτάσεων:
  ${}^{\mathbb{Q}(\pi)}/_{\mathbb{Q}}$, ${}^{\mathbb{Q}(e)}/_{\mathbb{Q}}$, ${}^{K(X)}/_{K}$

Πρόταση 6η:

Έστω ${}^{M}/_{L}$ και ${}^{L}/_{K}$ επεκτάσεις σωμάτων και $a \in M$ αλγεβρικό υπέρ το K. Το a θα είναι αλγεβρικό και υπέρ το L.

Απόδειξη:

Το $a \in M$ είναι αλγεβρικό υπέρ το K

$\Rightarrow (\ \exists\ f(X) \in K[X],\ f \neq 0$ τ.ω. $f(a) = 0)$

Επειδή $K \leq L$, έπεται ότι $K[X] \leq L[X]$.

Συνεπώς, το $f(X) \in L[X],\ f \neq 0$ και $f(a) = 0$, δηλαδή, το a αλγεβρικό υπέρ το L.

Παρατήρηση:

Βέβαια το $Irr(a, K)$ δεν είναι (εν γένει) το ίδιο με το $Irr(a, L)$.

Μάλιστα $Irr(a, L) \mid Irr(a, K)$.

Πρόταση 7η:

Έστω ${}^{L}/_{K}$ επέκταση και $a, \beta \in L$. Ισχύει $K(a, \beta) = (K(a))(\beta)$.

Απόδειξη:

Το σώμα $K(a, \beta)$ περιέχει τα K και a. Επομένως θα περιέχει και το $K(a)$.

Όμως περιέχει και το β. Συνεπώς θα περιέχει και το $(K(a))(\beta) \leq K(a, \beta)$.

(Αφού $(K(a))(\beta)$ το ελάχιστο σώμα που περιέχει το σώμα $K(a)$ και το στοιχείο β.)

Επίσης το $K(a)(\beta)$ περιέχει το K και τα a, β. Συνεπώς $K(a, \beta) \leq (K(a))(\beta)$.

(Αφού το $K(a, \beta)$ το ελάχιστο υπόσωμα μ΄ αυτή την ιδιότητα.)

Τελικά, έχουμε ότι $K(a, \beta) = (K(a))(b)$.

Πρόταση 8η:

Έστω ${}^{L}/_{K}$ επέκταση σωμάτων.

Το σύνολο $A(L) := \{a \in L \ / \ a$ είναι αλγεβρικό υπέρ το $k\}$ είναι υπόσωμα του L.

Απόδειξη:

Έστωσαν, $a, \beta \in A(L)$. Το $a - \beta \in K(a, \beta) \overset{\Pi\rho.7}{=\!=} (K(a))(b) \overset{\Pi\rho.3}{=\!=} (K[a])[b]$.

Το $\beta \in A(L) \Rightarrow [\beta$ αλγεβρικό υπέρ το $K] \overset{\Pi\rho.6}{\Longrightarrow}$ [β αλγεβρικό υπέρ το $K[a]$]

$\overset{\Pi\rho.3}{\Longrightarrow}$ η επέκταση $(K[a])[\beta]$ / $K[a]$ είναι πεπερασμένη.

Επίσης, $a \in A(L) \overset{\Pi\rho.5}{\Longrightarrow}$ η επέκταση ${}^{K[a]}/_{K}$ είναι πεπερασμένη.

Συνεπώς (Πρόταση 1) και η ${}^{K(a,\beta)}/_{K}$ είναι πεπερασμένη $\overset{\Pi\rho.5}{\Longrightarrow}$ ${}^{K(a,\beta)}/_{K}$ αλγεβρική, δηλαδή $a - \beta \in A(L)$.

Επίσης, αν $a, \beta \in A(L),\ \beta \neq 0$, τότε (όπως παραπάνω) η ${}^{K(a,\beta)}/_{K}$ είναι αλγεβρική και (αφού $K(a, \beta)$ σώμα) έπεται ότι $\frac{a}{\beta} \in K(a, \beta)$, δηλαδή $\frac{a}{\beta} \in A(L) \ \Rightarrow \ A(L)$ σώμα.

Παρατηρήσεις:

(1^{η}) $K \leq A(L)$

(2^{η}) $A(L) = L \ \Leftrightarrow \ {}^{L}/_{K}$ αλγεβρική

Ορισμός:

Το σώμα $A(L)$ θα λέγεται **αλγεβρική θήκη** του K στο L.

Ειδική περίπτωση:

Αν $K = \mathbb{Q}$ και $L = \mathbb{C}$ τότε το υπόσωμα του $\mathbb{C}$, $\widetilde{\mathbb{Q}} := A(\mathbb{C})$ θα λέγεται **σώμα των αλγεβρικών αριθμών**

Πρόταση 9η:

Η επέκταση ${}^{\widetilde{\mathbb{Q}}}/_{\mathbb{Q}}$ είναι άπειρη αλγεβρική.

Απόδειξη:

Έστω ότι είναι πεπερασμένη, $[\widetilde{\mathbb{Q}} : \mathbb{Q}] = m \ < \infty$.

Θεωρούμε το πολυώνυμο $f(X) := X^{m+1} - 2 \ \in \mathbb{Q}[X]$.

Το $f(X)$ είναι ανάγωγο υπέρ το $\mathbb{Q}$ (Κριτήριο του $Eisenstein$ για $p = 2$).

Αν a ρίζα του $f(X)$ π.χ. $a = \sqrt[m+1]{2}$ (Εδώ δεχόμαστε προσωρινά την ύπαρξη ρίζας σε επέκταση του $K = \mathbb{Q}$) τότε $[\mathbb{Q}(a) : \mathbb{Q}] = m + 1$.
Όμως τότε θα έχουμε $\mathbb{Q} \leq \mathbb{Q}(a) \leq \widetilde{\mathbb{Q}}$, δηλαδή το $(m+1)|m$, άτοπο.

Πρόταση 10η:

Έστω ${}^{L}/_{K}$ επέκταση σωμάτων, $a_1, a_2, \cdots, a_n \in L$ αλγεβρικά ως προς το K και $m_i(X) = Irr(a_i, K),\ i = 1, 2, \cdots, n$.
Ισχύει: $[K(a_1, a_2, \cdots, a_n) : K] = \prod_{i=1}^{n} deg\ m_i(X)$.
Απόδειξη:
Έχουμε ήδη αποδείξει ότι $K(a, \beta) = (K(a))(\beta)$.
Επαγωγικά αποδεικνύεται ότι $K(a_1, a_2, \cdots, a_n) = (K(a_1, a_2, \cdots, a_{n-1}))(a_n)$.
Τώρα εφαρμόζουμε επαγωγή ως προς n.
Για $n = 1$, ισχύει $[K(a_1) : K] = deg\ m_1(X)$, ισχύει.
Υποθέτουμε ότι $[K(a_1, a_2, \cdots, a_n) : K] \leq \prod_{i=1}^{n} deg\ m_i(X)$
$[K(a_1, a_2, \cdots, a_{n-1}, a_n) : K(a_1, a_2, \cdots, a_{n-1})] =$
$[(K(a_1, a_2, \cdots, a_{n-1}))(a_n) : K(a_1, a_2, \cdots, a_{n-1})] =$
$deg\ Irr(a_n, K(a_1, a_2, \cdots, a_{n-1}))$
Τώρα, $m_n(a_n) = 0 \overset{\Pi\rho.3}{\Longrightarrow} Irr(a_n, K(a_1, a_2, \cdots, a_{n-1})) \mid m_n(X) \Rightarrow$
$deg\ Irr(a_n, K(a_1, a_2, \cdots, a_{n-1})) \leq deg\ m_n(X)$
Επομένως, $[K(a_1, a_2, \cdots, a_n) : K] = [K(a_1, a_2, \cdots, a_n) : K(a_1, a_2, \cdots, a_{n-1})]$.
$[K(a_1, a_2, \cdots, a_{n-1}) : K] \leq deg\ m_n(X) \cdot \prod_{i=1}^{n-1} deg\ m_i(X)$

Παρατήρηση:

Δεν ισχύει πάντα η ισότητα. π.χ. $[\mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{15}) : \mathbb{Q}] = 4$

Πρόταση 11η:

Η επέκταση σωμάτων ${}^{L}/_{K}$ είναι πεπερασμένη $\Leftrightarrow$ (όταν $\exists a_1, a_2, \cdots, a_n \in L$ αλγεβρικά υπέρ το K τ.ω. $L = K(a_1, a_2, \cdots, a_n)$)
Απόδειξη:
'$\Leftarrow$' Η κατεύθυνση προκύπτει αμέσως από την πρόταση 10.

'$\Rightarrow$' Η $^{L}/_{K}$ είναι πεπερασμένη.

Επομένως (Πρόταση 5) είναι αλγεβρική.

Συνεπώς όλα τα στοιχεία του L είναι αλγεβρικά ως προς το K.

Έστω $[L:K] = n \ < \infty$ και $\mathscr{B} = \{a_1, a_2, \cdots, a_n\}$ μία βάση της επέκτασης $^{L}/_{K}$.

Το $L = Ka_1 + Ka_2 + \cdots + Ka_n \ \leq \ K(a_1, a_2, \cdots, a_n) \overset{a_i \text{ αλγ./}K}{=\!=\!=} K[a_1, a_2, \cdots, a_n]$.

Όμως $K \leq L$ και $a_1, a_2, \cdots, a_n \ \in L \ \Rightarrow K(a_1, a_2, \cdots, a_n) \leq L$.

Τελικά έχουμε $L = K(a_1, a_2, \cdots, a_n)$

Παρατήρηση:

Αν $^{L}/_{K}$ επέκταση σωμάτων, $a_1, a_2, \cdots, a_n$ αλγεβρικά υπέρ το K τότε, Πρόταση 11, η $^{L}/_{K}$ είναι πεπερασμένη και συνεπώς αλγεβρική.

Πρόταση 12η:

Έστω ότι $K \leq L \leq M$. Αν $a \in M$ είναι αλγεβρικό υπέρ το L και η επέκταση $^{L}/_{K}$ είναι αλγεβρική, τότε το a είναι αλγεβρικό υπέρ το K.

Απόδειξη:

Το a είναι αλγεβρικό υπέρ το L.

Συνεπώς, $\exists \ f(X) = a_0 + a_1X + \cdots + a_nX^n \ \in L[X]$ τ.ω. $f(a) = 0$.

Τα $\ a_0, a_1, \cdots, a_n \ \in L$ και είναι αλγεβρικά υπέρ το K.

Άμεση συνέπεια της πρότασης 11 είναι ότι η επέκταση $^{L_0}/_{K}$ όπου $L_0 := K(a_0, a_1, \cdots, a_n)$, είναι πεπερασμένη.

Όμως $f(X) \in L_0[X]$, δηλαδή το a είναι αλγεβρικό υπέρ το L_0.

Συνεπώς, η επέκταση $^{L_0(a)}/_{L_0}$ είναι πεπερασμένη.

Τελικά $[L_0(a) : K] = [L_0(a) : L_0][L_0 : K] < \infty \Rightarrow$ Το a είναι αλγεβρικό υπέρ το K.

Παρατήρηση:

Άμεση συνέπεια της πρότασης 12, είναι: Αν $^{M}/_{L}$ και $^{L}/_{K}$ είναι αλγεβρικές επεκτάσεις, τότε και η επέκταση $^{M}/_{K}$ είναι αλγεβρική.

Ερώτηση:

Ισχύει και το αντίστροφο;

Προφανώς ναι.

Αν ${}^{M}/_{K}$ αλγεβρική, και $a \in M \Rightarrow$ (a αλγεβρικό $|_L$), συνεπώς ${}^{M}/_{L}$ αλγεβρική.

Αν $a \in L,\ L \leq M \Rightarrow a \in M$ και συνεπώς (a αλγεβρικό $|_K$), δηλαδή ${}^{L}/_{K}$ αλγεβρική.

Πρόταση 13η:

Έστω σαν ${}^{L_1}/_{K}$, ${}^{L_2}/_{K}$ επεκτάσεις σωμάτων και $L_1 \leq N,\ L_2 \leq N$ (υποσώματα του σώματος N).

Αν $[L_1 : K] = m,\ [L_2 : K] = n$ και $[L_1L_2 : K] = t$ (εδώ $m,\ n,\ t\ \in \mathbb{N} \cup \{\infty\}$), τότε ισχύουν τα εξής:

(α) (t είναι πεπερασμένος) $\Leftrightarrow$ (m και n είναι πεπερασμένοι)

(β) Αν ισχύει η (α), τότε $m|t,\ n|t$ και $t \leq m \cdot n$

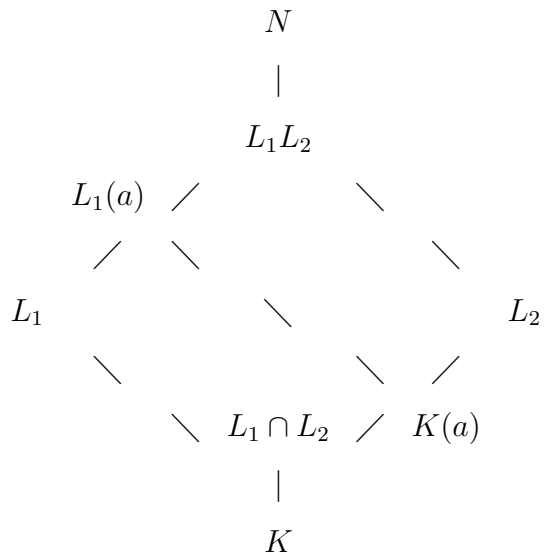
(γ) Αν ΜΚΔ$(m,\ n) = 1$, τότε $t = m \cdot n$

Σημείωση:

L_1L_2 είναι ελάχιστο, υπόσωμα του N που περιέχει τα L_1, L_2.

(δηλαδή η τομή όλων των σωμάτων, υποσωμάτων του N που περιέχουν το L_1 και L_2).

Απόδειξη:



Αν t, πεπερασμένο $\Rightarrow$ $[L_1L_2 : K] < \infty$ οπότε και m και n πεπερασμένοι, (από πρόταση 2)
(αφού $m = [L_1 : K]\ |t$ και $n = [L_2 : K]\ |t$).
Έστω τώρα ότι ${}^{L_1}/_K$ και ${}^{L_2}/_K$ πεπερασμένες $m, n \in \mathbb{N}$.
Θα αποδείξουμε ότι και ο t είναι πεπερασμένος και μάλιστα το πολύ $m \cdot n$.
Θα εφαρμόσουμε επαγωγή ως προς n.
Αν $n = 1 \Rightarrow L_2 = K$ οπότε $L_1L_2 = L_1K = L_1$ και συνεπώς
$t = [L_1L_2 : K] = [L_1 : K] = m < \infty$, ισχύει.
Υποθέτουμε ότι $n > 1$ και , έστω, $a \in L_2 \setminus K$.
Αν $r := [K(a) : K]$ και $s = [L_1(a) : L_1]$ $(a \in L_2 \Rightarrow a \in L_1L_2,\ L_1 \leq L_1(a) \leq L_1L_2)$.
Προφανώς ισχύει $s \leq r$.
(αφού το $Irr(a, L_1)|Irr(a, K)$)
$[L_1(a) : K] = [L_1(a) : L_1][L_1 : K] = m \cdot s$
Επίσης, $[L_1(a) : K] = [L_1(a) : K(a)][K(a) : K] \Rightarrow m \cdot s = [L_1(a) : K(a)] \cdot r \Rightarrow [L_1(a) : K(a)] = \frac{m \cdot s}{r}$
Τέλος, $[L_2 : K(a)] = \frac{[L_2:K]}{[K(1):K]} = \frac{n}{r}$
Εφαρμόζουμε την υπόθεση της μαθηματικής επαγωγής για τις επεκτάσεις ${}^{L_1(a)}/_{K(a)}$ και ${}^{L_2(a)}/_{K(a)}$ και έχουμε $[L_1(a) : K(a)] \leq \frac{m \cdot s}{r} \cdot \frac{n}{r} \overset{(\frac{s}{r} \leq 1)}{\leq} \frac{m \cdot n}{r}$
Όμως, $a \in L_2$, άρα $L_1(a)L_2 = L_1L_2$.
Συνεπώς, $[L_1L_2 : K] = [L_1L_2 : K(a)][K(a) : K] \leq \frac{m \cdot n}{r} \cdot r = m \cdot n$.
Έχουμε αποδείξει τα (α) και (β).
Το (γ): Από τις σχέσεις $m|t,\ n|t$ και την υπόθεση $\text{ΜΚΔ}(m, n) = 1 \Rightarrow m \cdot n|t$
Έχουμε όμως αποδείξει ότι και $t \leq m \cdot n$.
Άρα, αν $\text{ΜΚΔ}(m, n) = 1$, τότε $t = m \cdot n$.

3.4 Πολυώνυμα και επεκτάσεις

Υπενθύμηση:

Έστω R μια ακέραια περιοχή και $I \trianglelefteq R$ και $r \in R$.

Το σύνολο $r + I = \{r + x \mid x \in I\}$ θα λέγεται **κλάση υπολοίπων** του r $(modulo\ I)$.

Ισχύει $r_1 + I = r_2 + I \ \Leftrightarrow \ r_1 - r_2 \in I$.

Έστω τώρα το σύνολο ${}^R/_I = \{r + I \mid r \in I\}$. Ορίζουμε, **πρόσθεση** και **πολλαπλασιασμό** στο ${}^R/_I$

$(r_1 + I) \oplus (r_2 + I) = (r_1 + r_2) + I$

$(r_1 + I) \odot (r_2 + I) = (r_1 \cdot r_2) + I$

Αποδεικνύεται ότι οι πράξεις είναι ανεξάρτητες των αντιπροσώπων και ότι το $({}^R/_I, \oplus, \odot)$ αποτελεί δακτύλιο.

Λέγεται **δακτύλιος πηλίκων** $(modulo\ I)$.

Η απεικόνιση $\phi_I : R \to {}^R/_I$ είναι επιμορφισμός δακτυλίων και $ker\phi_I = I$.

Η απεικόνιση αυτή λέγεται **φυσικός ομομορφισμός** του R στον ${}^R/_I$

Ορισμός:

Το ιδεώδες $P \trianglelefteq R$ θα λέγεται **πρώτο** $\Leftrightarrow$ [Αν $a \cdot \beta \in P \ \Rightarrow \ a \in P \vee b \in P$].

Ισχύει: $[P \trianglelefteq R,\ P$ πρώτο$] \ \Leftrightarrow$ [ο δακτύλιος πηλίκων ${}^R/_P$ είναι ακέραια περιοχή].

Ορισμός:

Ένα ιδεώδες $\mathfrak{m} \trianglelefteq R$ θα λέγεται **maximal** $\Leftrightarrow$ όταν $\mathfrak{m} \neq R$ και αν $A \trianglelefteq R$ τ.ω.

$\mathfrak{m} \leq A \leq R \ \Rightarrow \ A = \mathfrak{m} \vee A = R$.

Ισχύουν: (1) Κάθε $maximal$ ιδεώδες του R είναι και πρώτο.

(Το αντίστροφο , εν γένει, δεν ισχύει.)

Ορισμός:

R ακέραια περιοχή.
Το $p \in R$ θα λέγεται **ανάγωγο** όταν

(ι) $p \notin E(R)$ και $p \neq 0$

(ιι) Το p δεν αναλύεται σε γινόμενο, μη-τετριμμένων, παραγόντων.

(Αν $p = a \cdot \beta,\ a, \beta \in R \ \Rightarrow$ ένα π.χ. $a \in E(R)$ και το άλλο πρώτο)
Αν τώρα R περιοχή κύριων ιδεωδών τότε οι παρακάτω προτάσεις είναι μεταξύ τους ισοδύναμες:

(ι) Το $p \in R$ είναι ανάγωγο.

(ιι) Το $< p > \trianglelefteq R$ είναι $maximal$.

(ιι) ${}^{R}/_{<p>}$ είναι σώμα.

¨Βίοι Παράλληλοι'		
	$\mathbb{Z}$	$K[X]$
1	Ευκλείδεια περιοχή (ως προς το μέτρο $\|.\|$) $\Downarrow$	Ευκλείδεια περιοχή (ως προς το μέτρο $deg\ f$) $\Downarrow$
2	Περιοχή κύριων ιδεωδών	Περιοχή κύριων ιδεωδών
3	Ανάγωγα στοιχεία (πρώτοι αριθμοί)	Ανάγωγα στοιχεία (ανάγωγα πολυώνυμα)
4	$maximal$ ιδεώδη $< p > \|p \in \mathbb{P}$	$maximal$ ιδεώδη $< f(X) > \|f(X)$ ανάγωγο του $K[X]$
5	σώματα ${}^{\mathbb{Z}}/_{<p>} = {}^{\mathbb{Z}}/_{p\mathbb{Z}}$	σώματα ${}^{K[X]}/_{<f(X)>}$ $f(X)$ ανάγωγο

Μέχρι τώρα είδαμε ότι σε κάθε απλή, αλγεβρική επέκταση ${}^{K(a)}/_{K}$ αντιστοιχεί ένα πολυώνυμο του $K[X]$, το $Irr(a, K)$.

Αντιστρέφουμε το ερώτημα:

Δίνεται ένα μονικό και ανάγωγο πολυώνυμο $m(X) \in K[X]$.

Μπορούμε να «κατασκευάσουμε» μια επέκταση του K τ.ω. να περιέχει ένα στοιχείο, έστω a, τ.ω. $Irr(a, K) = m(X)$??? - (δηλαδή μια ρίζα του $m(X)$).

Έστω $L := \frac{K[X]}{<m(X)>}$.

Το $m(X)$ ανάγωγο και $K[X]$ περιοχή κύριων ιδεωδών, άρα L σώμα.

Η απεικόνιση $\begin{array}{l} \phi : K \hookrightarrow L \\ a \longmapsto a+ < m(X) > \end{array}$ είναι ομομορφισμός σωμάτων.

Πράγματι

$\phi(a + \beta) = (a + \beta)+ < m(X) = (a+ < m(X) >) + (\beta+ < m(X) >) = \phi(a) + \phi(\beta)$.

Επίσης $\phi(a \cdot \beta) = a \cdot \beta+ < m(X) >= (a+ < m(X) >) \cdot (\beta+ < m(X) >) = \phi(a) + \phi(\beta)$.

Τέλος $\phi(1_K) = 1_K+ < m(X) >= 1_L$, η φ επίσης είναι μονομορφισμός.

(Αλλιώς αν $a+ < m(x) >= \beta+ < m(X) > \Rightarrow\ a - \beta \in < m(X) > \Rightarrow\ m(X)|a - \beta\ \Rightarrow$ $a - \beta = 0\ \Rightarrow\ a = \beta$)

Ταυτίζουμε το K με την εικόνα του $\phi(K)$ και έχουμε:

Το L είναι επέκταση του K.

Έστω τώρα $a := X+ < m(X) > \in L$.

Αν $f(X) = a_0 + a_1X + \cdots + a_nX^n\ \in K[X]$, ένα πολυώνυμο του $K[X]$, τότε έχουμε:

$$\begin{aligned} f(a) &= a_0 + a_1a + a_2a^2 + \cdots + a_na^n \\ &= a_0 + a_1(X+ < m(X) >) + \cdots + a_n(X+ < m(X) >)^n \\ &= a_0 + a_1X + \cdots + a_nX+ < m(X) > \\ &= f(X)+ < m(X) > \end{aligned}$$

Επομένως

$$\begin{aligned} & f(a) = 0+ < m(X) > \\ \Leftrightarrow\ & f(X)+ < m(X) >= 0+ < m(X) > \\ \Leftrightarrow\ & f(X) \in < m(X) > \\ \Leftrightarrow\ & m(X)|f(X) \end{aligned}$$

Επομένως

$m(X) = Irr(a, K) \quad (a = X+ < m(X) >)$

Επομένως:

Πρόταση 14η:

Αν K σώμα και $m(X)$ ένα μονικό, ανάγωγο πολυώνυμο του $K[X]$ τότε το σώμα
$L = \frac{K[X]}{<m(x)>} \cong K(a)\ \ (= K[a])\ \ ((a := X+ < m(x)\ ) \text{ και } Irr(a, K) = m(X)$

Πρόταση 15η:

Αν K σώμα και $f(X) \in K[X]$ ανάγωγο.
Αν L_1 και L_2 είναι δύο σώματα, επεκτάσεις του K τ.ω. το $a_1 \in L_1$ και $a_2 \in L_2$ δύο ρίζες του $f(X)$, τότε υπάρχει ένας K-ισομορφισμός σωμάτων $\psi : K(a_1) \longrightarrow K(a_2)$ τ.ω.
$\psi(a_1) = a_2$

Σημείωση:

K-ισομορφισμός σημαίνει $\psi(a) = a\ \forall a \in K$.

(Απόδειξη, αργότερα)

Παραδείγματα:

1. $K = \mathbb{R} \quad m(X) = X^2 + 1\ \in \mathbb{R}[X]$
   $L := \frac{K[X]}{<m(X)>} = \frac{\mathbb{R}[X]}{<(x^2+1)>}$
   Το $\alpha := X+ < (X^2 + 1) >$ είναι ρίζα του $X^2 + 1$ και μάλιστα το ανάγωγο του a υπέρ το $K = \mathbb{R}$.
   Επομένως, $\alpha^2 + 1 = 0\ \Rightarrow\ \alpha^2 = -1$
   $L = \mathbb{R}(\alpha)$ και $[\mathbb{R}(\alpha) : \mathbb{R}] = 2$
   Άρα $L = \{a + b\alpha\ /\ a, b \in \mathbb{R} \text{ και } \alpha^2 = -1\}$
   δηλαδή $L \cong \mathbb{C}$

2. $K = \mathbb{Q},\ \ m(X) = X^2 + 3\ \in \mathbb{Q}[X]$
   $L := \frac{\mathbb{Q}[X]}{(X^2+3)} \cong \mathbb{Q}(a),\ \ a^2 + 3 = 0\ \Rightarrow\ a = \pm\sqrt{-3}$, δηλαδή $\mathbb{Q}(\sqrt{-3}) \cong \frac{\mathbb{Q}[X]}{<X^2+3>}$

3. Το πολυώνυμο $f(X) = X^2 + X + 1\ \in \mathbb{F}_2[X]$, είναι ανάγωγο υπέρ το $\mathbb{F}_2$
   (αφού $deg\ f(X) = 2 \leq 3$ και $f(\pm 1) \neq 0$)

Το σώμα $L := \frac{\mathbb{F}_2[X]}{<f(X)>}$ έχει 4 στοιχεία.

Αυτά είναι: το $0+ < f(X) >$, το $1+ < f(X) >$, το $X+ < f(X) >$ και το $1+X+ < f(X) >$.

Τα γράφουμε σαν $0, 1, a, 1+a$ όπου $a^2+a+1=0$ και σχηματίζουμε τους πίνακες πρόσθεσης και πολλαπλασιασμού.

$+$	0	1	a	$1+a$
0	0	1	a	$1+a$
1	1	0	$1+a$	a
a	a	$1+a$	0	1
$1+a$	$1+a$	a	1	0

$\cdot$	1	a	$1+a$
1	1	a	$1+a$
a	a	$1+a$	1
$1+a$	$1+a$	1	a

3.5 Τα τρία άλυτα προβλήματα της αρχαιότητας

Στον $\mathbb{R}^2$ θεωρούμε ένα σύστημα συντεταγμένων και έστω $O(0,0)$ η αρχή τους.
Επιλέγουμε ένα σημείο I, διαφορετικό του O (με τον διαβήτη) σε έναν από τους δύο άξονες και θεωρούμε ότι αυτό έχει συντεταγμένες $(1,0)$.
Έστω τώρα B_0 ένα σύνολο σημείων του επιπέδου. Στο B_0 έχουμε δύο επιτρεπτές πράξεις:

(Πρ.1) [Χρήση κανόνα] Σε κάθε ζευγάρι σημείων του B_0, χαράσσω την ευθεία η οποία διέρχεται από αυτά.

(Πρ.2) [Χρήση διαβήτη] Γράφω κύκλο με κέντρο ένα σημείο του B_0 και ακτίνα όσο είναι η απόσταση του κέντρου από κάποιο άλλο σημείο του συνόλου B_0.

Ορισμός:

Κάθε σημείο του $\mathbb{R}^2$ το οποίο είναι τομή δύο τέτοιων ευθειών ή ευθείας και κύκλου ή δυο κύκλων θα λέγεται σημείο **κατασκευάσιμο από το B_0 σε ένα βήμα**.
Συμβολισμός:
Το σύνολο των σημείων αυτών θα το συμβολίζουμε $\mathbf{C(B_0)}$.
Έστω $B_1 := B_0 \cup C(B_0)$.
Εφαρμόζουμε την ίδια διαδικασία για το σύνολο B_1. Τα σημεία που θα κατασκευάσουμε θα τα λέμε: **Σημεία κατασκευάσιμα** από το B_0 **σε δύο βήματα** και το σύνολό τους θα το συμβολίζουμε $C(B_1)$.
Ορίζουμε το $B_2 := B_1 \cup C(B_1)$ και συνεχίζουμε ...
Το $B_n := B_{n-1} \cup C(B_{n-1})$ για $n = 1, 2, 3, \cdots$

Ορισμός:

Το $P \in \mathbb{R}^2$ θα λέγεται κατασκευάσιμο από το B_0, ακριβώς τότε όταν $P \in B_n$ για κάποιο $n \in \mathbb{N}$.

Παράδειγμα:

Έστω $B_0 = \{0, 1\}$.

Θέλουμε να κατασκευάσουμε το μέσον του ευθύγραμμου τμήματος OI.

Ακολουθούμε τα εξής βήματα:

1. Χαράσσουμε το ευθύγραμμο τμήμα OI.
2. Γράφουμε κύκλο κέντρου O και ακτίνας $R := |OI|$.
3. Γράφουμε κύκλο κέντρου I και ακτίνας R.
4. Οι δύο κύκλοι τέμνονται σε δύο σημεία, έστω P και Q. Επομένως το σύνολο $C(B_0) = \{P, Q\}$ και $B_1 = \{O, I, P, Q\}$.
5. Χαράσσουμε το ευθύγραμμο τμήμα PQ.
6. Έστω M το σημείο τομής των ευθυγράμμων τμημάτων OI και $PQ \ \Rightarrow \ C(B_1) = \{M\}$ και $B_2 = \{O, I, P, Q, M\}$.

Επομένως το M είναι κατασκευάσιμο από το $B_0 = \{O, I\}$.

Βασική Ιδέα: Η σύνδεση κάθε συνόλου B_i με ένα υπόσωμα του $\mathbb{R}$ που παράγεται από τις συντεταγμένες των σημείων του συνόλου B_i.

Επιστρέφουμε στο παράδειγμα:

Στο $B_0 = \{(0, 0), (1, 0)\}$ αντιστοιχεί το σώμα $K_0 := \mathbb{Q}$.

Η εξίσωση του πρώτου κύκλου είναι $X^2 + Y^2 = 1$ ενώ του δεύτερου $(X - 1)^2 + Y^2 = 1$.

Λύνουμε το σύστημα αυτών των δύο εξισώσεων.

Τα σημεία τομής των δύο κύκλων έχουν συντεταγμένες $P = (\frac{1}{2}, \frac{\sqrt{3}}{2})$ και $Q = (\frac{1}{2}, -\frac{\sqrt{3}}{2})$.

Επομένως $B_1 = \{(0, 0), (1, 0), (\frac{1}{2}, \frac{\sqrt{3}}{2}), (\frac{1}{2}, -\frac{\sqrt{3}}{2})\}$ και σ΄ αυτό αντιστοιχεί το σώμα $K_1 = \mathbb{Q}(\sqrt{3})$.

Το σημείο $M = (\frac{1}{2}, 0)$, δηλαδή $C(B_1) = \{(\frac{1}{2}, 0)\}$.

Άρα $B_2 = \{(0, 0), (1, 0), (\frac{1}{2}, \frac{\sqrt{3}}{2}), (\frac{1}{2}, -\frac{\sqrt{3}}{2}), (\frac{1}{2}, 0)\}$ και σ΄ αυτό αντιστοιχεί το σώμα $K_2 = \mathbb{Q}(\sqrt{3})$.

Ο βαθμός της επέκτασης $[K_2 : \mathbb{Q}] = 2$.

Πρόταση 16η:

Έστω ότι το P είναι κατασκευάσιμο από το σύνολο $B_0 = \{(0,0),(1,0)\}$.

(Συνεπώς το $P \in B_n$ για κάποιο $n \in \mathbb{N}$)

Αν K_n είναι το σώμα το οποίο παράγεται υπέρ το $\mathbb{Q}$ από το σύνολο B_n, $K_n = \mathbb{Q}(B_n)$, για $n = 0, 1, 2, \cdots$, τότε $[K_n : \mathbb{Q}] = 2^l,\ l \in \mathbb{N}$.

Απόδειξη:

$K_0 = \mathbb{Q}(B_0) = \mathbb{Q}$, άρα $[K_0 : \mathbb{Q}] = 1 = 2^0$.

Υποθέτουμε ότι $[K_{n-1} : \mathbb{Q}] = 2^k$ για κάποιο $k \geq 0$.

Θα αποδείξουμε ότι και $[K_n : K_{n-1}] =$ δύναμη του 2.

Τα επιπλέον σημεία του συνόλου B_n από το B_{n-1}, προκύπτουν από το B_{n-1} με τρεις τρόπους:

1ος τρόπος: Σαν τομή δύο ευθειών.

2ος τρόπος: Σαν τομή ευθείας και κύκλου.

3ος τρόπος: Σαν τομή δύο κύκλων.

1η περίπτωση: Έστω $A = (a_1, a_2),\ \ B(b_1, b_2)\ \ C = (c_1, c_2)$ και $D = (d_1, d_2)$ σημεία του $\mathbb{R}^2$ με συντεταγμένες στο σώμα K_{n-1}.

Εξίσωση ευθείας AB : $\ (y - b_2)(a_1 - b_1) = (x - b_1)(a_2 - b_2)$

Εξίσωση ευθείας CD : $\ (y - d_2)(c_1 - d_1) = (x - d_1)(c_2 - d_2)$

Οι συντελεστές του σημείου τομής υπολογίζονται από την λύση του συστήματος.

Εφαρμόζουμε ρητές πράξεις, τις τέσσερις πράξεις της αριθμητικής με στοιχεία από το σώμα K_{n-1}. Επομένως το σημείο τομής έχει συντεταγμένες στο K_{n-1}.

2η περίπτωση: Το σημείο τομής της ευθείας AB $(A = (a_2, a_2),\ B = (b_1, b_2))$ και κύκλου κέντρου $C(c_1, c_2)$ και ακτίνας $r = |PQ|$ όπου $P, Q \in B_{n-1}$, δηλαδή τα σημεία P, Q έχουν συντεταγμένες στο σώμα K_{n-1}.

Επομένως το σημείο τομής θα έχει συντεταγμένες τη λύση του συστήματος

$$\left\{ \begin{array}{l} (y - b_2)(a_1 - b_1) = (x - b_1)(a_2 - b_1) \\ (x - c_1)^2 + (y - c_2)^2 = r^2,\ \text{όπου } r \in K_{n-1} \end{array} \right\}$$

Λύνουμε την πρώτη εξίσωση ως προς y, συναρτήσει του x και αντικαθιστούμε στην δεύτερη. Προκύπτει εξίσωση $2^{ου}$ βαθμού ως προς x με συντελεστές από το σώμα K_{n-1}.

Η λύση περιέχει $\sqrt{\Delta}$, όπου Δ η διακρίνουσα της δευτεροβάθμιας εξίσωσης.

Επομένως οι συντεταγμένες της λύσης ανήκουν στο σώμα $K_{n-1}(\sqrt{\Delta})$.

(Παρατήρηση: (Η $\sqrt{\Delta} \in K_{n-1} \Leftrightarrow K_{n-1}(\sqrt{\Delta}) = K_{n-1}$))

3^{η} περίπτωση: Τα σημεία τομής δύο κύκλων κέντρων $A = (a_1, a_2),\ B = (b_1, b_2)$ και ακτίνων $r, s \in K_{n-1}$ αντιστοίχως.

Τα σημεία τομής θα έχουν συντεταγμένες τις λύσεις του συστήματος

$$\left\{ \begin{array}{l} (y - b_2)(a_1 - b_1) = (x - b_1)(a_2 - b_1) \\ (x - c_1)^2 + (y - c_2)^2 = r^2, \text{ όπου } r \in K_{n-1} \end{array} \right| r, s \in K_{n-1} \Bigg\}$$

Αφαιρούμε τις εξισώσεις κατά μέλη και έχουμε μια γραμμική και μια δευτεροβάθμια εξίσωση, οπότε το πρόβλημα ανάγεται στην 2^{η} περίπτωση.

Επομένως, τα καινούρια σημεία που εμφανίζονται στο σύνολο B_n έχουν συντεταγμένες που ανήκουν

- είτε στο σώμα K_{n-1}
- είτε σε μια τετραγωνική επέκταση $K_{n-1}(\sqrt{\Delta})/\Delta \in K_{n-1}$, αυτού.

Από τα παραπάνω συμπεραίνουμε ότι $K_n = K_{n-1}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \cdots, \sqrt{\Delta_l})$ και άρα $[K_n : K_{n-1}] =$ δύναμη του 2.

Παρατήρηση: Αργότερα θα αποδείξουμε την πρόταση. Αν $B_0 = \{O, I\}$ και $\mathbb{Q} = K_0 \leq K_1 \leq \cdots \leq K_n = L$ μια πεπερασμένη ακολουθία σωμάτων (υποσωμάτων του $\mathbb{R}$) τ.ω. $[K_i : K_{i-1}] = 2$ για $i = 1, 2, \cdots, n$ τότε κάθε σημείο με συντεταγμένες από το σώμα L είναι κατασκευάσιμο.

Άμεση συνέπεια αυτής θα είναι η:

Πρόταση Αν η $^{K}/_{\mathbb{Q}}$ είναι κανονική (η έννοια θα οριστεί αργότερα !) και $[K : \mathbb{Q}] = 2^m\ \ (m \geq 1)$, τότε κάθε σημείο (a_1, a_2) του K είναι κατασκευάσιμο.

Πάμε τώρα στα τρία «άλυτα» προβλήματα της Αρχαιότητας.

[I] Διπλασιασμός του κύβου

χ.β.τ.γ. υποθέτουμε ότι ο αρχικός κύβος έχει ακμή μήκους 1.
Θα πρέπει να επεκτείνουμε το $\mathbb{Q}$, σύμφωνα με τους κανόνες κατασκευής, σε ένα σώμα K τ.ω. $a \in K$ όπου $a^3 = 2$.
Όμως $f(X) = X^3 - 2 \in \mathbb{Q}[X]$, είναι ανάγωγο υπέρ το $\mathbb{Q}$ $(Eisenstein$ για $p = 2)$
Επομένως $[\mathbb{Q}(a) : \mathbb{Q}] = 3$.
Επειδή $\mathbb{Q} \leq \mathbb{Q}(a) \leq K$, $3|[K : \mathbb{Q}] \Rightarrow [K : \mathbb{Q}]$ όχι δύναμη του 2 $\Rightarrow$ η κατασκευή είναι αδύνατη.

Ιστορικό Σημείωμα:
(Διπλασιασμός του κύβου)
Υπάρχουν δύο εκδοχές:
1η εκδοχή: Ο Βασιλιάς Μίνωας δεν ήταν ευχαριστημένος με το μέγεθος του τάφου, που ήταν σε κυβική μορφή, του γυιού του Γλαύκου και έδωσε εντολή να κατασκευάσουν νέο διπλάσιου όγκου.
1η εκδοχή: Οι Αθηναίοι, προκειμένου να αντιμετωπίσουν μια επιδημία, έστειλαν αντιπροσωπεία στο ιερό της Δήλου και ζήτησαν συμβουλή. Το μαντείο τους προέτρεψε να διπλασιάσουν το μέγεθος του ναού του Απόλλωνα.
Από την δεύτερη εκδοχή λέγεται και «Δήλιο πρόβλημα».

[II] Τριχοτόμηση οποιασδήποτε δοθείσας γωνίας

Υποθέτουμε ότι μας δίνεται μια γωνία $\omega = 3\theta$.
Συνεπώς γνωρίζουμε το $cos\ \omega = cos\ 3\theta =: a$.
Γνωστός ο τύπος $cos\ 3\theta = 4cos^3\theta = 3cos\ \theta$.
Επομένως για να τριχοτομήσουμε την ω θα πρέπει να μπορέσουμε να κατασκευάσουμε την ϑ, δηλαδή να γνωρίζουμε-κατασκευάσουμε το $cos\ \theta$. Αυτό σημαίνει ότι θα πρέπει να μπορούμε να κατασκευάσουμε μια ρίζα, έστω a της κυβικής εξίσωσης $4X^3 - 3X - a = 0$

Παραδείγματα:

1. Έστω ότι $\hat{\omega} = \frac{\pi}{2} \Rightarrow 3\theta = \frac{\pi}{2}$ και $a := cos\ \frac{\pi}{2} = 0$.
   Επομένως, η εξίσωση γράφεται
   $4X^3 - 3X = 0 \Rightarrow X(4X^2 - 3) = 0 \Rightarrow [X = 0, X = \pm\frac{\sqrt{3}}{2}]$ $({}^{\mathbb{Q}(\sqrt{3})}/_{\mathbb{Q}})$ κανονική.
   Συνεπώς $[\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$, δηλαδή: Η τριχοτόμηση της γωνίας $\frac{\pi}{2}$ με κανόνα και διαβήτη είναι δυνατή.

2. Έστω τώρα $\hat{\omega} = \frac{\pi}{3} \Rightarrow a = cos\ \frac{\pi}{3} = \frac{1}{2}$ και $3\theta = \frac{\pi}{3}$. Το $cos\ \theta$ είναι μια ρίζα της εξίσωσης $4X^3 - 3X - \frac{1}{2} = 0 \Rightarrow 8X^3 - 6X - 1 = 0$.
   Το πολυώνυμο $f(X) = 8X^3 - 6X - 1 \in \mathbb{Q}[X]$ είναι ανάγωγο υπέρ το $\mathbb{Q}$.
   (Σημείωση: Αν $\frac{r}{s} \in \mathbb{Q}$ $(r, s) = 1$, ρίζα του $\Rightarrow r| - 1$ και
   $s|8 \Rightarrow \frac{r}{s} \in \{\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}\}$ και $f(\frac{r}{s}) \neq 0$ ή ισοδύναμα [$f(X)$ ανάγωγο $\Leftrightarrow$ $f(\frac{X}{2})$ ανάγωγο υπέρ το $\mathbb{Q}$].
   Αλλά $g(X) := f(\frac{X}{2}) = X^3 - 3X - 1$ και $g(\pm 1) \neq 0 \Rightarrow g(X)$ ανάγωγο, δηλαδή $f(X)$ ανάγωγο υπέρ το $\mathbb{Q}$)
   Αν λοιπόν a ρίζα του $f(X), a := cos\ \frac{\pi}{9}$, τότε $[\mathbb{Q}(a) : \mathbb{Q}] = 3$ και ,όπως παραπάνω, έπεται ότι ο a δεν είναι κατασκευάσιμος με κανόνα και διαβήτη, δηλαδή είναι αδύνατη με κανόνα και διαβήτη η τριχοτόμηση της γωνίας $\frac{\pi}{3}$.

[III] Ο τετραγωνισμός του κύκλου

Κύκλος ακτίνας 1 έχει εμβαδό π.
Τετράγωνο εμβαδού π, έχει μήκος πλευράς $\sqrt{\pi}$.
Αν ο π ήταν κατασκευάσιμος τότε και ο $\sqrt{\pi}$ θα ήταν κατασκευάσιμος, αφού
$[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}(\pi)] = 2$ (ή δες το παράδειγμα κατασκευής της $\sqrt{a}$)
Όμως ο π είναι υπερβατικός ($Lindemann1882$) (ένα από τα σημαντικότερα αποτελέσματα του $19^{ου}$ αιώνα !)
Συνεπώς, η επέκταση ${}^{\mathbb{Q}(\pi)}/_{\mathbb{Q}}$ είναι άπειρη.
Άρα, αφού $\mathbb{Q}(\pi) \leq \mathbb{Q}(\sqrt{\pi})$, και η ${}^{\mathbb{Q}(\sqrt{\pi})}/_{\mathbb{Q}}$ άπειρη.
Συνεπώς $\sqrt{\pi}$ όχι κατασκευάσιμος με κανόνα και διαβήτη.
Τελικά ο τετραγωνισμός του κύκλου είναι αδύνατος με κανόνα και διαβήτη.

3.6 Σώμα ανάλυσης (διάσπασης) ενός πολυωνύμου $\mathbf{f(X) \in K[X]}$

Στην παράγραφο αυτή θα αποδείξουμε ότι υπάρχει πάντοτε μια (τουλάχιστον) επέκταση L του K η οποία περιέχει όλες τις ρίζες του $f(X)$.

Έστω $f(X) = X^2 - 2 \ \in \mathbb{Q}[X]$.

Οι ρίζες του είναι, $x_1 = \sqrt{2}, x_2 = -\sqrt{2}$.

Το σώμα $\mathbb{Q}(\sqrt{2}) = \{a + \beta\sqrt{2}/a, b \ \in \mathbb{Q}\}$ περιέχει τη ρίζα $\sqrt{2}$, (για $a = 0, b = 1$!) αλλά και την $-\sqrt{2}$, δηλαδή περιέχει όλες τις ρίζες του $f(X)$.

Επιπλέον, αν K σώμα τ.ω. $\mathbb{Q} \leq K$ και $\sqrt{2} \in K$, τότε $\mathbb{Q}(\sqrt{2}) \leq K$ αφού το $\mathbb{Q}(\sqrt{2})$ είναι το ελάχιστο μ΄ αυτήν την ιδιότητα.

Έστω $g(X) = X^3 - 2 \in \mathbb{Q}[X]$.

Το $g(X)$ είναι ανάγωγο υπέρ το $\mathbb{Q}$.

Μια ρίζα αυτού είναι το $a := \sqrt[3]{2} \in \mathbb{R}$.

Το $g(X)$ έχει μια ρίζα (το a) στο σώμα $\mathbb{Q}(\sqrt[3]{2})$.

Το $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, μια βάση της επέκτασης ${}^{\mathbb{Q}(\sqrt[3]{2})}/_{\mathbb{Q}}$ είναι το σύνολο $\mathscr{B} = \{1, \sqrt[3]{2}, \sqrt[3]{4}\}$, δηλαδή $\mathbb{Q}(\sqrt[3]{2}) = \{a + \beta \ \sqrt[3]{2} + c \ \sqrt[3]{4} \ / \ a, b, c \in \mathbb{Q}\}$

Το $X^3 - 2 = X^3 - (\sqrt[3]{2})^3 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$

Το πολυώνυμο, όμως $X^2 + \sqrt[3]{2}X + \sqrt[3]{4} \ \in \mathbb{Q}(\sqrt[3]{2})[X]$ είναι ανάγωγο υπέρ το $\mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{R}$. (Η διακρίνουσα $\Delta = -3\sqrt[3]{4} < 0$, άρα ανάγωγο και στο $\mathbb{R}$)

Τώρα, αν X ρίζα του πολυωνύμου, $X^3 - (\sqrt[3]{2})^2 = 0 \ \Rightarrow \ X^3 = (\sqrt[3]{2})^3 \ \Rightarrow \ (\frac{X}{\sqrt[3]{2}})^3 = 1$, δηλαδή το $\frac{X}{\sqrt[3]{2}}$ ρίζα της εξίσωσης $Y^3 = 1$.

Οι ρίζες της $Y^n = 1$ λέγονται n-ρίζες της μονάδας.

Οι 3-ες ρίζες της μονάδας είναι:

$(Y - 1)(Y^2 + Y + 1) = 0 \ \Rightarrow \ y_1 = 1, \ y_{2,3} = \frac{-1 \pm \sqrt{-3}}{2} = \frac{-1 \pm i\sqrt{3}}{2}$

Επομένως το $X^3 - 2$, αναλύεται πλήρως σε σώμα $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$.

Ο βαθμός της επέκτασης $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}] = 6$.

Ορισμός:

Έστω $f(X) \in K[X], \ K$ σώμα και L επέκταση του K.

Το σώμα L θα λέγεται **σώμα ανάλυσης του f ως προς το K** όταν:

1. Το f αναλύεται πλήρως στο L.
2. Το L είναι το ελάχιστο σώμα μ΄ αυτή την ιδιότητα, δηλαδή το $f(X)$ δεν αναλύεται πλήρως σε κανένα γνήσιο υπόσωμα του L.

Παρατήρηση:

Αν $deg\ f(X) = n$ και $a_1, a_2, \cdots, a_n$ οι ρίζες αυτού τότε το $L = K(a_1, a_2, \cdots, a_n)$ είναι σώμα ανάλυσης αυτού.

Πρόταση 17η:

Έστω $f(X) \in K[X]$, (K σώμα) και $deg\ f(X) = n$.
Υπάρχει πάντοτε ένα σώμα ανάλυσης L του $f(X)$ υπέρ το K τ.ω. $[L : K] \leq n!$
Απόδειξη:
Το $f(X)$ αναλύεται (μονοσήμαντα) σε γινόμενο ανάγωγων παραγόντων.
Έστω $g(X)$ ένας από αυτούς. (Αν το $f(X)$ είναι ανάγωγο τότε $g(X) = f(X)$)
Στο σώμα $E_1 := \frac{K[X]}{<g(X)>}$, ανήκει μία ρίζα του $g(X)$, συνεπώς και του $f(X)$, η
$a_1 := X + g(X)$ και μάλιστα, $E_1 = K(a_1)$ και $g(X) = Irr(a_1, K)$ (Πρόταση 14)
Ο βαθμός, $[E_1 : K] = deg\ (g(X)) \leq n$ και $g(X) = (X - a)g_1(X)$ στον $E_1[X]$.
Υπόθεση της μαθηματικής επαγωγής:
Για κάθε $r = 1, 2, \cdots, n-1$ κατασκευάζουμε μία επέκταση ${}^{E_r}/_{K}$ τ.ω. το $f(X)$ να έχει στον $E_r[X]$ τουλάχιστον r γραμμικούς παράγοντες και $[E_r : K] \leq n(n-1)\cdots(n-r+1)$
Επομένως το $f(X)$ στον $E_r[X]$, γράφεται: $f(X) = (X - a_1)\cdots(X - a_r)f_r(X)$ και
$deg\ f_r(X) = n - r$
Εντελώς ανάλογα με την αρχή της απόδειξης, κατασκευάζουμε επέκταση ${}^{E_{r+1}}/_{E_r}$ τ.ω. το $f_r(X)$ να έχει στον $E_{r+1}[X]$ τουλάχιστον ένα γραμμικό παράγοντα $(X - a_{r+1})$ και
$[E_{r+1} : E_r] \leq n - r$, δηλαδή
$[E_{r+1} : E_r] \leq n - r \ \Rightarrow\ [E_{r+1} : K] = [E_{r+1} : E_r][E_r : K] \leq n(n-1)\cdots(n-r)$
Επομένως, υπάρχει ένα σώμα E_n τ.ω. το $f(X)$ αναλύεται πλήρως στον $E_n[X]$ και
$[E_n : K] \leq n!$

Αν τώρα $L := K(a_1, a_2, \cdots, a_n) \leq E_n$ τότε L είναι ένα σώμα ανάλυσης του $f(X)$ υπέρ το K.

Επειδή είναι δυνατόν να βρεθούν διάφορες επεκτάσεις του K στις οποίες το δοθέν πολυώνυμο $f(X) \in K[X]$ έχει μια ρίζα, μπορούν να βρεθούν και διάφορες επεκτάσεις του K που να αποτελούν σώμα αναλύσεως του πολυωνύμου $f(X) \in K[X]$.
Για παράδειγμα τα σώματα $\mathbb{C}$ και $\frac{\mathbb{R}[X]}{<(X^2+1)>}$ είναι σώματα αναλύσεως του
$f(X) = X^2 + 1 \in \mathbb{R}[X]$.
Όμως, έχουμε ήδη αναφέρει, ότι ισχύει $\frac{\mathbb{R}[X]}{<(X^2-1)>} \cong \mathbb{C}$.
Αυτό ισχύει γενικά, δηλαδή ισχύει:

Πρόταση 18η:

Αν $f(X) \in K[X]$ και L και L' σώματα ανάλυσης του $f(X)$ υπέρ το K, τότε και $L \cong L'$.

Συνεπώς, στο μέλλον θα μπορούμε να αναφερόμαστε στο σώμα ανάλυσης του πολυωνύμου $f(X)$ υπέρ το K
Για την απόδειξη θα γενικεύσουμε την Πρόταση 15.

Πρόταση 19η$_1$:

Αν ϕ ένας ισομορφισμός σωμάτων $\phi : K \to K'$ και
$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in K[X]$ ανάγωγο υπέρ το K, ορίζουμε
$f'(X) = \phi(f(X)) = \phi(a_n) X^n + \cdots + \phi(a_1) X + \phi(a_0)$
Αν L επέκταση του K, η οποία περιέχει μια ρίζα a του $f(X)$ και L' επέκταση του K' η οποία περιέχει μια ρίζα a' του $f'(X)$ τότε υπάρχει ένας ισομορφισμός σωμάτων
$\psi : K(a) = K[a] \cong K'(a') = K'[a']$ τ.ω. ${}^{\psi}/_{K} = \phi$, δηλαδή ο περιορισμός του ψ στο K ταυτίζεται με τον ϕ. (Αλλιώς, ο ψ επεκτείνει τον ϕ)
Απόδειξη:
Η συνάρτηση $\phi : K[X] \to K'[X]$ όπως ορίστηκε παραπάνω είναι ισομορφισμός δακτυλίων.
Αν ορίσουμε:

$$\psi : K(a) = K[a] \longrightarrow K'(a') = K'[a']$$
$$g(a) \longmapsto \phi(g(a')) = g'(a')$$

η απεικόνιση αυτή είναι καλά ορισμένη.

(Αν $g(a) = h(a) \Rightarrow (g-h)(a) = 0 \Rightarrow f(x)|_{K[X]}(g(x)-h(x)) \Rightarrow f'(X) =$
$\phi(f(X))|_{K'[X]}(g'(X)-h(X)) \Rightarrow g'(a') = h'(a')$)
Η ψ είναι ισομορφισμός σωμάτων (άσκηση).

Παρατήρηση:

Η Πρόταση 15 είναι άμεση συνέπεια της 19_1 για $K' = K$ και $\phi : K \longrightarrow K,\ \phi = Id|_K$

Πρόταση $19^{η}{}_2$:

Έστω $\phi : K \longrightarrow K'$ ισομορφισμός σωμάτων και $\hat{\phi} : K[X] \longrightarrow K'[X]$ η επέκταση του ϕ στον δακτύλιο $K[X]$.
Αν L και L' δύο σώματα ανάλυσης των $f(X)$ υπέρ το Κ και $f'(X) := \hat{\phi}(f(X))$ υπέρ το Κ′ αντίστοιχα, τότε ο φ επεκτείνεται σε έναν ισομορφισμό σωμάτων
$\phi^* : L \longrightarrow L'$ τ.ω. $\phi^*|_K = \phi$
Απόδειξη:
Υποθέτουμε ότι, $deg\ f(X) = n$ και έστω ότι το $f(X)$ έχει την ανάλυση
$f(X) = a \cdot (X-a_1)(X-a_2)\cdots(X-a_n)$ στον $L[X]$ $(a \in K)$
Προφανώς $a_1, a_2, \cdots, a_n \in L$
Υποθέτουμε ότι για κάποιο $m \in \{0, 1, \cdots, n\}$ οι ρίζες $a_1, a_2, \cdots, a_n \notin K$ και
$a_{m+1}, a_{m+2}, \cdots, a_n \in K$.
Επαγωγή ως προς m.
Αν $m = 0$, όλες οι ρίζες του $f(X)$ ανήκουν στο Κ οπότε
$f'(X) = \hat{\phi}(f(X) = \phi(a)(X-\phi(a_1))\cdots(X-\phi(a_n)))$
Συνεπώς το Κ′ είναι ένα σώμα ανάλυσης του $\hat{\phi}(f)$ και $\phi^* = \phi$.
Υποθέτουμε τώρα ότι $m > 0$.
Επαγωγική υπόθεση:
Για κάθε σώμα Ε και κάθε πολυώνυμο $g(X) \in E[X]$ με λιγότερες από m ρίζες εκτός του Ε σε ένα σώμα ανάλυσης του $g(X)$, έστω L, κάθε ισομορφισμός του Ε επεκτείνεται σε ισομορφισμό του L.
Η υπόθεση $m > 0 \Rightarrow \exists$ ανάγωγος παράγοντας του $f(X) \in K[X]$ που δεν είναι γραμμικός.

Έστω $f_1(X)$.

Επομένως και ο $\hat{\phi}(f_1)$ θα είναι ανάγωγος παράγοντας του $\phi(f)$ στο K′.

Οι ρίζες του f_1 στο L ανήκουν στο $\{a_1, a_2, \cdots, a_n\}$

χ.β.τ.γ έστω a_1 ρίζα του f_1

Ομοίως υπάρχει μια ρίζα $\beta_1 = \phi(a_i)$ (για κάποιο i) του $\hat{\phi}(f_1)$ (από το σύνολο $\{\phi(a_1), \phi(a_2), \cdots, \phi(a_n)\}$)

Από Πρόταση $19_1 \Rightarrow \exists$ ένας ισομορφισμός $\phi' : K(a_1) \longrightarrow K'(\beta_1)$ τ.ω. $\phi'|K = \phi$

Τώρα το f έχει ρίζες λιγότερες του m εκτός του $K(a_1)$ και, λόγω της υπόθεσης της μαθηματικής επαγωγής, υπάρχει ένας ισομορφισμός $\phi^* : L \longrightarrow L'$ τ.ω. $\phi^*|_{K(a_1)} = \phi'$ και συνεπώς $\phi^*|_K = \phi'|_K = \phi$

Πρόταση 20η:

Αν $f(X) \in K[X]$ και L_1, L_2 δύο σώματα ανάλυσης του $f(X)$ υπέρ το K, τότε υπάρχει ένας K-ισομορφισμός, $\psi : L_1 \cong L_2$.

Απόδειξη:

Από πρόταση 19_2, για $\phi = Id_K : K \longrightarrow K$.

Παρατήρηση:

Δικαιούμαστε από εδώ και κάτω να μιλάμε για το σώμα ανάλυσης του $f(X) \in K[X]$

Παραδείγματα:

1. Ποιο είναι το σώμα ανάλυσης του $f(X) = X^4 - 2 \in \mathbb{Q}[X]$
   (Απάντηση: Το $\mathbb{Q}(\sqrt[4]{2}, i)$)

2. Τα πολυώνυμα $X^2+1,\ X^2+X+1,\ X^2+X-1$ είναι τα μοναδικά ανάγωγα πολυώνυμα δεύτερου βαθμού υπέρ το $\mathbb{F}_3$
   Στο σώμα $L = \frac{\mathbb{F}_3[X]}{<(X^2+1)>}$ ανήκει μία ρίζα του X^2+1, η $a := X+ < (X^2+1) >$, δηλαδή $a^2 + 1 = 0$.
   Συνεπώς το $X^2 + 1 = (X - a)(X + a)$, στο $L[X]$.
   Έστω $L' = \frac{\mathbb{F}_3[X]}{<(X^2+X-1)>}$. Το L' είναι σώμα ανάλυσης του $X^2 + X + 1$, δηλαδή, αν

$\beta := X+ < (X^2 + X + 1) >$, τότε $\beta^2 + \beta + 1 = 0$

Τα σώματα L και L' θα έχουν 9 στοιχεία το καθένα.

Μπορούσαμε να συμπεράνουμε ότι υπάρχουν 2-διακεκριμένα σώματα με 9 στοιχεία; ΟΧΙ !

$(a+1)^2 + (a+1)^2 - 1 = (a^2 - 1 + 1) + (a+1) + 1 = 0$

(Εργαζόμαστε *modulo* 3 και λαμβάνουμε υπ' όψιν ότι $a^2 = -1$)

Επίσης $(-a+1)^2 + (-a+1) - 1 = (-1 + a + 1) + (-a+1) - 1 = 0$

Επομένως στο $L[X]$ το $X^2 + X - 1$ αναλύεται στην μορφή

$(X - (a+1))(X - (-a+1)) = 0$

δηλαδή το L είναι σώμα ανάλυσης και του $X^2 + X - 1$ υπέρ το $\mathbb{F}_3$.

Σύμφωνα με την Πρόταση 20, $\frac{\mathbb{F}_3[X]}{<(X^2+1)>} \cong \frac{\mathbb{F}_3[X]}{<(X^2+X-1)>} \cong \frac{\mathbb{F}_3[X]}{<(X^2-X-1)>}$

«Ηθικό» δίδαγμα

Υπάρχει ακριβώς ένα (κατά προσέγγιση ισομορφίας) σώμα με 9-στοιχεία.

Από τα παραπάνω συνάγουμε την ύπαρξη σώματος ανάλυσης για κάθε πεπερασμένο σύνολο πολυωνύμων

$\{f_i(X) \in K[X] \ / \ i = 1, 2, \cdots, n\}$

Τι γίνεται όμως αν έχουμε ένα άπειρο σύνολο;

Υποθέτουμε ότι υπάρχει ένα σώμα L το οποίο είναι σώμα ανάλυσης όλων των πολυωνύμων $f(X) \in K[X]$ $(f \neq 0)$

Προσοχή: Δεν γνωρίζουμε ότι υπάρχει, θα το αποδείξουμε σε λίγο (Ίσως στις διαλέξεις)

Αν ${}^M/_L$ αλγεβρική και $a \in M \ \Rightarrow \ (a$ αλγ $|_L)$, η ${}^L/_K$ αλγεβρική $\Rightarrow \ (a$ αλγ $|_K)$

Έστω $f(X) = Irr(a, K)$. Το $f(X)$ αναλύεται πλήρως στο $L \ \Rightarrow \ a \in L$, δηλαδή $M = L$.

Άρα δεν υπάρχει αλγεβρική επέκταση του L.

Πρόταση 21η:

Αν Κ σώμα οι παρακάτω προτάσεις είναι μεταξύ τους ισοδύναμες:

(*i*) Δεν υπάρχει γνήσια αλγεβρική επέκταση του Κ

(*ii*) Δεν υπάρχει γνήσια πεπερασμένη επέκταση του Κ

(iii) Αν L επέκταση του Κ τότε το σώμα $A := \{a \in L / a \text{ αλγ.}|_K\} = K$

(iv) Κάθε $f(X) \in K[X]$, αναλύεται στο Κ

(v) Κάθε $f(X) \in K[X]$, έχει μια ρίζα στο Κ

(vi) Κάθε ανάγωγο πολυώνυμο του $K[X]$ έχει βαθμό ένα.

Απόδειξη:

- $[(i) \Rightarrow (ii)]$ Αφού κάθε πεπερασμένη είναι αλγεβρική.

- $[(ii) \Rightarrow (iii)]$ Αν $a \in A \ \Rightarrow \ (a \text{ αλγ. } |_K) \ \Rightarrow \ [K(a) : K] < \infty$, πεπερασμένη οπότε η $(ii) \ \Rightarrow \ K(a) = K \ \Rightarrow \ a \in K \ \Rightarrow \ A = K$

- $[(iii) \Rightarrow (iv)]$ Έστω $f(X) \in K[X]$ και L το σώμα ανάλυσης του $f(X)|_K$.
  Η επέκταση ${}^L/_K$ είναι αλγεβρική $\xrightarrow{(iii)} L = K \ \Rightarrow \ (f(X)$ αναλύεται στο $K)$

- $[(iv) \Rightarrow (v)]$ Προφανής

- $[(v) \Rightarrow (vi)]$ Έστω $P(X) \in K[X]$, ανάγωγο.
  Από $\xrightarrow{(v)}$ το $P(X)$ έχει μία ρίζα στο $K \ \Rightarrow \ P(X) = (X - a)p_1(X), \ p_1(X) \in K[X]$
  Το $p(X)$ ανάγωγο στο Κ $\Rightarrow \ p_1(X) =$ σταθερά,
  δηλαδή $p(X) = c(X - a)$, γραμμικό.

- $[(iv) \Rightarrow (i)]$ Αν ${}^L/_K$ αλγεβρική και $a \in L$, τότε, αν
  $p(X) = Irr(a, K), \ \xrightarrow{(vi)} \ deg\, p(X) = 1 \ \Rightarrow \ [K(a) : K] = 1 \ \Rightarrow \ a \in K \ \Rightarrow \ L = K$

Ορισμός:

Αν Κ πληρεί μια από τις παραπάνω προτάσεις, και συνεπώς όλες!, θα λέγεται **αλγεβρικά κλειστό**

Αν τώρα ${}^L/_K$ επέκταση σωμάτων και

(ι) ${}^L/_K$ αλγεβρική

(ιι) L αλγεβρικά κλειστό

τότε το L θα λέγεται **αλγεβρική θήκη του Κ**

Πρόταση 22η:

Το $\mathbb{C}$ είναι αλγεβρικά κλειστό (Θεμελιώδες Θεώρημα της Άλγεβρας)

Θα αποδειχθεί στις διαλέξεις

Το $\tilde{\mathbb{Q}} = \{a \in \mathbb{C} / a \text{αλγ. } |_{\mathbb{Q}}\}$ είναι αλγεβρικά κλειστό και $^{\tilde{\mathbb{Q}}}/_{\mathbb{Q}}$ είναι αλγεβρική.

Συνεπώς το $\tilde{\mathbb{Q}}$ είναι αλγεβρική θήκη του $\mathbb{Q}$.

Κεφάλαιο 4

ΘΕΩΡΙΑ GALOIS

4.1 Αυτομορφισμοί Σωμάτων

Ιδέα:Αντί να μελετούμε ιδιότητες των επεκτάσεων σωμάτων, μελετούμε συναρτήσεις που ορίζουμε στα σώματα. Στη συγκεκτιμένη περίπτωση αυτομορφισμούς σωμάτων.
Η έννοια του αυτομορφισμού ενός σώματος, έχει οριστεί στο προηγούμενο Κεφάλαιο.

Πρόταση 1η:

Το σύνολο των αυτομορφισμών ενός σώματος K, ας το συμβολίσουμε $AutK$, αποτελεί ομάδα με πράξη την σύνθεση απεικονίσεων.
Απόδειξη:

- Η σύνθεση δυο αυτομορφισμών ενός σώματος, είναι αυτομορφισμός αυτού.
- Ο προσεταιρισμός ισχύει στη σύνθεση συναρτήσεων.
- Η ταυτοτική συνάρτηση είναι μοναδιαίο στοιχείο του συνόλου $AutK$, αφού είναι αυτομορφισμός και $f \circ Id_K = Id_K \circ f = f,\ \forall f \in AutK$.
- Αν $f \in AutK \ \Rightarrow \ (f \ \underset{\text{επί}}{\overset{1-1}{}}) \ \Rightarrow \ (\exists\, f^{-1} : K \ \underset{1\text{-}1}{\overset{\text{επί}}{\longrightarrow}}; K)$ και, αν
  $f(X) = Y \ \Rightarrow \ f^{-1}(Y) = X$
  Επομένως, $f^{-1}(Y_1 + Y_2) = f^{-1}(f(X_1) + f(X_2)) \overset{f,\ \text{ομομορφισμός}}{=\!=\!=} f^{-1}(f(X_1 + X_2)) =$

$(f^{-1} \circ f)(X_1 + X_2) = X_1 + X2 = f^{-1}(Y_1) + f^{-1}(Y_2)$
Ομοίως, $f^{-1}(Y_1Y_2) = f^{-1}[f(X_1) \cdot f(X_2)] \overset{f,\ \text{ομομορφισμός}}{=\!=\!=} f^{-1}(f(X_1X_2)) = X_1X_2 = f^{-1}(Y_1)f^{-1}(Y_2)$

Έστω τώρα $^L/_K$ επέκταση σωμάτων.

Ορισμός:

Αν $\sigma \in AutL$ τ.ω. $\sigma(a)=a \ \forall\, a \in K$ τότε ο σ θα λέγεται K-αυτομορφισμός του L.
Συμβολισμός: $Aut(^L/_K) = \{\sigma \ \in \ AutL \ | \ \sigma(\alpha)=\alpha \ \forall\, \alpha \in K\}$

Πρόταση 2^{η}:

$Aut(^L/_K) \ \leq AutL$
Απόδειξη:
Αν σ, τ $\in \ \ Aut(^L/_K) \ \Rightarrow \ [\sigma \in AutL$ και $\sigma(a) = a, \ \forall a \in K], \ [\tau \in AutL$ και $\tau(a) = a, \ \forall a \in K]$
Άρα $(\sigma \circ \tau) \in AutL$ και $(\sigma \circ \tau)(a) = \sigma(\tau(a)) = \sigma(a) = a \ \forall a \in K.$
Συνεπώς $\sigma \circ \tau \in Aut(^L/_K)$.
Επίσης, αν $\sigma \in Aut(^L/_K) \ \Rightarrow \ [\sigma \in AutL$ και $\sigma(a) = a \ \ \forall a \in K]$.
Συνεπώς και $\sigma^{-1} \in AutL$ και $\sigma^{-1}(a) = a \ \ \forall a \in K \ \Rightarrow \ \sigma^{-1} \in Aut(^L/_K)$.

Παρατήρηση: Συχνά λέγεται και ομάδα $Galois$ αλλά δημιουργείται σύγχυση.

ΣΗΜΑΝΤΙΚΗ ΙΔΕΑ

Πώς συνδέονται τα ενδιάμεσα σώματα $K \leq E \leq L$ με τις υποομάδες $H \leq Aut(^L/_K)$;

Ορισμός:

Για κάθε ενδιάμεσο σώμα $K \leq E \leq L$ ορίζουμε $\Gamma(E) := \{\sigma \in AutL \ / \ \sigma(a) = a \ \ \forall a \in E\}$
Για κάθε $H \leq Aut(^L/_K)$ ορίζουμε $\ \Phi(H) = \{a \in L \ / \ \sigma(a) = a, \ \forall \sigma \in H\}$

Πρόταση 3η:

Έστω ${}^{L}/_{K}$ επέκταση σωμάτων και Ε ενδιάμεσο σώμα $K \leq E \leq L$.

Ισχύει: $\Gamma(E) \leq Aut({}^{L}/_{K})$.

Επίσης, αν $H \leq Aut({}^{L}/_{K})$ τότε $\Phi(H)$ ενδιάμεσο σώμα της ${}^{L}/_{K}$, $K \leq \Phi(H) \leq L$.

Απόδειξη:

1 $\Gamma(E) \neq \emptyset$, αφού $Id_L \in \Gamma(E)$

- Αν $\sigma \in \Gamma(E) \Rightarrow [\sigma \in AutL$ και $\sigma(a) = a \ \forall a \in E]$
  Επειδή, $K \leq E \Rightarrow \sigma(a) = a \ \forall a \in K$,
  άρα $\sigma \in Aut({}^{L}/_{K})$.
  Επομένως, $\Gamma(E) \subseteq Aut({}^{L}/_{K})$

- Αν $\sigma, \tau \in \Gamma(E) \Rightarrow \sigma \circ \tau \in \Gamma(E)$
  (αφού $\sigma \circ \tau \in AutL$ και $(\sigma \circ \tau)(a) = \sigma(\tau(a)) = \sigma(a) = a \ \forall a \in E$)

- Αν $\sigma \in \Gamma(E) \Rightarrow \sigma^{-1} \in \Gamma(E)$
  (αφού $\sigma^{-1} \in AutL$ και $\sigma^{-1}(a) = a \ \forall a \in E$)

2 $H \leq Aut({}^{L}/_{K}) \Rightarrow$
Αν $a \in K \Rightarrow [\forall \sigma \in Aut({}^{L}/_{K}) \ \sigma(a) = a]$
Συνεπώς και $[\forall \sigma \in H$, ισχύει $\sigma(a) = a]$, δηλαδή $K \subseteq \Phi(H)$.
Αν $a, b \in \Phi(H) \Rightarrow [\forall \sigma \in H$ ισχύει: $\sigma(a) = a$ και $\sigma(b) = b]$
$\Rightarrow [\forall \sigma \in H, \sigma(a - b) = \sigma(a) - \sigma(b) = a - b \Rightarrow a - b \in \Phi(H)$.
Επίσης, αν $a, b \in \Phi(H)$ και $b \neq 0$, τότε
$[\forall \sigma \in H, \ \sigma(ab^{-1}) = \sigma(a)\sigma^{-1}(b)) = a \cdot b^{-1}]$, δηλαδή $ab^{-1} \in \Phi(H)$.
Συνεπώς, $\Phi(H) \leq L$.
Ερώτημα: Αν $K \leq E_1 \leq E_2 \leq L$ όπου $E_1 \rightarrow \Gamma(E_1)$ και $E_2 \rightarrow \Gamma(E_2)$.
Τι σχέση έχουν οι $\Gamma(E_1)$ και $\Gamma(E_2)$;
Αντίστροφα: Αν $H_2 \leq H_1 \leq Aut({}^{L}/_{K})$ όπου $H_2 \rightarrow \Phi(H_2)$ και $H_1 \rightarrow \Phi(H_1)$.
Τι σχέση έχουν οι $\Phi(H_2)$ και $\Phi(H_1)$;

Πρόταση 4η:

Έστω ${}^{L}/_{K}$ επέκταση σωμάτων.

1 Αν E_1, E_2 ενδιάμεσα σώματα τ.ω. $E_1 \leq E_2 \Rightarrow \Gamma(E_1) \geq \Gamma(E_2)$

2 Αν $H_1, H_2 \leq Aut({}^{L}/_{K})$ τ.ω. $H_1 \leq H_2 \Rightarrow \Phi(H_1) \geq \Phi(H_2)$

Δηλαδή οι Γ και Φ αντιστρέφουν τη διάταξη.

Απόδειξη:

1 Έστω $\sigma \in \Gamma(E_2) \Rightarrow [\sigma \in AutL$ και $\sigma(a) = a, \ \forall a \in E_2]$
Επειδή $E_1 \leq E_2 \Rightarrow [\sigma \in AutL$ και $\sigma(a) = a, \ \forall a \in E_1]$.
Άρα $\sigma \in \Gamma(E_1) \Rightarrow \Gamma(E_2) \leq \Gamma(E_1)$.

2 Έστω $a \in \Phi(H_2) \Rightarrow [a \in L$ και $\sigma(a) = a \ \forall \sigma \in H_2]$
Επειδή $H_1 \leq H_2$
$\Rightarrow [a \in L$ και $\sigma(a) = a \ \forall \sigma \in H_1] \Rightarrow a \in \Phi(H_1) \Rightarrow \Phi(H_2) \leq \Phi(H_1)$.

Ερώτημα: Μήπως οι δύο συναρτήσεις Φ και Γ είναι η μία αντίστροφη της άλλης;
Αν τις εφαρμόσω διαδοχικά τότε η τελική εικόνα τι σχέση έχει με την αρχική;

$$\left.\begin{array}{l} E \xrightarrow{\Gamma} \Gamma(E) \xrightarrow{\Phi} E' \\ H \xrightarrow{\Phi} \Phi(H) \xrightarrow{\Gamma} H' \end{array}\right\} \overset{???}{=\!=}$$

Αντιπαράδειγμα: $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2})$
Αν $\sigma \in Aut({}^{L}/_{K})$ τότε, από $(\sqrt[3]{2})^3 - 2 = 0 \Rightarrow [\sigma(\sqrt[3]{2})]^3 - \sigma(2) = \sigma(0) \Rightarrow$
$[\sigma(\sqrt[3]{2})]^3 - \sigma(2) = \sigma(0) \Rightarrow [\sigma(\sqrt[3]{2})]^3 - 2 = 0 \Rightarrow \sigma(\sqrt[3]{2})$ ρίζα του $X^3 - 2 \in \mathbb{Q}[X]$.
Οι ρίζες είναι $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$.
Επειδή $L = \mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{R}$, κατ' ανάγκη $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$.
Συνεπώς, $\forall a \in L$ ισχύει $\sigma(a) = a$, δηλαδή $\sigma = Id_L \Rightarrow Aut({}^{L}/_{K}) = \{Id_L\}$
Επομένως $\Gamma(L) = \Gamma(\mathbb{Q}(\sqrt[3]{2})) = \{Id_L\}$ και $\Gamma(K) = \Gamma(\mathbb{Q}) = \{Id_L\}$, δηλαδή Γ όχι ένα προς ένα.
Επίσης, $\Phi(\{Id_L\}) = L = \mathbb{Q}(\sqrt[3]{2})$ και
$\Phi(\Gamma(\mathbb{Q})) = \{a \in L / \sigma(a) = a \ \forall \sigma \in \Gamma(\mathbb{Q}) = \{Id_L\}\} = L$

Παράδειγμα:

$\mathbb{C} = \mathbb{R}(i) = a + bi \ / \ a, b \in \mathbb{R}\}$

Αν $\sigma \in Aut(^{\mathbb{C}}/_{\mathbb{R}})$, από $i^2 + 1 = 0$

$\Rightarrow \ \sigma[i^2 + 1] = \sigma(0) = 0 \ \Rightarrow \ [\sigma(i)]^2 + \sigma(1) = 0 \ \Rightarrow \ [\sigma(i)]^2 + 1 = 0$

$\Rightarrow \ \sigma(i)$ ρίζα του $X^2 + 1$

Άρα $\sigma(i) = \left\{ \begin{array}{c} +i \\ -i \end{array} \right\}$

Αν $\sigma(i) = i \ \Rightarrow \ \sigma(a + bi) = \sigma(a) + \sigma(b)\sigma(i) = a + bi, \ \ \forall z = a + bi \in \mathbb{C} \ \Rightarrow \ \sigma = Id_{\mathbb{C}}$

Αν $\sigma(i) = -i$, τότε $\sigma(a + bi) = a - bi$

Ο αυτομορφισμός αυτός λέγεται μιγαδική συζυγία.

Επομένως $Aut(^{\mathbb{C}}/_{\mathbb{R}}) = \{1, \sigma\} = \{Id_{\mathbb{C}}, \sigma\}$

Εδώ $[\mathbb{C} : \mathbb{R}] = 2$ και $\#Aut(^{\mathbb{C}}/_{\mathbb{R}}) = 2$

Δεν υπάρχουν ενδιάμεσα σώματα.

$\mathbb{C} \ \longleftrightarrow \ \{Id_L\}$

$\mathbb{R} \ \longleftrightarrow \ Aut(^{\mathbb{C}}/_{\mathbb{R}})$

Δηλαδή εδώ ισχύει η αμφιμονοσήμαντη αντιστοιχία.

Πρόταση 5η:

Έστω $^{L}/_{K}$ επέκταση σωμάτων και $a \in L$

Αν α ρίζα του $f(X) \in K[X]$ και $\sigma \in Aut(^{L}/_{K})$ τότε και το $\sigma(a)$ είναι επίσης ρίζα του $f(X)$

Απόδειξη:

Έστω $f(X) = a_0 + a_1X + \cdots + a_nX^n \ \in K[X]$ και ότι $f(a) = 0 \ \Rightarrow =$

$a_0 + a_1a + \cdots + a_na^n = 0 \ \Rightarrow \ a_0 + a_1\sigma(a) + \cdots + a_n\sigma(a)^n = 0 \ \Rightarrow \ f(\sigma(a)) = 0 \ \Rightarrow \ \sigma(a)$ επίσης ρίζα του $f(X) \in K[X]$.

Πρόταση 6η:

Έστω $^{L}/_{K}$ επέκταση σωμάτων και Ε ενδιάμεσο σώμα καθώς και $H \leq Aut(^{L}/_{K})$

Ισχύουν: $E \leq \Phi(\Gamma(E))$ και $H \leq \Gamma(\Phi(H))$

Απόδειξη:

Αν $a \in E$, τότε $[\forall \sigma \in \Gamma(E) \ \Rightarrow \ \sigma(a) = a] \ \Rightarrow \ a \in \Phi(\Gamma(E))$

Έστω τώρα $\sigma \in H$

$\Phi(H) = \{a \in L \ / \ \sigma(a) = a \ \ \forall \sigma \in H\}$

Αν λοιπόν

$a \in \Phi(H) \ \Rightarrow \ [\sigma(a) = a \ \ \forall \sigma \in H] \ \Rightarrow \ [\sigma(a) = a \ \ \forall a \in \Phi(H)] \ \Rightarrow \ \sigma \in \Gamma(\Phi(H))$.

Οι επεκτάσεις με τις οποίες θα ασχοληθούμε στη συνέχεια θα είναι πεπερασμένες και οι ομάδες που θεωρούμε θα είναι επίσης πεπερασμένες.

Επομένως το ερώτημα, πότε στην Πρόταση 6, ισχύει η ισότητα θα ήταν ισοδύναμο με

$[E : K] = [\Phi(\Gamma(E)) : E]$

Πρόταση 7η:

Έστω ${}^{L}/_{K}$ πεπερασμένη επέκταση σωμάτων και G πεπερασμένη υποομάδα της $Aut({}^{L}/_{K})$.

Ισχύει: $[L : \Phi(G)] = \#G$

(χωρίς απόδειξη: $Howie, 100 - 102$, Κ. Λάκκη, $198 - 201$ κ.τ.λ.)

4.2 Κανονικές Επεκτάσεις

Ερώτημα: Πότε ισχύουν $(\Phi \circ \Gamma)(E) = E, \ \forall E, \ \ K \leq E \leq L$ και
$(\Gamma \circ \Phi)(H) = H, \ \forall \ H \leq Aut(^L/_K)$;
Υποθέτουμε ότι η επέκταση $^L/_K$ είναι πεπερασμένη. (Το πρόβλημα σε άπειρες επεκτάσεις, χρήζει εντελώς διαφορετικής αντιμετώπισης.)
Μελετούμε και πάλι τα δύο παραδείγματα της προηγούμενης παραγράφου.
Στο πρώτο παράδειγμα παρατηρούμε ότι $[L : K] = 3$, ενώ $\#Aut(^L/_K) = 1$ ενώ στο δεύτερο $[L : K] = 2$ και $\#Aut(^L/_K) = 2$.
Αργότερα θα δούμε ότι πάντοτε (όταν η $^L/_K$ είναι πεπερασμένη) ισχύει:
$\#Aut(^L/_K) \leq [L : K]$
Η «καλή περίπτωση», αυτή που θα ονομάσουμε επέκταση $Galois$ και στην οποία η απάντηση στο αρχικό ερώτημα θα είναι θετική, ισχύει ακριβώς τότε όταν
$\#Aut(^L/_K) = [L : K]$

Παρατήρηση: Αυτό συμβαίνει σύμφωνα με την Πρόταση 7, ακριβώς τότε όταν $[L : \Phi(Aut(^L/_K))] = [L : K]$, δηλαδή όταν $K = \Phi(Aut(^L/_K))$, το Κ είναι σώμα σταθερών στοιχείων της $Aut(^L/_K)$.
Την περίπτωση αυτή θα μελετήσουμε στην επόμενη παράγραφο.
Ας επιστρέψουμε και πάλι στα παραδείγματα της προηγούμενης παραγράφου.
Στο πρώτο παράδειγμα το $L = \mathbb{Q}(\sqrt[3]{2})$ περιέχει μια ρίζα του πολυωνύμου $f(X) = X^3 - 2$, αλλά δεν περιέχει τις υπόποιπες, δηλαδή το $f(X)$ δεν αναλύεται πλήρως στο L.
Στο δεύτερο παράδειγμα, στο $L = \mathbb{C} = \mathbb{R}(i)$, το πολυώνυμο $f(X) = X^2 + 1 \ \in \mathbb{R}[X]$ αναλύεται πλήρως στο $\mathbb{C}$, αφού και η άλλη ρίζα του $f(X)$, το $-i \in \mathbb{C}$

Ορισμός:

Η επέκταση σωμάτων $^L/_K$ θα λέγεται κανονική ($normal$) όταν κάθε ανάγωγο πολυώνυμο του $K[X]$ το οποίο έχει μία (τουλάχιστο) ρίζα του στο L, αναλύεται πλήρως στο L.
Πώς όμως θα ελέγξουμε αν δοθείσα επέκταση είναι κανονική;
Ισχύει η ακόλουθη:

Πρόταση 8η:

Έστω ${}^{L}/_{K}$ πεπερασμένη επέκταση σωμάτων. (Η ${}^{L}/_{K}$ είναι κανονική) $\Rightarrow$ (το L είναι σώμα ανάλυσης ενός πολυωνύμου $f(X) \in K[X]$).
(και η πρόταση αυτή θα αποδειχθεί στις διαλέξεις των φοιτητών)

Παραδείγματα:

1. Αν $[L : K] = 2$, τότε η ${}^{L}/_{K}$ είναι κανονική.
   Απόδειξη: Αν $a \in L \setminus K$,τότε $L = K(a)$,
   ($[L : K] = 2 < \infty \Rightarrow {}^{L}/_{K}$ αλγεβρική $\Rightarrow$ a αλγ.$|_K$)
   Έστω $P(X) := Irr(a, K)$. Το $P(X)$ αναλύεται πλήρως στο L και μάλιστα είναι σώμα ανάλυσης του $P(X) \in K[X]$
   Συνεπώς, η ${}^{L}/_{K}$ είναι κανονική.

2. Η επέκταση ${}^{\mathbb{Q}(\omega, \sqrt[3]{2})}/_{\mathbb{Q}}$ είναι κανονική, αφού το $L := \mathbb{Q}(\omega, \sqrt[3]{2})$ είναι σώμα ανάλυσης του $P(X) = X^3 - 2 \in \mathbb{Q}[X]$

3. Η επέκταση ${}^{\mathbb{Q}(\sqrt[4]{2}, i)}/_{\mathbb{Q}}$ είναι κανονική, αφού το σώμα $L := \mathbb{Q}(\sqrt[4]{2}, i)$ είναι σώμα ανάλυσης το πολυώνυμο $f(X) = X^4 - 2 \in \mathbb{Q}[X]$

4. Έστω K, $chK = p > 0$ και $L = K(a)$ τ.ω. $a^p \in K$
   Το a είναι ρίζα του πολυωνύμου $f(X) = X^p - a^p \in K[X]$
   Το $f(X)$ αναλύεται στο L, στη μορφή $f(X) = (X - a)^p$.
   Συνεπώς το L είναι σώμα ανάλυσης του $f(X) \in K[X]$, δηλαδή η επέκταση ${}^{L}/_{K}$ είναι κανονική.
   Το πολυώνυμο $f(X)$ έχει μία μόνο ρίζα, το a. Άρα και το ανάγωγό του αφού, αν $P(X) = Irr(a, K)|setminus(X - a)^p \Rightarrow P(X) = (X - a)^r, \ 1 \leq r \leq p$.
   Επειδή κάθε K-αυτομορφισμός του L, έστω σ, απεικονίζει ρίζα του $P(X)$ σε ρίζα αυτού, έπεται ότι: $\sigma(a) = a$, δηλαδή $\sigma = Id_L$ στο $L = K(a)$.
   Επομένως $Aut({}^{L}/_{K}) = \{Id_L\}$.

5. Έστωσαν, $K = \mathbb{Q} \leq L = \mathbb{Q}(\sqrt{2}) \leq M = \mathbb{Q}(\sqrt[4]{2})$
   Η επέκταση ${}^{L}/_{K}$ είναι κανονική αφού $[L : K] = 2$.
   Η επέκταση ${}^{M}/_{L}$ είναι κανονική αφού $[M : L] = 2$.

Όμως η ${}^{M}/_{K}$ δεν είναι κανονική.

Υπάρχει πολυώνυμο $f(X) = X^4 - 2 \ \in \mathbb{Q}[X]$ το οποίο έχει μια ρίζα στο M, αλλά δεν αναλύεται πλήρως στο M.

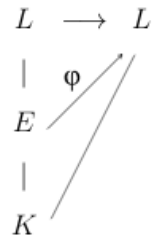
Συμπέρασμα: Εν γένει [${}^{M}/_{L}$ κανονική και ${}^{L}/_{K}$ κανονική] $\nRightarrow$ [${}^{M}/_{K}$ κανονική]
Βέβαια ισχύει: [Αν $K \leq L \leq M$ και ${}^{M}/_{K}$ κανονική] τότε [${}^{M}/_{L}$ κανονική]
(άσκηση)

Πόρισμα 1:

Αν ${}^{L}/_{K}$ πεπερασμένη και κανονική και E ενδιάμεσο σώμα, τότε κάθε K-μονομορφισμός του E στο L μπορεί να επεκταθεί σε έναν K-αυτομορφισμό του L.

Απόδειξη:

Έστω φ: K-μονομορφισμός του E στο L.



Η Πρόταση 8 συνεπάγεται ότι υπάρχει ένα πολυώνυμο $f(X) \in K[X]$ τ.ω. το L είναι σώμα ανάλυσης του $f(X)$ υπέρ το K.
Επομένως και $f(X) \in E[X]$ και L είναι σώμα ανάλυσης του $f(X)$ υπέρ το E.
Επίσης και $\phi(f(X)) \in \phi(E) \leq L$ και L είναι σώμα ανάλυσης του $\phi(f(X))$ υπέρ το $\phi(E)$.
Σύμφωνα με την Πρόταση 19_2, ο ϕ επεκτείνεται σε κάποιο K-αυτομορφισμό ϕ^* του L ο οποίος επεκτείνει τον ϕ.

Σημείωση: $\phi(f(X)) = f(X)$, αφού ϕ K-μονομορφισμός.

Παραδείγματα:

$K = \mathbb{Q} \leq E = \mathbb{Q}(\sqrt{3}) \leq L = \mathbb{Q}(\sqrt{3}, \sqrt{7})$
Ο $\phi : E \hookrightarrow L \quad \phi(a + b\sqrt{3}) = a - b\sqrt{3}$ είναι K-μονομορφισμός του E στο L.
Επεκτείνεται στο $L = \mathbb{Q}(\sqrt{3}, \sqrt{7})$,

$\phi^* : L \to L$

$a + b\sqrt{3} + c\sqrt{7} + d\sqrt{21} \longmapsto a - b\sqrt{3} + c\sqrt{7} - d\sqrt{21}$

Πόρισμα 2:

Έστω ${}^{L}/_{K}$ κανονική επέκταση σωμάτων. Αν $P(X) \in K[X]$, ανάγωγο και $a_1, a_2 \in L$, ρίζες του $P(X)$, τότε υπάρχει ένας K-αυτομορφισμός του L, έστω σ τ.ω. $\sigma(a_1) = a_2$

Απόδειξη:

Η πρόταση 15, συνεπάγεται την ύπαρξη ενός K-ισομορφισμού $\phi : K(a_1) \longrightarrow K(a_2)$ τ.ω. $\phi(a_1) = a_2$.

$$\begin{array}{ccc} L & \xrightarrow{\phi^*} & L \\ | & & | \\ K(a_1) & \underset{\cong}{\xrightarrow{\phi}} & K(a_2) \\ \diagdown & & \diagup \\ & K & \end{array}$$

Από Πόρισμα 1, έπεται ότι ο ϕ επεκτείνεται σε K-αυτομορφισμό $\phi^* : L \longrightarrow L$ και προφανώς $\phi(a_1) = a_2$.

«Ωραίο πράγμα» η κανονικότητα επεκτάσεων!

Αλλά αν η επέκταση δεν είναι κανονική, μήπως μπορούμε να την εμφυτεύσουμε σε μια κανονική;

Ορισμός:

Έστω ${}^{L}/_{K}$ πεπερασμένη επέκταση σωμάτων.

Το σώμα $N \quad L \leq N$ θα λέγεται κανονική θήκη του L υπέρ το K όταν:

$$\left\{ \begin{array}{l} (1) \ {}^{N}/_{K} \text{ είναι κανονική} \\ (2) \ \text{Αν E γνήσιο υπόσωμα του N, τ.ω.} L \leq E \ \ (\text{δηλαδή} L \leq E \nleqq N) \\ \qquad \text{τότε η } {}^{E}/_{K} \text{ δεν είναι κανονική} \end{array} \right\}$$

Πρόταση 9η:

Έστω ${}^{L}/_{K}$ πεπερασμένη επέκταση σωμάτων.

1. Υπάρχει πάντοτε μια κανονική θήκη N της ${}^{L}/_{K}$.

2. Αν ${}^{L'}/_{K}$ πεπερασμένη επέκταση και υπάρχει κάποιος K-ισομορφισμός σωμάτων $\phi : L \to L'$ και N′ η κανονική θήκη του L' υπέρ το K, τότε υπάρχει ένας ισομορφισμός $\psi : N \to N'$ τ.ω. να επεκτείνει τον ϕ

Απόδειξη:

1. Έστω $\{\omega_1, \omega_2, \cdots, \omega_n\}$ μια βάση της επέκτασης ${}^{L}/_{K}$.
   Η ${}^{L}/_{K}$ είναι πεπερασμένη, άρα όλα τα ω_i είναι αλγεβρικά υπέρ το K.
   Έστω $P_i(X) = Irr(\omega_i, K) \quad (i = 1, 2, \cdots, n)$ και $f(X) = \prod_{i=1}^{n} P_i(X)$.
   Αν N ένα σώμα ανάλυσης του πολυωνύμου $f(X)$ υπέρ το K, τότε (Πρόταση 8), η επέκταση ${}^{N}/_{K}$ είναι κανονική.
   Περιέχει όλες τις ρίζες των $P_i(X), \quad (i = 1, 2, \cdots, n)$, συνεπώς και τα $\omega_1, \omega_2, \cdots, \omega_n$.
   Επομένως $L \leq N$.
   Έστω E ένα ενδιάμεσο σώμα της επέκτασης ${}^{N}/_{L}$.
   Υποθέτουμε ότι η ${}^{E}/_{K}$ είναι κανονική.
   Για κάθε $i \in \{1, 2, \cdots, n\}$ το σώμα E περιέχει μια (τουλάχιστον) ρίζα του πολυωνύμου $P_i(X)$, την ω_i.
   Λόγω της υπόθεσης ότι η ${}^{E}/_{K}$ είναι κανονική, έπεται ότι το E περιέχει όλες τις ρίζες όλων των $P_i(X) \quad (i = 1, 2, \cdots, n)$.
   Το N είναι το σώμα ανάλυσης του $f(X)$, άρα $E = N$, δηλαδή το N είναι μια κανονική θήκη του L υπέρ το K.

2.
$$\begin{array}{ccc} N & \xrightarrow{\psi} & N' \\ \uparrow & & \uparrow \\ K & \xrightarrow{Id_K} & K \end{array}$$

   Έστω N′ η κανονική θήκη του L' υπέρ το K.
   Αν $a \in L$, το a έχει μονοσήμαντη παράσταση,
   $a = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n \mid a_i \in K$.
   Έστω $a' = \phi(a)$ ένα οποιοδήποτε στοιχείο του L'.
   Το $a' = a_1\phi(\omega_1) + a_2\phi(\omega_2) + \cdots + a_n\phi(\omega_n)$.

Το σύνολο $\{\phi(\omega_1), \cdots, \phi(\omega_n)\}$ είναι βάση της επέκτασης ${}^{L'}/_{K}$.

(Αν $\lambda_1\phi(\omega_1) + \cdots + \lambda_n\phi(\omega_n) = 0 \Rightarrow \phi(\lambda_1\omega_1 + \cdots + \lambda_n\omega_n) = 0$

Ο ϕ είναι ισομορφισμός, συνεπώς $(\lambda_1\omega_1 \cdots + +\lambda_n\omega_n) = 0$ και αφού $\{\omega_1, \omega_2, \cdots, \omega_n\}$ βάση της επέκτασης ${}^{L}/_{K} \Rightarrow \lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$)

Ο ϕ είναι ισομορφισμός σωμάτων, συνεπώς για κάθε $i = 1, 2, \cdots, n$ το ανάγωγο πολυώνυμο του $\phi(\omega_i)$ υπέρ το Κ, είναι το $\hat{\phi}(P_i(X))$.

Η ${}^{N'}/_{K}$ είναι, εξ υποθέσεως, κανονική.

Επομένως περιέχει όλες τις ρίζες, όλων των $\hat{\phi}(P_i(X))$.

Συνεπώς θα είναι ένα σώμα ανάλυσης του πολυωνύμου $\hat{\phi}(f(X))$.

Από Πρόταση 19_2, προκύπτει αμέσως το (2).

Παρατήρηση: Από την Πρόταση 9, προκύπτει ότι, αν ${}^{L}/_{K}$ πεπερασμένη και έστω ότι $[L : K] = n$, τότε υπάρχουν αλγεβρικά στοιχεία $\omega_1, \omega_2, \cdots, \omega_n$ υπέρ το Κ τ.ω. $L = K(\omega_1, \omega_2, \cdots, \omega_n)$.

Έστω $P_i(X) = Irr(\omega_i, K)$, για $i = 1, 2, \cdots, n$.

Αν $f(X) := \prod_{i=1}^{n} P_i(X)$, τότε το σώμα Ν που προκύπτει από το Κ, με επισύναψη όλων των ριζών του πολυωνύμου $f(X)$ είναι μια (λόγω της Πρότασης 9 το (2) κανονική θήκη του L υπέρ το Κ.

Παραδείγματα:

1. Αν $K = \mathbb{Q}$ και $L = \mathbb{Q}(\sqrt[3]{2})$ τότε $N = \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$.
2. Αν $K = \mathbb{Q}$ και $L = \mathbb{Q}(\sqrt[4]{2})$ τότε $N = \mathbb{Q}(\sqrt[4]{2}, i)$.
3. Αν $K = \mathbb{Q}$ και $L = \mathbb{Q}(\sqrt[8]{2})$ τότε $N = \mathbb{Q}(\sqrt[8]{2}, i)$.

Χωρίς απόδειξη, αναφέρουμε τέλος την:

Πρόταση $10^{η}$:

Έστω ${}^{L}/_{K}$ πεπερασμένη επέκταση σωμάτων.

Υποθέτουμε ότι η ${}^{L}/_{K}$ είναι κανονική.

Αν Ε ενδιάμεσο σώμα της ${}^{L}/_{K}$, τότε η (${}^{E}/_{K}$ είναι κανονική) $\Rightarrow$ (Κάθε Κ-μονομορφισμός, $E \rightarrow L$ είναι Κ-αυτομορφισμός του Ε)

4.3 Διαχωρίσιμες Επεκτάσεις

Υπενθύμιση το Παράδειγμα 4 της παραγράφου 2.
Αν Κ σώμα, $chK = p > 0$ και $L = K(a)$ τ.ω. $a^p \in K$, το
$P(X) = Irr(a, K) \mid X^p - a^p \in K[X]$ και αν $a \notin K$, τότε το $P(X) = (X - a)^r$ με
$2 \leq r \leq p$
Πάλι $[K(a) : K] = r \geq 2$, ενώ $Aut(^L/_K) = \{Id_L\}$, δηλαδή δεν ισχύει η ισότητα
$[K(a) : K] \neq \#(Aut(^L/_K))$.
Ο λόγος είναι εδώ ότι το ανάγωγο πολυώνυμο $P(X)$ έχει ρίζες με πολλαπλότητα μεγαλύτερη του 1. (εδώ μια ρίζα).

Ορισμός:

1. Ένα ανάγωγο πολυώνυμο $f(X) \in K[X]$ θα λέγεται διαχωρίσιμο (*seperable*) υπέρ το Κ, όταν σε κάποιο σώμα ανάλυσης του δεν έχει ρίζες πολλαπλότητας > 1, δηλαδή όλες οι ρίζες του είναι απλές.

2. Ένα ,οποιοδήποτε, πολυώνυμο $g(X) \in K[X]$ θα λέγεται διαχωρίσιμο υπέρ το Κ όταν όλοι οι ανάγωγοι παράγοντες του είναι διαχωρίσιμοι.

3. Έστω $^L/_K$ επέκταση σωμάτων και $a \in L$, a αλγεβρικό υπέρ το Κ. Το a θα λέγεται διαχωρίσμο υπέρ το Κ όταν το $P(X) = Irr(a, K)$ είναι διαχωρίσιμο υπέρ το Κ.

4. Η αλγεβρική επέκταση $^L/_K$ θα λέγεται διαχωρίσιμη όταν κάθε $a \in L$ είναι διαχωρίσιμο υπέρ το Κ.

5. Ένα σώμα Κ θα λέγεται τέλειο (*perfect*) όταν κάθε πολυώνυμο $f(X) \in K[X]$, είναι διαχωρίσιμο υπέρ το Κ.

Πρόταση 11η:

Έστω $f(X) \in K[X]$ και L ένα σώμα ανάλυσης αυτού.
(Το $f(X)$ έχει διακεκριμένες ρίζες στο L) $\Leftrightarrow$ (ο ΜΚΔ$(f(X), f'(X)) = 1$).
Απόδειξη:

Αν $f(X) = (X-a)^r g(X)$ στον $L[X]$ με $r \geq 2$, τότε

$f'(X) = (X-a)^r g'(X) + r(X-a)^{r-1} g(X)$.

Συνεπώς $(X-a) \mid \text{ΜΚΔ}(f(X), f'(X))$, δηλαδή $\text{ΜΚΔ}(f(X), f'(X)) \neq 1$.

Αντίστροφα, υποθέτουμε ότι το $f(X)$ έχει διακεκριμένες ρίζες. Επομένως για κάθε ρίζα $a \in L$ του $f(X)$ ισχύει $f(X) = (X-a)g(X)$ και $g(a) \neq 0$.

Επομένως $f'(X) = g(X) + (X-a)g'(X) \Rightarrow f'(a) = g(a) \neq 0$, δηλαδή $(X-a) \nmid f'(X)$.

Αυτό ισχύει για κάθε παράγοντα του $f(X)$ και συνεπώς $\text{ΜΚΔ}(f(X), f'(X)) = 1$

Πρόταση 12η:

Έστω $f(X)$ ανάγωγο πολυώνυμο του $K[X]$.

(ι) Αν $chK = 0$, τότε το $f(X)$ είναι διαχωρίσιμο υπέρ το K

(ιι) Αν $chK = p$, τότε το $f(X)$ είναι διαχωρίσιμο υπέρ το K, εκτός αν έχει τη μορφή $f(X) = b_0 + b_1 X^p + b_2 X^{2p} + \cdots + b_m X^{mp}$.

Απόδειξη:

(ι) Έστω $f(X) = a_0 + a_1 X + \cdots + a_n X^n$, $degf(X) = n \geq 1$.

Υποθέτουμε ότι δεν είναι διαχωρίσιμο.

Επομένως, $\xrightarrow{\text{Πρόταση 11}} \exists \ \ d(X) \in K[X],\ degd(X) \geq 1$

$d(X) | f(X)$ και $d(X) | f'(X)$.

Επειδή $f(X)$ ανάγωγο $\Rightarrow$ $d(X) = cf(X)$, $(c \in K)$ αλλά $degf'(X) \leq n-1$ οπότε για να ισχύει $f(X) | f'(X)$ θα πρέπει $f'(X) \equiv 0$:

$f'(X) = a_1 + 2a_2 X + \cdots + na_n X^{n-1} = 0 \ \Leftrightarrow \ (a_1 = 2a_2 = \cdots = na_n = 0)$

Αν $chK = 0$, τότε κατ' ανάγκη $a_1 = a_2 = \cdots = a_n = 0$, δηλαδή $f(X) = a_0$, άτοπο.

Άρα το $f(X)$ είναι διαχωρίσιμο.

(ιι) Υποθέτουμε τώρα ότι $chK = p$.

Επομένως $[ra_r = 0 \Rightarrow a_r = 0] \Leftrightarrow (p \nmid r)$

Οι μόνοι, μη-μηδενικοί όροι του $f(X)$ είναι αυτοί που είναι της μορφής $a_{kp} X^{kp}$ για $k = 0, 1, 2, \cdots$, δηλαδή το $f(X) = b_0 + b_1 X^p + b_2 X^{2p} + \cdots + b_m X^{mp}$.

Πόρισμα:

Κάθε σώμα χαρακτηριστικής μηδέν είναι τέλειο.

Χωρίς απόδειξη αναφέρουμε ότι:

Πρόταση 13η:

Κάθε πεπερασμένο σώμα είναι τέλειο. (Θα αποδειχθεί στις διαλέξεις των φοιτητών.)

Σημείωση: Ισχύει μάλιστα το εξής:
Ένα σώμα Κ, $chK = p$ είναι τέλειο $\Leftrightarrow\ K^p = K$.
Κάτι που προφανώς ισχύει για πεπερασμένα σώματα.
«Μεταβατικότητα» της διαχωρισιμότητας.

Πρόταση 14η:

Αν ${}^{L}/_{K}$ πεπερασμένη και διαχωρίσιμη επέκταση σωμάτων και Ε ενδιάμεσο σώμα αυτής, τότε και η ${}^{L}/_{E}$ είναι πεπερασμένη και διαχωρίσιμη.
Απόδειξη:
Έστω $a \in L,\ \ p(X) = Irr(a, K)$ και $q(X) = Irr(a, E)$.
Έχουμε ήδη παρατηρήσει, ότι το $q(X) \underset{E[X]}{|} p(X)$, δηλαδή
$p(X) = q(X) \cdot \pi(X),\ \ \pi(X) \in E[X]$.
Αν το $q(X)$ δεν ήταν διαχωρίσιμο τότε (Πρόταση 11) θα υπήρχε $f(X) \in E[X]$ τ.ω.
$(f(X) \neq$ σταθ.$)\ \ f(X)|q(X)$ και $f(X)|q'(X)$
Όμως $p(X) = q(X) \cdot \pi(X)\ \Rightarrow\ p'(X) = q'(X)\pi(X) + q(X)\pi'(X)$
Τότε βέβαια, θα είχαμε $f(X)|p(X)$ και $f(X)|p'(X)$, οπότε (Πρόταση 11) το $p(X)$ θα είχε ρίζα πολλαπλότητας > 1, (σε κάποιο σώμα ανάλυσης του), άτοπο, αφού $p(X)$ διαχωρίσιμο.

Παρατήρηση: Ισχύει γενικότερα η «μεταβατικότητα» της διαχωρισιμότητας.
$K \leq E \leq L,\ \ ({}^{L}/_{K}$ διαχωρίσιμη $)\ \Leftrightarrow\ ({}^{L}/_{E}$ και ${}^{E}/_{K}$ διαχωρίσιμη)
(δες, π.χ. Βιβλίο «Άλγεβρα» του Κ.Λάκκη)

4.4 Επεκτάσεις Galois

Ορισμός:

Μια πεπερασμένη επέκταση ${}^{L}/_{K}$ θα λέγεται επέκταση $Galois$ όταν είναι κανονική και διαχωρίσιμη.
Θα αποδείξουμε ότι, για μια επέκταση $Galois$, οι απεικονίσεις Γ και Φ είναι αμφιμονοσήμαντες.

Παραδείγματα:

1. Η επέκταση ${}^{\mathbb{C}}/_{\mathbb{R}}$ είναι $Galois$ αφού είναι κανονική, (το $\mathbb{C}$ σώμα ανάλυσης του $f(X) = X^2 + 1 \in \mathbb{R}[X]$, ή $[\mathbb{C} : \mathbb{R}] = 2$) και διαχωρίσιμη, αφού $ch\mathbb{R} = 0$
   Έχουμε ήδη δείξει ότι $[\mathbb{C} : \mathbb{R}] = \#(Aut({}^{L}/_{K}))$
2. $K = \mathbb{Q}$ και $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$
   Η επέκταση ${}^{L}/_{K}$ είναι κανονική και διαχωρίσιμη (αφού $chK = ch\mathbb{Q} = 0$)
   Άρα είναι $Galois$.
3. Η επέκταση ${}^{\mathbb{Q}(\sqrt[4]{2},i)}/_{\mathbb{Q}}$ είναι επίσης $Galois$.

Αν η επέκταση ${}^{L}/_{K}$ είναι $Galois$ τότε την $Aut({}^{L}/_{K})$ θα συμβολίζουμε ως $Gal({}^{L}/_{K})$ και θα λέμε ομάδα $Galois$ της επέκτασης αυτής.
Σκοπός μας είναι να αποδείξουμε ότι αν η ${}^{L}/_{K}$ είναι $Galois$ τότε $[L : K] = |Gal({}^{L}/_{K})|$, το οποίο όπως έχουμε παρατηρήσει πιο πριν, είναι ισοδύναμο με την έκφραση ότι
$K = \Phi(G) \mid G = Gal({}^{L}/_{K})$, δηλαδή ότι το Κ είναι ακριβώς το σώμα των σταθερών στοιχείων της G.
Τέλος, να παρατηρήσουμε ότι ο ορισμός, λόγω της Πρότασης 8, είναι ισοδύναμος προς τον:
(Η πεπερασμένη επέκταση ${}^{L}/_{K}$ είναι $Galois$) $\Leftrightarrow$ (Το L είναι σώμα ανάλυσης ενός διαχωρίσιμου υπέρ το Κ πολυωνύμου $f(X) \in K[X]$)

Πρόταση 15η:

Υποθέτουμε ότι η ${}^{L}/_{K}$ είναι διαχωρίσιμη επέκταση βαθμού $[L : K] = n$.
Υπάρχουν ακριβώς n, Κ-μονομορφισμοί του L σε μία κανονική θήκη του L υπέρ το Κ.

Απόδειξη:

Επαγωγικά, ως προς n.

Αν $[L:K]=1 \Rightarrow L=K=N$ (λόγω του ορισμού σελ.59, κάθε ανάγωγο $f(X)\in K[X]$ που έχει μια ρίζα του στο $K=L$, αναλύεται πλήρως στο K).

Επομένως, ο μόνος K-μονομορφισμός του K στο N=K είναι η ταυτότητα Id_K.

Υποθέτουμε ότι το συμπέρασμα της Πρότασης ισχύει για όλους τους φυσικούς $k\leq n-1$ και θα αποδείξουμε ότι ισχύει και για n, $[L:K]=n>1$

Έστω $a_1\in L\setminus K$ και $P(X)=Irr(a_1,K)$.

Προφανώς $degP(X)=r\geq 2 \;\; K\subsetneqq K(a_1)\leq L$

N είναι η κανονική θήκη του L υπέρ το K και το $a_1\in N \Rightarrow$ Το $P(X)$ αναλύεται πλήρως στο N.

Η ${}^{L}/_{K}$ είναι διαχωρίσιμη $\Rightarrow$ το $P(X)$ έχει απλές ρίζες.

Έστωσαν $a_1,a_2,\cdots,a_r$ οι ρίζες του $P(X)$ και έστω $[L:K(a_1)]=s, \;\; 1\leq s\leq n$ οπότε $r\cdot s=n$.

Το N είναι μια κανονική θήκη του L υπέρ το $K(a_1)$, οπότε λόγω της υπόθεσης της μαθηματικής επαγωγής υπάρχουν ακριβώς s, $K(a_1)$-μονομορφισμοί του L στο N, έστω $\sigma_1,\sigma_2,\cdots,\sigma_s$.

Από, Πόρισμα 2, σελ 61, έχουμε:

Υπάρχουν r (διακεκριμένοι) K-αυτομορφισμοί του N, έστω $\tau_1,\tau_2,\cdots,\tau_r$ και μάλιστα $\tau_i(a_1)=a_i \;\; \forall i=1,2,\cdots,r$.

Ορίζουμε τις συναρτήσεις $\Phi_{i,j}: L\to N$

$[\Phi_{ij}(a)=\tau_i(\sigma_j(a)) \;\; \forall i=1,2,\cdots,r, \;\; \forall j=1,2,\cdots,s]$

Οι ϕ_{ij} είναι K-μονομορφισμοί του L στο N.

Θα αποδείξουμε:(i) Ότι είναι όλοι διακεκριμένοι μεταξύ τους και (ii) ότι δεν υπάρχουν άλλοι.

(ι) $\phi_{ij}(a_1)=\tau_i(\sigma_j(a_1))=\tau_i(a_1)=a_i$.

Επομένως, αν $\phi_{ij}=\phi_{kl}$, τότε $i=k$ (αφού $\phi_{ij}(a_1)=a_i$ και $\phi_{kl}(a_1)=a_k$).

Έστω λοιπόν ότι $\phi_{ij}=\phi_{il}$.

Θα αποδείξουμε ότι $\forall a\in L$, ισχύει $\tau_i(\sigma_j(a))=\tau_i(\sigma_l(a))$.

Οι τ_i είναι 1-1. Συνεπώς $\sigma_j(a)=\sigma_l(a) \;\; \forall a\in L$.

Επομένως $j = l$

(ιι) Έστω ψ ένας K-μονομορφισμός του L στο N.

Θα αποδείξουμε ότι είναι κάποιος από τον ϕ_{ij}.

Ο ψ απεικονίζει το a_1, έστω στο a_i, $\psi(a_1) = a_i$.

Ορίζουμε $\chi : L \to N$ ως εξής: $\chi(a) := \tau_i^{-1}(\psi(a)),\ \forall a \in L$.

Ο χ είναι ένας K-μονομορφισμός του L στο N, αλλά

$\chi(a_1) = \tau_i^{-1}(\psi(a_1)) = \tau_i^{-1}(a_i) = a_1$, δηλαδή ο χ είναι $K(a_1)$-μονομορφισμός του L στο N.

Συνεπώς $\exists\, j \in \{1, 2, \cdots, s\}$ τ.ω. $\chi = \sigma_j$.

Για κάθε $a \in L$, έχουμε

$\sigma_j(a) = \tau_i^{-1}(\psi(a)) \ \Rightarrow\ \psi(a) = \tau_i(\sigma_j(a)) = \phi_{ij}(a) \ \Rightarrow\ \psi = \phi_{ij}$

Αν τώρα υποθέσουμε ότι η ${}^{L}/_{K}$ είναι διαχωρίσιμη αλλά και κανονική, δηλαδή $N = L$, τότε έχουμε:

Πόρισμα:

Αν η επέκταση ${}^{L}/_{K}$ είναι *Galois* τότε $[L : K] = |G|$, $G := Gal({}^{L}/_{K})$

Πρόταση 16η:

Έστω ${}^{L}/_{K}$ πεπερασμένη επέκταση σωμάτων.

(Ισχύει $\Phi(Gal({}^{L}/_{K}) = K) \ \Leftrightarrow$ (το L είναι διαχωρίσιμη και κανονική επέκταση του K)

Απόδειξη:

Υποθέτουμε ότι η ${}^{L}/_{K}$ είναι διαχωρίσιμη και κανονική και έστω $[L : K] = n$.

Από το Πόρισμα της Πρότασης 15, έπεται ότι $|Gal({}^{L}/_{K})| = n$.

Αν $E := \Phi(Gal({}^{L}/_{K}))$, τότε, Πρόταση 6, $K \leq \Phi(\Gamma(K)) = \Phi(Gal({}^{L}/_{K})) =: K'$

Λόγω της Πρότασης 7,

$[L : K'] = [L : \Phi(Gal({}^{L}/_{K}))] = [L : K'] = |Gal({}^{L}/_{K})| = n = [L : K]$

Συνεπώς $K' = K$

Αντίστροφα " $\Rightarrow$ ", έστω $K' := \Phi(Gal({}^{L}/_{K})) = K$ και έστω

$Gal({}^{L}/_{K}) = \{Id_L, \sigma_2, \cdots, \sigma_n\}$.

Υποθέτουμε ότι το ανάγωγο πολυώνυμο $f(X) \in K[X]$ έχει μια ρίζα $a \in L$.

Κάποιοι αυτομορφισμοί κρατούν το a σταθερό και κάποιοι άλλοι όχι.

Ας υποθέσουμε ότι οι $\sigma_1, \sigma_2, \cdots, \sigma_r$ δίδουν διαφορετικές εικόνες του a, έστω λοιπόν ότι $\sigma_i(a) = a_i \ \ (a_1 = a) \ \ (i = 1, 2, \cdots, r)$

Λήμμα 1ο:

Για κάθε $\sigma_j \in Gal(^L/_K)$ τα σύνολα $\{a_1, a_2, \cdots, a_r\}$ και $\{\sigma_j(a_1), \sigma_j(a_2), \cdots, \sigma_j(a_r)\}$ είναι ίσα.

Απόδειξη του λήμματος:

Το $\sigma_j(a_i) = (\sigma_j \circ \sigma_i)(a), \quad \sigma_j \circ \sigma_i \in Gal(^L/_K)$ συνεπώς η εικόνα του $a, (\sigma_j \circ \sigma_i)(a)$ θα είναι πάλι μια ρίζα του $f(X)$, δηλαδή $(\sigma_j \circ \sigma_i)(a) = a_k \ \Rightarrow \ \sigma_j(a_i) = a_k$.

Επειδή οι σ_j είναι 1-1, μεταθέτουν τις ρίζες $a_1, a_2, \cdots, a_r$.

Έστω τώρα $g(X) := (X - a_1)(X - a_2) \cdots (X - a_r) = X^r - b_1 X^{r-1} + \cdots + (-1)^r b_r$.

Οι συντελεστές $b_1 = \sum_{i=1}^{r}(a_i), \ \ b_2 = \sum_{i \neq j} a_i \cdot a_j$ και $b_r = a_1 a_2 \cdots a_r$ είναι οι στοιχειώδεις συμμετρικές συναρτήσεις τνω ριζών $a_1, a_2, \cdots, a_r$.

Άρα θα παραμένουν σταθεροί για κάθε $\sigma_j \in Gal(^L/_K)$.

Συνεπώς το $g(X)$ έχει συντελεστές στο $\Phi(Gal(^L/_K))$.

Όμως εξ υποθέσεως, $\Phi(Gal(^L/_K)) = K$, δηλαδή $f(X) \in K[X]$.

Λήμμα 2ο:

Το $g(X) \in K[X]$, είναι το ανάγωγο πολυώνυμο του a υπέρ το K.

Απόδειξη:

Θα αποδείξουμε ότι για κάθε $h(X) \in K[X]$ τ.ω. $h(a) = 0$, ισχύει: $g(X)|h(X)$.

Έστω $h(X) = c_0 + c_1 X + \cdots + c_m X^m \ \in K[X]$ τ.ω. $h(a) = 0$, δηλαδή

$c_0 + c_1 a + \cdots + c_m a^m = 0 \ \ \Rightarrow \ \ c_0 + c_1 \sigma_j(a) + \cdots + c_m \sigma_j(a)^m = 0 \ \ \forall \sigma_j \ \ (j = 1, 2, \cdots, r) \ \ \Rightarrow \ \ c_0 + c_1 a_j + \cdots + c_m a_j^m = 0$

Επομένως το πολυώνυμο $h(X)$ διαιρείται από τα $(X - a_1), (X - a_2), \cdots, (X - a_{rr})$ και επειδή $a_i \neq a_j \ \ \forall i \neq j$ και από το γινόμενο τους, δηλαδή $g(X)|h(X)$.

Τώρα το $a \in L$ είναι ρίζα του $g(X) \in K[X]$ και $g(X) = Irr(a, K)$.

Επομένως το $g(X)|f(X)$.

Είχαμε όμως υποθέσει ότι το $f(X) = Irr(a, K)$, άρα $f(X) = a \cdot g(X), \ \ a \in K$.

Το πολυώνυμο $g(X)$ αναλύεται πλήρως στο L, άρα και το $f(X)$.

Το $f(X)$ έχει διακεκριμένες ρίζες, αφού διακεκριμένες είναι οι ρίζες του $g(X)$, άρα είναι διαχωρίσιμο $\Rightarrow$ $^L/_K$ είναι μια διαχωρίσιμη και κανονική επέκταση του K.

Πρόταση 17η:

Έστω $^L/_K$ είναι (πεπερασμένη) επέκταση $Galois$ και E ένα ενδιάμεσο σώμα.

Αν $\sigma \in Gal(^L/_K)$ τότε $\Gamma(\sigma(E)) = \sigma\Gamma(E)\sigma^{-1}$.

Απόδειξη:

Έστω $\sigma(E) = E', \quad \Gamma(E) := H, \quad \Gamma(E') := H'$.

Θα πρέπει να αποδείξουμε ότι: $H' = \sigma H \sigma^{-1}$.

Έστω $\tau \in H$. Θα αποδείξουμε ότι $\sigma\tau\sigma^{-1} \in H'$.

Αν $a' \in E'$ τότε $\exists \ ! \ a \in E$ τ.ω. $\sigma(a) = a'$

$\tau \in H = \Gamma(E)$.

Επομένως $(\tau(a) = a \quad \forall a \in E)$, δηλαδή $\sigma\tau\sigma^{-1}(a') = \sigma\tau(a) = \sigma(a) = a'$ [Αυτό ισχύει $\forall a' \in E'] \ \Rightarrow \ \sigma\tau\sigma^{-1} \in H' \ \Rightarrow \ \sigma H \sigma^{-1} \leq H'$.

Έστω τώρα $\sigma' \in H'$ και $a \in E$, άρα $\sigma(a) \in E' = \sigma(E)$ και συνεπώς $\sigma'(\sigma(a)) = \sigma(a)$.

Επομένως $(\sigma^{-1}\sigma'\sigma)(a) = \sigma^{-1}\sigma'(\sigma(a)) = \sigma^{-1}(\sigma(a)) = a$, δηλαδή

$\sigma^{-1}\sigma'\sigma \in H = \Gamma(E) \ \Rightarrow \ \sigma^{-1}H'\sigma \leq H \ \Rightarrow \ H' \leq \sigma H \sigma^{-1}$.

Τελικά $\sigma H \sigma^{-1} = H'$

4.5 Το Θεμελιώδες Θεώρημα της Θεωρίας Galois

Θεώρημα:

Υποθέτουμε ότι ${}^{L}/_{K}$ είναι μια πεπερασμένη κανονική και διαχωρίσιμη επέκταση σωμάτων.

(ι) Για όλα τα ενδιάμεσα σώματα E, $K \leq E \leq L$ και όλες τις υποομάδες $H \leq G := Gal({}^{L}/_{K})$ ισχύουν: $\Phi(\Gamma(E)) = E$ και $\Gamma(\Phi(H)) = H$.
Επομένως $|\Gamma(E)| = [L : E]$ και $[E : K] = \frac{|G|}{|\Gamma(E)|}$.
Η ${}^{L}/_{E}$ είναι πάντοτε επέκταση $Galois$.

(ιι) Η ${}^{E}/_{K}$ είναι $Galois$ (κανονική, αφού, ούτως ή άλλως είναι διαχωρίσιμη)
$\Leftrightarrow \Gamma(E) \trianglelefteq G = Gal({}^{L}/_{K})$.
Στην περίπτωση αυτή $Gal({}^{E}/_{K}) \cong {}^{G}/_{\Gamma(E)}$

Απόδειξη:

(ι) Έστω Ε ένα ενδιάμεσο σώμα της ${}^{L}/_{K}$, $K \leq E \leq L$.
Γνωστό, (άσκηση), η ${}^{L}/_{E}$ είναι κανονική.
Επίσης, Πρόταση 14, η ${}^{L}/_{E}$ είναι διαχωρίσιμη.
Συνεπώς η ${}^{L}/_{E}$ είναι $Galois$ και επομένως (Πόρισμα στην Πρόταση 15, σελ 70)
$|\Gamma(E)| = [L : E]$.
Άρα $[E : K] = [L : K]/[L : E] = \frac{|G|}{|\Gamma(E)|}$.
Η $\Gamma(E) = Gal({}^{L}/_{E}) \xRightarrow{\text{Πρόταση 16}} \Phi(\Gamma(E)) = E$.
Έστω τώρα $H \leq G := Gal({}^{L}/_{K})$.
Από, Πρόταση 6, έπεται ότι $H \leq \Gamma(\Phi(H)) =: H'$.
Από την άσκηση 2, φυλλάδιο 6^o, έπεται ότι $\Phi(H) = \Phi(\Gamma(\Phi(H))) = \Phi(H')$.
Η πρόταση 7 τώρα μας δίνει: $|H| = [L : \Phi(H)]$ και $|H'| = [L : \Phi(H')]$.
Επειδή $\Phi(H) = \Phi(H')$, έπεται ότι $[L : \Phi(H)] = [L : \Phi(H')] \Rightarrow |H| = |H'|$.
Έχουμε και $H \leq H'$ (είναι και πεπερασμένες) άρα $H' = H$, δηλαδή $H = \Gamma(\Phi(H))$.

(ιι) " $\Rightarrow$ " Υποθέτουμε ότι η ${}^{E}/_{K}$ είναι κανονική.
Έστω $\sigma \in G = Gal({}^{L}/_{K})$ και $t := Res_{|_E}\sigma$, $t : E \to L$, είναι μονομορφισμός σωμάτων και ${}^{L}/_{K}$ είναι κανονική.
Λόγω της Πρότασης 10, ο $t \in Gal({}^{L}/_{K})$.

Τώρα, $\sigma(E) = t(E) = E$, οπότε, λόγω της Πρόταση 16,

$\Gamma(E) = \Gamma(\sigma(E)) = \sigma\Gamma(E)\sigma^{-1}$, δηλαδή $\Gamma(E) \trianglelefteq G := Gal({}^{L}/_{K})$.

" $\Leftarrow$ " Τώρα υποθέτουμε ότι $\Gamma(E) \trianglelefteq Gal({}^{L}/_{K})$.

Έστω t ένας K-μονομορφισμός του $E \leftarrow L$.

Αυτός μπορεί (Πόρισμα 1 της Πρότασης 8) να επεκταθεί σε κάποιον K-αυτομορφισμό του L, έστω σ.

Λόγω της υπόθεσης ότι $\Gamma(E) \trianglelefteq Gal({}^{L}/_{K})$, έχουμε $\sigma\Gamma(E)\sigma^{-1} = \Gamma(E)$.

Από Πρόταση 16, $\Gamma(\sigma(E)) = \sigma\Gamma(E)\sigma^{-1}$.

Συνεπώς $\Gamma(\sigma(E)) = \Gamma(E)$.

Στο πρώτο μέρος (i) της απόδειξης του θεωρήματος, αποδείξαμε ότι η Γ είναι αμφιμονοσήμαντη.

Επομένως $\sigma(E) = E$.

Επειδή $t = Res_E\sigma$, έπεται ότι $t(E) = E$, δηλαδή ότι (t είναι ένας K-αυτομορφισμός του E).

Η Πρόταση 10, τώρα μας δίνει: ${}^{E}/_{K}$ είναι κανονική.

Τέλος, θα πρέπει να αποδείξουμε ότι, αν ${}^{E}/_{K}$ κανονική τότε

$Gal({}^{E}/_{K}) \cong {}^{Gal({}^{L}/_{K})}/_{\Gamma(E)}$.

Αν $\sigma \in Gal({}^{L}/_{K})$, έστω $t := Res_E\sigma \cdot {}^{E}/_{K}$ κανονική, συνεπώς $t \in Gal({}^{E}/_{K})$.

Ορίζουμε $\phi : Gal({}^{L}/_{K}) \to Gal({}^{E}/_{K})$ όπου $\sigma \longmapsto t = Res_E\sigma$.

Ο φ είναι επιμορφισμός ομάδων. (άσκηση)

Ο $Ker\phi = \{\sigma \in Gal({}^{L}/_{K}) \mid \phi(\sigma) = Id_E\} = \{\sigma \in Gal({}^{L}/_{K}) \mid t := Res_E\sigma = Id_E\} = \{\sigma \in Gal({}^{L}/_{K}) \mid \sigma(a) = a \ \ \forall a \in E\} = \Gamma(E)$.

Άρα ${}^{Gal({}^{L}/_{K})}/_{\Gamma(E)} \cong Gal({}^{E}/_{K})$

Ερώτημα:

Αν τώρα ${}^{L}/_{K}$ (πεπερασμένη) επέκταση *Galois* και $H_1, H_2 \leq G = Gal({}^{L}/_{K})$ τότε σε ποιο σώμα αντιστοιχεί η $H_1 \cap H_2$?

Αν πάλι E_1, E_2 ενδιάμεσα σώματα της επέκτασης ${}^{L}/_{K}$ σε ποια ομάδα αντιστοιχεί η $E_1 \cap E_2$?

Παρατήρηση:

Αν $H_1, H_2 \leq G$, G ομάδα, η τομή $H_1 \cap H_2$ είναι πάντοτε ομάδα.

Η ένωση δύο υποομάδων $H_1 \cup H_2$ δεν είναι πάντοτε υποομάδα της G. Η ελάχιστη

υποομάδα της G που περιέχει τις H_1 και H_2 θα συμβολίζεται $H_1 \vee H_2$ και θα λέγεται η σύνθεση των $H_i \quad (i = 1, 2)$

(Αποδεικνύεται ότι τα στοιχεία της $H_1 \vee H_2$ είναι πεπερασμένα γινόμενα της μορφής $a_1\beta_1 a_2\beta_2 \cdots a_n\beta_n$ για όλα τα n όπου $a_i \in H_1$ και τα $\beta_j \in H_2$)

Αν μια τουλάχιστον από τις δύο είναι κανονική τότε η σύνθεση

$H_1 \vee H_2 = H_1 \cdot H_2 = \{a \cdot \beta \ / \ a \in H_1, \ \beta \in H_2\}$.

Αντίστοιχα για τα σώματα, έχουμε ήδη ορίσει την σύνθεση δύο ενδιάμεσων σωμάτων E_1, E_2 της ${}^{L}/_{K}$.

Το $E_1 \vee E_2$ εδώ το γράφουμε $E_1 \cdot E_2$ και εννοούμε το ελάχιστο ενδιάμεσο σώμα της ${}^{L}/_{K}$ το οποίο περιέχει τα E_1, E_2

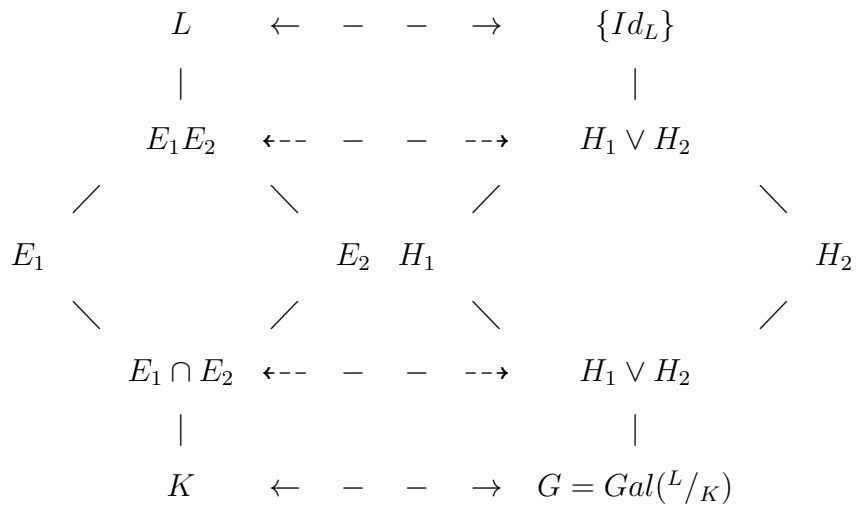
Πρόταση 17η:

Έστω ${}^{L}/_{K}$ πεπερασμένη επέκταση $Galois$ με $G := Gal({}^{L}/_{K})$ και E_1, E_2 δύο ενδιάμεσα σώματα της ${}^{L}/_{K}$.

Αν $\Gamma(E_i) = H_i \mid i = 1, 2$ τότε

1. $\Gamma(E_1 \cap E_2) = H_1 \vee H_2$ και
2. $\Gamma(E_1 \vee E_2) := \Gamma(E_1E_2) = H_1 \cap H_2$

Απόδειξη:



1. $E_1 \leq E_1 \vee E_2 = E_1E_2 \ \Rightarrow \ \Gamma(E_1E_2) \leq \Gamma(E_1) = H_1$

   Έπίσης, $\Gamma(E_1E_2) \leq \Gamma(E_2) = H_2$

Επομένως $\Gamma(E_1E_2) \leq H_1 \cap H_2$

Έστω τώρα $\sigma \in H_1 \cap H_2 \ \Rightarrow \ \sigma \in H_1$ και $\sigma \in H_2$.

Αφού $\sigma \in H_1 = \Gamma(E_1)$, έπεται ότι, $\forall a \in E_1$ ισχύει $\sigma(a) = a$

Επίσης $\sigma \in H_2 = \Gamma(E_2) \ \Rightarrow \ \forall \beta \in E_2, \ \ \sigma(\beta) = \beta$

Το E_1E_2 είναι το σύνολο όλων των πηλίκων πεπερασμένου πλήθους γραμμικών συνδυασμών (με συντελεστές από το E_1) πεπερασμένων γινομένων στοιχείων του E_2

Επομένως, $\forall \gamma \in E_1E_2$, ισχύει $\sigma(\gamma) = \gamma$, δηλαδή

$\sigma \in \Gamma(E_1E_2) \ \Rightarrow \ H_1 \cap H_2 \leq \Gamma(E_1 \cdot E_2)$ και τελικά η ισότητα.

2. Εντελώς όμοια, αφού $E_1 \cap E_2 \leq E_i \quad (i = 1, 2)$

$H_i = \Gamma(E_i) \leq \Gamma(E_1 \cap E_2) \quad (i = 1, 2)$

Συνεπώς $H_1 \vee H_2 \leq \Gamma(E_1 \cap E_2) \quad (1)$

Έστω τώρα $a \in L \setminus E_1 \cap E_2$

Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $a \notin E_1$.

Η $H_1 = \Gamma(E_1) = \{\sigma \in G \ / \ \sigma(\beta) = \beta, \ \ \forall \beta \in E_1\}$

Επομένως, $(\exists \ \ \sigma \in H_1 \ \ \text{τ.ω.} \ \ \sigma(a) \neq a)$

Τώρα, επειδή $H_1 \leq H_1 \vee H_2$, έχουμε $(\exists \ \ \sigma \in H_1 \vee H_2 \ \text{τ.ω.} \ \ \sigma(a) \neq a)$

Άρα $a \notin \Phi(H_1 \vee H_2)$

Αποδείξαμε λοιπόν ότι $[a \notin E_1 \cap E_2 \ \Rightarrow \ a \notin \Phi(H_1 \vee H_2)]$

Αυτό σημαίνει ότι $\Phi(H_1 \vee H_2) \leq E_1 \cap E_2$

$\Rightarrow \ \Gamma(E_1 \cap E_2) \leq \Gamma(\Phi(H_1 \vee H_2)) = H_1 \vee H_2 \quad (2)$

Οι σχέσεις (1)και (2) $\Rightarrow \ \Gamma(E_1 \cap E_2) = H_1 \vee H_2$.

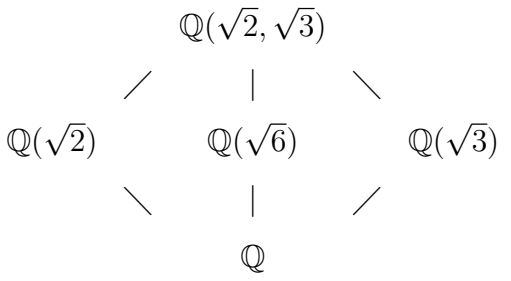
Παραδείγματα:

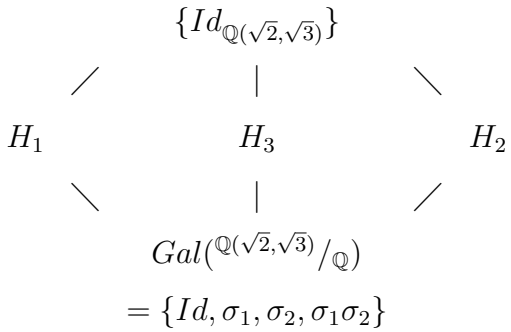
1. $K = \mathbb{Q}, \quad L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

2. $K = \mathbb{Q}, \quad L = \mathbb{Q}(\sqrt[3]{2}, \omega)$

3. $K = \mathbb{Q}, \quad L = \mathbb{Q}(\sqrt[4]{2}, i)$

1. Στο (1) αποδείξαμε την αντιστοιχία





όπου

$H_1 =< \sigma_1 > \quad \sigma_1 := \{\sqrt{2} \to \sqrt{2} \text{ και } \sqrt{3} \to \sqrt{3}\}$

$H_2 =< \sigma_2 > \quad \sigma_2 := \{\sqrt{2} \to \sqrt{2} \text{ και } \sqrt{3} \to \sqrt{3}\}$

$H_3 =< \sigma_1 \cdot \sigma_2 >$

2. Η επέκταση $^L/_{\mathbb{Q}}$ είναι $Galois$.

   Αν $\sigma \in Gal(^L/_{\mathbb{Q}})$, ο σ καθορίζεται πλήρως από τις τιμές στους $\sqrt[3]{2}$ και ω.

   Το $\sigma(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$

   και αφού $Irr(\omega, \mathbb{Q}) = X^2 + X + 1$ το οποίο έχει ρίζες τα ω, ω^2, έπεται ότι

   $\sigma(\omega) \in \{\omega, \omega^2\}$.

   Συνολικά έχουμε 6 - δυνατότητες, όσο φυσικά και ο βαθμός της επέκτασης $[L : \mathbb{Q}]$.

   Έστωσαν $\sigma : \left\{ \begin{array}{l} \sqrt[3]{2} \longmapsto \omega\sqrt[3]{2} \\ \omega \longmapsto \omega \end{array} \right\}$ και $\tau : \left\{ \begin{array}{l} \sqrt[3]{2} \longmapsto \sqrt[3]{2} \\ \omega \longmapsto \omega^2 \end{array} \right\}$

   Υπολογίζουμε: $\sigma^2 : \left\{ \begin{array}{l} \sqrt[3]{2} \longmapsto \omega^2\sqrt[3]{2} \\ \omega \longmapsto \omega \end{array} \right\}$ και $\sigma^3 : \left\{ \begin{array}{l} \sqrt[3]{2} \longmapsto \sqrt[3]{2} \\ \omega \longmapsto \omega \end{array} \right\}$

   δηλαδή $\sigma^3 = Id_L$.

   Επίσης $\tau^2 : \left\{ \begin{array}{l} \sqrt[3]{2} \longmapsto \sqrt[3]{2} \\ \omega \longmapsto \omega \end{array} \right\}$ δηλαδή $\tau^2 = Id_L$.

   Η ομάδα $Gal(^L/_{\mathbb{Q}})$, περιέχει σαν υποομάδα την $\{Id_L, \sigma, \sigma^2\}$ και επειδή

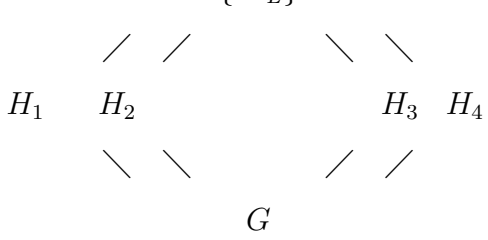
   $\tau \notin \{Id_L, \sigma, \sigma^2\}$ θα περιέχει και το $coset$ (σύμπλοκο) $\{\tau, \sigma\tau, \sigma^2\tau\}$

Συνεπώς: $Gal(^L/_{\mathbb{Q}}) = \{Id_L, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$

Κάθε υποομάδα αυτής, διάφορη της $\{Id_L\}$ και της $Gal(^L/_{\mathbb{Q}})$, θα έχει τάξη 2 ή 3 $\in \mathbb{P}$ θα είναι κατ΄ ανάγκη κυκλική.

Επομένως όλες οι υποομάδες της G θα είναι: $G, \{Id_L, \sigma, \sigma^2\} = H_1$,

$\{Id_L, \tau\} = H_2, \quad \{Id_L, \tau\sigma\} = H_3, \quad \{Id_L, \tau\sigma^2\} = H_4, \quad \{Id_L\}.$



Πώς θα βρούμε τα αντίστοιχα σώματα ;

<u>Αναλυτικά:</u>

Μια βάση της $^L/_{\mathbb{Q}}$ είναι η $B = \{1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \omega\sqrt[3]{2}, \omega\sqrt[3]{4}\}$

Ας πάρουμε την $H_3 = \{Id_L, \tau\sigma\}$

Υπολογίζουμε: $\left\{ \begin{array}{l} \tau\sigma(\sqrt[3]{2}) = \omega^2\sqrt[3]{2} \\ \tau\sigma(\omega) = \omega^2 \end{array} \right\}$ και θυμόμαστε ότι, $\omega^2 = -\omega - 1$.

Αν $a \in L, \quad a = a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\omega + e\omega\sqrt[3]{2} + f\omega\sqrt[3]{4}$

$a \in \Phi(H_3) \Leftrightarrow (\tau\sigma)(a) = a$

$\Leftrightarrow a + b(-\sqrt[3]{2} - \omega\sqrt[3]{2}) + c\omega\sqrt[3]{4} + d(-1-\omega) + e\omega\sqrt[3]{2} + f\sqrt[3]{4} =$

$a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\omega + e\omega\sqrt[3]{2} + f\omega\sqrt[3]{4}$

$$\Leftrightarrow \left\{ \begin{array}{l} a - d = a \\ -b = b \\ c = f \\ -d = d \\ e - b = e \\ f = c \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} d = 0 \\ b = 0 \\ f = c \end{array} \right\}$$

$\Leftrightarrow a = a + c\sqrt[3]{4} + e\omega\sqrt[3]{2} + c\omega\sqrt[3]{4}$

$= a + c(a+\omega)\sqrt[3]{4} + e\omega\sqrt[3]{2}$

$= a - c\omega^2\sqrt[3]{4} + e\omega\sqrt[3]{2}$

$\Leftrightarrow a \in \mathbb{Q}(\omega\sqrt[3]{2})$

<u>Πρακτικά:</u>

Προφανές ότι $\Phi(H_1) = \mathbb{Q}(\sqrt[3]{2})$ και $\Phi(H_2) = \mathbb{Q}(\omega)$

Τώρα για την H_3, παρατηρούμε ότι

$(\tau\sigma)(\omega\sqrt[3]{2}) = \omega^2 \cdot \omega^2\sqrt[3]{2} = \omega\sqrt[3]{2} \Rightarrow \mathbb{Q}(\omega\sqrt[3]{2}) \leq \Phi(H_3)$

Όμως από τι Θεμελιώδες Θεώρημα της Θεωρίας του $Galois$

$[\Phi(H_3) : \mathbb{Q}] = [G : H_3] = 3$ και επειδή $[\mathbb{Q}(\omega\sqrt[3]{2}) : \mathbb{Q}] = 3$, έπεται ότι

$\Phi(H_3) = \mathbb{Q}(\omega\sqrt[3]{2})$.

Ερώτημα:

Ποια είναι η ομάδα του $Galois$ $Gal({}^{L}/_{\mathbb{Q}})$???

(εννοώ κατά προσέγγιση ισομορφίας)

Επειδή $\sigma\tau = \tau\sigma^2$, έπεται ότι η ομάδα $G \cong D_3 = \{\sigma, \tau \mid \sigma^3 = 1, \tau^2 = 1, \sigma\tau = \tau\sigma^2\}$ είναι δίεδρη ομάδα D_3.

Βέβαια είναι γνωστό ότι, για $n = 3$ η $D_3 \cong S_3$,την συμμετρική ομάδα τριών στοιχείων.

Χωρίς απόδειξη αναφέρουμε:

Πρόταση 18η:

(Θεώρημα της μεταφοράς)

Έστωσαν ${}^{L}/_{K}$ επέκταση σωμάτων και E_1, E_2 ενδιάμεσα σώματα της επέκτασης αυτής.

Υποθέτουμε ότι η ${}^{E_1}/_{K}$ είναι $Galois$.

Τότε και η ${}^{E_1 \cdot E_2}/_{E_2}$ είναι επέκταση $Galois$ και μάλιστα

$Gal({}^{E_1 \cdot E_2}/_{E_2}) \cong$ (προς υποομάδα της $Gal({}^{E_1}/_{K})$), έστω H.

Επιπλέον ισχύει $\Phi(H) = E_1 \cap E_2$.

$$\begin{array}{ccccc} & & E_1 & - & E_1 \cdot E_2 & & \\ & \diagup & | & & | & \diagdown & Galois \\ Galois & & E_1 \cap E_2 & - & E_2 & \diagup & \\ & \diagdown & | & \diagup & & & \\ & & K & & & & \end{array}$$

Πόρισμα:

Αν ${}^{E_1}/_{K}$ επέκταση $Galois$ και ${}^{E_2}/_{K}$ (οποιαδήποτε) επέκταση του K, τότε

$[E_1E_2 : E_2] \mid [E_1 : K]$.

Κεφάλαιο 5

ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΘΕΩΡΙΑΣ GALOIS

5.1 Μερικά στοιχεία Θεωρίας Ομάδων

5.1.1 ΑΒΕΛΙΑΝΕΣ ΟΜΑΔΕΣ

(Στις αβελιανές ομάδες συμβολίζουμε την πράξη, συνήθως, προσθετικά.)
Έστω λοιπόν $(A, +)$ πεπερασμένη αβελιανή ομάδα.
Αν $H_1, H_2, \cdots H_k \leq A$ τότε:

Ορισμός:

(Η A θα λέγεται ευθύ άθροισμα των H_i, $(i = 1, 2, \cdots, k) : \Leftrightarrow$ (κάθε $a \in A$ έχει μοναδική παράσταση της μορφής $a = h_1 + h_2 + \cdots + h_k$, $h_i \in H_i$)

Παρατήρηση: Αν η A είναι το ευθύ άθροισμα των H_i $i = 1, 2, \cdots, k$, τότε κατ΄ ανάγκη, $H_i \cap H_j = \{0\}$ $\forall i \neq j$.
(Πράγματι, αν $a \in H_i \cap H_j$ και $a \neq 0$, τότε το a θα έχει δύο διαφορετικές μεταξύ τους παραστάσεις: Μία στη θέση "i" a και στη θέση "j" o και μία αντίστροφα.

Συμβολισμός για το ευθύ άθροισμα:
$A = H_1 \bigoplus H_2 \bigoplus \cdots \bigoplus H_k$. (*)

Παρατήρηση: Αν (*) και $h_1 + h_2 + \cdots + h_k = 0 \Rightarrow h_i = 0 \quad \forall i = 1, 2, \cdots, k$
(Αλλιώς το μηδέν θα είχε δύο διαφορετικές μεταξύ τους παραστάσεις.)

Πρόταση 1η:

Αν Α πεπερασμένη, αβελιανή και $a \in A$, με $ord(a) = m \cdot n$, όπου $(m, n) = 1$, τότε υπάρχουν μονοσήμαντα ορισμένα β και γ$\in A$ με $ord(\beta) = m$ και $ord(\gamma) = n$ τ.ω.
$a = \beta + \gamma$
Απόδειξη:

1. ύπαρξη
   Έστω $\beta' = na$ και $\gamma' = ma$.
   Προφανώς $ord(\beta') = m$ και $ord(\gamma') = n$.
   Λόγω της υπόθεσης ότι $(m, n) = 1 \Rightarrow \exists s, t \in \mathbb{Z}$ τ.ω. $sm + tn = 1$.
   Επομένως, $a = a \cdot 1 = a(sm + tn) = t(n \cdot a) + s(m \cdot a) = t \cdot \beta' + s \cdot \gamma'$
   Παρατηρούμε ότι ΜΚΔ$(t, m) = 1$ και ΜΚΔ$(s, n) = 1$.
   Συνεπώς $ord(t\beta') = m$ και $ord(s\gamma') = n$
   Θέτουμε $\beta := t\beta'$ και $\gamma := s\gamma'$ και έχουμε $a = \beta + \gamma$, με $ord(\beta) = m, \ \ ord(\gamma) = n$

2. μοναδικότητα
   Αν $a = \beta_1 + \gamma_1 = \beta_2 + \gamma_2$ με $ord(\beta_1) = ord(\beta_2) = m$ και $ord(\gamma_1) = ord(\gamma_2) = n$
   Έστω, $d := \beta_1 - \beta_2 = \gamma_1 - \gamma_2$
   Επομένως $md = m\beta_1 - m\beta_2 = 0$ και $nd = n\gamma_2 - n\gamma_1 = 0$
   Συνεπώς $ord(d) \mid m$ και $ord(d) \mid n \Rightarrow ord(d) \mid (m, n) = 1 \Rightarrow ord(d) = 1$. Σε προσθετική αβελιανή ομάδα, αυτό σημαίνει ότι το d είναι το ουδέτερο στοιχείο αυτής, δηλαδή ότι $d = 0$ και επομένως $\beta_1 = \beta_2$ και $\gamma_1 = \gamma_2$

Πόρισμα:

Έστω Α πεπερασμένη αβελιανή ομάδα.

Αν $a \in A$ και $ord(a) = m_1 m_2 \cdots m_r$ όπου $(m_i, m_j) = 1, \quad \forall i \neq j$, τότε το a γράφεται μονοσήμαντα σαν $a = a_1 + a_2 + \cdots + a_r$, με $ord(a_i) = m_i$

Απόδειξη: Επαγωγικά ως προς r

Πρόταση 2η:

Έστω Α αβελιανή ομάδα τάξης $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}, \quad (p_i \in \mathbb{P}, \quad p_i \neq p_j \quad \forall i \neq j)$

Αν $H_i = \{a \in A \mid ord(a) = \text{δύναμη του} p_i\}$, τότε $H_i \leq A$

Απόδειξη:

Έστωσαν $a, \beta \in H_i$ και ότι $ord(a) = p_i^k, \quad ord(\beta) = p_i^l$

Προφανώς $p_i^m(a - \beta) = 0$, για κάθε

$m \geq max\{k, l\} \Rightarrow ord(a - \beta) \mid p_i^m \Rightarrow ord(a - \beta) = \text{δύναμη του} p_i \Rightarrow a - \beta \in H_i$,

δηλαδή $H_i \leq A$

Πρόταση 3η:

Κάθε πεπερασμένη και αβελιανή ομάδα Α γράφεται σαν ευθύ άθροισμα αβελιανών p-ομάδων.

Απόδειξη:

Έστω ότι η τάξη της Α είναι: $ord(A) = n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$

Αν $a \in A$ τότε $ord(a) \mid ord(A)$, συνεπώς $ord(a) = p_1^{d_1} p_2^{d_2} \cdots p_s^{d_s}$, για

$0 \leq d_i \leq a_i \quad i = 1, 2, \cdots, s$

Από το Πόρισμα της Πρότασης 1, έπεται ότι $a = a_1 + a_2 + \cdots + a_s$, (μονοσήμαντα) με $ord(a_i) = p_i^{d_i}$

Επομένως, $A = H_1 \bigoplus H_2 \bigoplus \cdots \bigoplus H_s$

Θεώρημα:

(Θεμελιώδες Θεώρημα των πεπερασμένων αβελιανών ομάδων.)

Κάθε πεπερασμένη αβελιανή ομάδα Α αναλύεται πάντοτε σε ευθύ άθροισμα κυκλικών ομάδων.

(χωρίς απόδειξη)

Παρατήρηση: Για την απόδειξη του Θεωρήματος, αρκεί η περίπτωση που η A είναι μια p-ομάδα.

Παράδειγμα:

Ποιες είναι οι δυνατές αβελιανές ομάδες τάξης 5^3 ;

Απάντηση: (εδώ τις γράφουμε πολλαπλασιαστικά)

$\frac{\mathbb{Z}}{5^3\mathbb{Z}}, \quad \frac{\mathbb{Z}}{5\mathbb{Z}} \times \frac{\mathbb{Z}}{25\mathbb{Z}}, \quad \frac{\mathbb{Z}}{5\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}}$

5.1.2 SYLOW ΥΠΟΟΜΑΔΕΣ

Πρόταση 4η:

Έστω τώρα G πεπερασμένη ομάδα (όχι κατ' ανάγκη πλέον αβελιανή).

Αν $|G| = p^n \cdot m$, όπου $p \in \mathbb{P}, \quad n \geq 1$ και $p \nmid m$, τότε υπάρχει πάντοτε μια (τουλάχιστον) υποομάδα $H \leq G$ τ.ω. $|H| = p^n$

(χωρίς απόδειξη)

Ορισμός:

Κάθε τέτοια υποομάδα H της G θα λέγεται μια $p - Sylow$ υποομάδα της G

Πόρισμα:

Αν G πεπερασμένη ομάδα και $p \in \mathbb{P}$ τ.ω. $p||G|$, τότε υπάρχει $a \in G$ τ.ω. $ord(a) = p$.

(Λέγεται και θεώρημα του $Cauchy$).

Απόδειξη:

Αν $|G| = p^n \cdot m$, τότε $\xrightarrow{\text{Πρόταση 3}} \quad \exists H \leq G, \quad |H| = p^n$.

Έστω $a \in H, \quad (a \neq 1) \quad ord(a) \mid |H| = p^n$.

Άρα, $ord(a) = p^k$ για κάποιο $k \geq 1$.

Συνεπώς, αν $\beta := a^{p^{k-1}}$, τότε $ord(\beta) = p$

Πρόταση 5η:

Αν G πεπερασμένη p-ομάδα, δηλαδή $|G| = p^n$ για $n \geq 1$, τότε υπάρχει μια αλυσίδα κανονικών υποομάδων της $G : \{1\} = H_0 \leq H_1 \leq \cdots \leq H_{m-1} \leq H_m = G$ τ.ω. $|H_i| = p^i$ για $i = 0, 1, 2, \cdots, m$
(χωρίς απόδειξη)

5.1.3 ΕΠΙΛΥΣΙΜΕΣ ΟΜΑΔΕΣ

Ορισμός:

Μια πεπερασμένη ομάδα G θα λέγεται επιλύσιμη, όταν για κάποιο $m \geq 0$ έχει μια αλυσίδα υποομάδων της, $\{1\} = G_0 \leq G_1 \leq \cdots \leq G_m = G$ τ.ω.

1. $\forall i = 1, 2, \cdots, m-1$ ισχύει: $G_i \trianglelefteq G_{i+1}$ και
2. ${}^{G_{i+1}}/_{G_i}$ είναι κυκλική.

Πρόταση 6η:

Κάθε πεπερασμένη αβελιανή ομάδα είναι επιλύσιμη.

Απόδειξη:

Για τεχνικούς λόγους (ομάδα $Galois$) θα θεωρήσουμε ότι η Α είναι πολλαπλασιαστική.
Από το Θεμελιώδες Θεώρημα των πεπερασμένων αβελιανών ομάδων, έχουμε:
$A \cong H_1 \times H_2 \times \cdots \times H_r$, όπου H_i κυκλική.
Θεωρούμε τις ομάδες $V_i := H_1 \times H_2 \times \cdots \times H_i \quad i = 1, 2, \cdots, r$
Επειδή Α αβελιανή ισχύει: $\{1\} = V_0 \trianglelefteq V_1 \trianglelefteq \cdots V_r = A$
Επίσης: ${}^{V_i}/_{V_{i-1}} \cong \frac{H_1 \times H_2 \times \cdots \times H_{i-1} \times H_i}{H_1 \times H_2 \times \cdots \times H_{i-1}} \cong H_i$ κυκλική.
Επομένως, η Α είναι επιλύσιμη.

Παρατήρηση: Η «κανονικότητα» δεν έχει την «μεταβατική» ιδιότητα.

Πρόταση 7η:

Κάθε πεπερασμένη p-ομάδα ($p \in \mathbb{P}$) είναι επιλύσιμη.

Απόδειξη:

Από την Πρόταση 5 $\Rightarrow \ H_{i-1} \trianglelefteq H_i$, αφού $H_{i-1} \trianglelefteq G$.

Επίσης η ${}^{H_i}/_{H_{i-1}}$, έχει τάξη πρώτο αριθμό p δηλαδή, είναι κυκλική $\forall i = 1, 2, \cdots, m$
Επομένως είναι επιλύσιμη.

Πρόταση 8η:

Έστω G μια πεπερασμένη ομάδα.

(ι) Αν η G είναι επιλύσιμη, τότε και κάθε υποομάδα αυτής είναι επιλύσιμη.

(ιι) Αν G επιλύσιμη και $N \trianglelefteq G$, τότε και η ${}^{G}/_{N}$ επιλύσιμη.

(ιιι) Έστω $N \trianglelefteq G$. Τότε ισχύει η ισοδυναμία
(Η G είναι επιλύσιμη) $\Leftrightarrow$ (Ν και ${}^{G}/_{N}$ είναι επιλύσιμες)
(χωρίς απόδειξη)

5.1.4 ΟΜΑΔΕΣ ΜΕΤΑΘΕΣΕΩΝ

Υπενθυμίζουμε: S_n συμβολίζει την συμμετρική ομάδα των n-στοιχείων, δηλαδή όλων των αμφιμονοσήμαντων απεικονίσεων του συνόλου $\{1, 2, \cdots, n\}$ στον εαυτό του, με πράξη την σύνθεση συναρτήσεων.

Παραδοχή: Αν $\pi_1, \pi_2 \in S$, το $\pi_1 \cdot \pi_2$ θα σημαίνει εφαρμόζω πρώτα την π_1 και έπειτα την π_2.

Ορισμός:

Ένας κύκλος μήκους k της S_n είναι ένα στοιχείο $\sigma = (a_1, a_2, \cdots, a_k) \in S_n$ τ.ω.
$a_1\sigma = a_2,\ a_2\sigma = a_3, \cdots, a_{k-1}\sigma = a_k$ και $a_k\sigma = a_1$, ενώ $x\sigma = x, \quad \forall x \notin \{a_1, a_2, \cdots, a_k\}$

Πρόταση 9η:

Κάθε $\pi \in S_n$ αναλύεται σε γινόμενο κύκλων ξένων μεταξύ τους ανά δύο.

Απόδειξη:

Έστω $x_1 \in \{1, 2, \cdots, n\}$

Αν $x_1\pi = x_1$, τότε το (x_1) είναι κύκλος (μήκους 1).

Αν δεν ισχύει αυτό, τότε $x_1\pi = x_2$ και συνεχίζουμε $x_2\pi = x_3,\ \ x_3\pi = x_4,\ \cdots$

Επειδή το $\{1, 2, \cdots, n\}$ είναι πεπερασμένο σε κάποιο βήμα θα έχουμε επανάληψη.

Έστω ότι για πρώτη φορά έχουμε επανάληψη όταν $x_k\pi = x_j \quad (k > j)$

Αν $j \neq 1$, τότε $x_{j-1}\pi = x_j$ και $x_k\pi = x_j$ δηλαδή $x_{j-1}\pi = x_k\pi$, που σημαίνει ότι θα έχουμε επανάληψη πιο πριν, άτοπο.

Επομένως $j = 1$, δηλαδή ο περιορισμός του π στο σύνολο $\{x_1, x_2, \cdots, x_k\}$ μας δίνει τον κύκλο $(x_1, x_2, \cdots, x_k)$.

Τώρα παίρνουμε ένα $y_1 \in \{1, 2, \cdots, n\}$ και $y_1 \notin \{x_1, x_2, \cdots, x_k\}$ και συνεχίζουμε όμοια «μέχρι εξαντλήσεως των αποθεμάτων!».

Επομένως, ο π γράφεται σαν γινόμενο ξένων κύκλων.

Τώρα, παρατηρούμε ότι η τάξη ενός κύκλου είναι ίση με το μήκος του.

Επίσης παρατηρούμε ότι: (Ξένοι κύκλοι αντιμετατίθενται μεταξύ τους)

Έστω λοιπόν $\pi = \sigma_1\sigma_2 \cdots \sigma_r \mid \sigma_i$ κύκλοι μήκους λ_i.

Τότε, για κάθε $m \geq 1$ ισχύει: $\pi^m = \sigma_1^m\sigma_2^m \cdots \sigma_r^m$.

Επομένως $\pi^m = Id_{\{1,2,\cdots,n\}} \Leftrightarrow$ το m είναι πολλαπλάσιο των $\lambda_1, \lambda_2, \cdots, \lambda_r$ και

$ord(\pi) = m \Leftrightarrow$ το m είναι το ελάχιστο (κοινό) πολλαπλάσιο των $\lambda_1, \lambda_2, \cdots, \lambda_r$

Παρατήρηση: Η ανάλυση είναι κατά κάποιο τρόπο μοναδική.

π.χ. Ο $(145)(23)$ γράφεται και σαν $(32)(451)$, αλλά η βασική δομή δεν αλλάζει.

Ορισμός:

Ένας κύκλος μήκους 2 θα λέγεται αντιμετάθεση.

Πόρισμα:

Κάθε μετάθεση $\pi \in S_n$, αναλύεται σε γινόμενο αντιμεταθέσεων.

Απόδειξη:

Προφανώς, αφού κάθε κύκλος $\sigma = (a_1a_2 \cdots a_k) = (a_1a_2)(a_1a_3) \cdots (a_1a_k)$.

Σημείωση: Στο Πόρισμα η παράσταση δεν είναι μονοσήμαντη.

Αναλλοίωτη όμως παραμένει η *parity*

(Ας θεωρήσουμε το πολυώνυμο $\Delta(X_1, X_2, \cdots, X_n) = \prod_{1 \leq i < j \leq n} (X_i - X_j) =$

$(X_1 - X_2)(X_1 - X_3) \cdots (X_1 - X_n)(X_2 - X_3) \cdots (X_2 - X_n) \cdots (X_{n-1} - X_n)$

Πρόκειται για ένα πολυώνυμο n-μεταβλητών βαθμού $\frac{1}{2}n(n-1)$)

$\forall \pi \in S_n$, ορίζουμε $\pi(\Delta) = \prod_{1 \le i < j \le n} (X_{\pi(i)} - X_{\pi(j)})$.

Οι παράγοντες του $\pi(\Delta)$ είναι οι ίδιοι με αυτούς του Δ.

Η μόνη διαφορά είναι ότι μερικοί από αυτούς αντιστρέφονται.

Επομένως $\pi(\Delta) = \pm\Delta$.

Παράδειγμα:

Αν $\pi = (1\ 2)$ ο $x_1 - x_2$ γίνεται $x_2 - x_1$ και όλοι οι υπόλοιποι παραμένουν σταθεροί.

Επομένως $\pi(\Delta) = -\Delta$

Αν πάλι $\pi = (1\ 2\ 3) = (1\ 2)(1\ 3)$ τότε αντιστρέφονται οι $x_1 - x_2$ και $x_1 - x_3$

Επομένως $\pi(\Delta) = \Delta$

Ορισμός:

$\pi \in S_n$, π άρτια (αντίστοιχα περιττή) $\Leftrightarrow$ $\pi(\Delta) = \Delta$ (αντίστοιχα $-\Delta$)

Παρατηρούμε ότι η π άρτια (περιττή) $\Leftrightarrow$ ο Π αναλύεται σε γινόμενο από άρτιο (περιττό) πλήθος αντιμεταθέσεων.

Επομένως,

Αν π_1 άρτια, π_2 άρτια $\Rightarrow$ $\pi_1\pi_2$ άρτια.

Αν π_1 άρτια, π_2 περιττή $\Rightarrow$ $\pi_1\pi_2$ περιττή.

Αν π_1 περιττή, π_2 άρτια $\Rightarrow$ $\pi_1\pi_2$ περιττή.

Αν π_1 περιττή, π_2 περιττή $\Rightarrow$ $\pi_1\pi_2$ άρτια.

Συμπέρασμα: Το σύνολο $A_n := \{\pi \in S_n \ / \ \text{άρτια}\}$ είναι κανονική υποομάδα της S_n (Το σύμπλοκο $A_n(1\ 2)$ περιέχει μόνο περιττές μεταθέσεις. Επίσης κάθε περιττή Π γράφεται $[\pi(1\ 2)](1\ 2)$ και $\pi(1\ 2)$ είναι άρτια).

Συνεπώς, $[S_n : A_n] = 2$, δηλαδή $|A_n| = \frac{n!}{2}$

Πρόταση 10^{η}:

Η S_3 είναι επιλύσιμη.

Απόδειξη:

$$S_3 = \left\{ 1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, a = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \right.$$
$$\left. x = \begin{pmatrix} 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, y = \begin{pmatrix} 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, z = \begin{pmatrix} 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

Η $H = \{1 = a^3,\ a,\ b = a^2\}$ είναι υποομάδα της S_3 τάξεως 3.

Επομένως $[S_3 : H] = \frac{3!}{3} = \frac{6}{3} = 2 \ \Rightarrow \ H \trianglelefteq S_3$.

Επίσης $\#({}^{S_3}/_H) = 2 \in \mathbb{P}$, άρα είναι κυκλική.

Έχουμε $\{1\} \trianglelefteq H \trianglelefteq S_3$, ${}^{S_3}/_H$ κυκλική, ${}^{H}/_{\{1\}}$ κυκλική (τάξης 3)

Δηλαδή S_3 επιλύσιμη.

Πρόταση 11η:

Η S_4 είναι επιλύσιμη.

Απόδειξη:

Επειδή $[S_4 : A_4] = 2$, έχουμε $A_4 \trianglelefteq S_4$.

Επίσης $\#{}^{S_4}/_{A_4} = 2 \in \mathbb{P}$, άρα κυκλική.

$A_4 = \{(1), (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 3\ 4), (1\ 4\ 2), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3),$
$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$

Η $V := \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ είναι μια υποομάδα της A_4, τάξεως 4
(η τετραεδρική του $Klun$)

Η $V \trianglelefteq A_4$.

Πράγματι, $V(1\ 2\ 3) = \{(1\ 2\ 3), (1\ 3\ 4), (1\ 4\ 2), (2\ 4\ 3)\} = (1\ 2\ 3)V$

Ομοίως και τα υπόλοιπα.

Επίσης $\#({}^{A_4}/_V) = 3 \in \mathbb{P}$, άρα κυκλική.

Όμως $\#V = 4 \notin \mathbb{P}$.

Θεωρούμε την $\mathbb{Z}_2 = \{(1), (1\ 2)(3\ 4)\}$ $\quad [V : \mathbb{Z}_2] = 2 \ \Rightarrow \ \mathbb{Z}_2 \trianglelefteq V$.

Επίσης, $\#({}^{V}/_{Z_2}) = 2 \in \mathbb{P}$, άρα κυκλική.

Τελικά $\{(1)\} \trianglelefteq \mathbb{Z}_2 \trianglelefteq V \trianglelefteq A_4 \trianglelefteq S_4$ και τα πηλίκα κυκλικά $\Rightarrow$ S_4 επιλύσιμη.

Ερώτηση: Τι γίνεται με τις S_n, $\quad n \geq 5$;

και γιατί μας ενδιαφέρει η επιλυσιμότητα ;

Στο πρώτο ερώτημα η απάντηση θα πρέπει να περάσει μέσα από την μελέτη της A_n.

Πρόταση 12η:

Για κάθε $n \geq 3$ η A_n παράγεται από το σύνολο όλων των κύκλων μήκους 3.

Απόδειξη:

Από τον ορισμό της παράγεται η A_n από στοιχεία που είναι γινόμενο δύο αντιμεταθέσεων $(a\ b)(c\ d)$.

- Αν $(c\ d) = (a\ b)$ τότε $(a\ b)(c\ d) = (1)$
- Αν $(c\ d) = (a\ c)$ τότε $(a\ b)(c\ d) = (a\ b\ c)$
- Αν $(c\ d) \neq (a\ b)$ τότε $(a\ b)(c\ d) = [(a,b)(a,c)][(c\ a)(c\ d)] = (a\ b\ c)(c\ a\ d)$

Ορισμός:

Μια ομάδα G θα λέγεται απλή όταν δεν έχει γνήσιες (διαφορετικές των $\{1\}$ και G) κανονικές υποομάδες.

Θεώρημα:

$\forall n \geq 5$ η A_n είναι απλή.

Απόδειξη:

Έστω $N \trianglelefteq A_n, \quad N \neq \{1\}$.

Θα αποδείξουμε ότι N περιέχει όλους τους 3-κύκλους και συνεπώς $N = A_n$.

Θα ξεχωρίσουμε διάφορες περιπτώσεις:

1η Περίπτωση: Έστω ότι η N περιέχει έναν 3-κύκλο, $(a\ b\ c)$.

Έστω $x, y, z \in \{1, 2, \cdots, n\}$ τρία διακεκριμένα οποιαδήποτε στοιχεία του συνόλου και έστω $\alpha := \begin{pmatrix} a & b & c \\ x & y & z \end{pmatrix} \in S_n$

$$\alpha^{-1}(a\ b\ c)\alpha = \begin{pmatrix} x & y & z \\ a & b & c \end{pmatrix} \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \begin{pmatrix} a & b & c \\ x & y & z \end{pmatrix} = \begin{pmatrix} x & y & z \\ y & z & x \end{pmatrix} = \begin{pmatrix} x & y & z \end{pmatrix}$$

Αν α άρτια μετάθεση, τότε $\alpha^{-1}(a\ b\ c)\alpha = (x, y, z) \in A_n$ και αφού $N \trianglelefteq A_n$ και

$(a, b, c) \in N \ \Rightarrow\ (x\ y\ z) \in N$

Αν α περιττή, θεωρούμε την μετάθεση $\beta = (d\ e)\alpha \in A_n$ όπου $(d, e \notin \{a, b, c\})$

(Αυτό είναι δυνατό, αφού $n \geq 5$)

Και πάλι $\beta^{-1}(a\ b\ c)\beta = (x\ y\ z)$

Επομένως ο N περιέχει όλους τους 3-κύκλους.

Άρα $N = A_n$

2η Περίπτωση: Υποθέτουμε ότι $\pi \in N$ και $\pi = \sigma_1\sigma_2\cdots\sigma_r$, γινόμενο ξένων μεταξύ τους κύκλων, εκ των οποίων ένας, χ.β.τ.γ. ο σ_1, έχει μήκος $s \geq 4 \quad \sigma_1 = (a_1\ a_2\ \cdots\ a_s)$

Έστω $\alpha = (a_1\ a_2\ a_3)$

Επειδή οι κύκλοι $\sigma_2, \cdots, \sigma_r$ είναι ξένοι προς τον α, αντιμετατίθενται με τον α.

Συνεπώς $\alpha^{-1}\pi\alpha = (\alpha^{-1}\sigma_1\alpha)\sigma_2\cdots\sigma_r$

Όμως $\alpha^{-1}\sigma_1\alpha = (a_1\ a_3\ a_2)(a_1\ a_2\ \cdots\ a_s)(a_1\ a_2\ a_3) = (a_2\ a_3\ a_1\ a_4\ a_5\ \cdots\ a_s\ )$

Το $\pi \in N\ \Rightarrow\ \pi^{-1} \in N$.

$N \trianglelefteq A_n$ και $\alpha = (a_1\ a_2\ a_3) \in A_n \quad \Rightarrow\ \alpha^{-1}\pi\alpha \in N$

Συνεπώς $\pi^{-1}\alpha^{-1}\pi\alpha \in N$

Το $\pi^{-1}\alpha^{-1}\pi\alpha = \sigma_1^{-1}(\alpha^{-1}\sigma_1\alpha) =$

(όλα τα υπόλοιπα, φεύγουν $\sigma_r^{-1}r\cdots\sigma_2^{-1}\sigma_2\sigma_3\cdots\sigma_r$)

$= (a_1\ a_{s-1}\cdots a_1)(a_2\ a_3\ a_1\ a_4\ a_5\ \cdots\ a_s) = (a_1\ a_2\ a_4) \in N$ και το πρόβλημα ανάγεται στην πρώτη περίπτωση.

3η Περίπτωση: Η N περιέχει μόνο στοιχεία τα οποία αναλυμένα σε κύκλους, έχουν μόνο κύκλους μήκους 2 και 3.

- Αν $\pi \in N$ και η ανάλυση του περιέχει ακριβώς ένα κύκλο μήκους 3 (όλοι οι άλλοι είναι μήκους 2), έστω $\pi = (a\ b\ c) \in N\ \Rightarrow\ 1^{\eta}$ περίπτωση.
  (Στο π^2 όλες οι αντιμεταθέσεις εξαφανίζονται)

- Υποθέτουμε ότι ο π περιέχει τουλάχιστον δυο 3-κύκλους, έστω $(a\ b\ c)$ και $(d\ e\ f)$ δύο από αυτούς.
  $N \trianglelefteq A_n, \quad \pi \in N\ \Rightarrow\ \pi' := (e\ c\ d)^{-1}\pi(e\ c\ d) = (e\ c\ d)\pi(e\ c\ d) \in N$
  Το $\pi' = (a\ b\ d)(c\ f\ e)\cdots$
  Επομένως $\pi\pi' = (a\ b\ c)(d\ e\ f)\cdots(a\ b\ d)(c\ f\ e)\cdots = (a\ d\ c\ b\ f\cdots)$ και το πρόβλημα ανάγεται στην 2^{η} περίπτωση.

4η Περίπτωση: Υποθέτουμε ότι ο π είναι γινόμενο (άρτιου πλήθους) αντιμεταθέσεων.

- Αν $\pi = (a\ b)(a\ d)$ (δηλαδή ακριβώς 2)

Αφού $n \geq 5$ υπάρχει τουλάχιστον ένα ακόμη στοιχείο $e \in \{1, 2, \cdots, n\}$ διαφορετικό από τα a, b, c, d.

Υπολογίζουμε το

$\pi[(a\ b\ e)^{-1}\pi(a\ b\ e)] = (a\ b)(c\ d)(a\ e\ b)(a\ b)(c\ d)(a\ b\ e) = (a\ b\ e) \in N$ και το πρόβλημα ανάγεται στην 1^{η} περίπτωση.

- Τέλος αν $\pi = (a\ b)(c\ d)(e\ f)(g\ h)\cdots$

  τότε $\pi[(b\ c)^{-1}(d\ e)^{-1}\pi(d\ e)(b\ c)] = \pi(b\ c)(d\ e)\pi(d\ e)(b\ c) = (a\ e\ d)(b\ c\ f)\cdots \in N$

  και το πρόβλημα ανάγεται στην 3^{η} περίπτωση.

Πρόταση 13η:

Η συμμετρική ομάδα S_n παράγεται από τους κύκλους $\sigma = (1\ 2\ 3\ \cdots\ n)$ και $\tau = (1\ 2)$ δηλαδή $S_n =< (1\ 2\ 3\ \cdots\ n), (1\ 2) >$

Απόδειξη:

$\sigma^{-1} = \sigma^{n-1} = (n\ n-1\ \cdots\ 2\ 1)$

Επομένως $\sigma^{-1}\tau\sigma = (n\ n-1\ n-2\ \cdots\ 4\ 3\ 2\ 1)(1\ 2)(1\ 2\ \cdots\ n) = (3\ 2) = (2\ 3)$

Επίσης $\sigma^1(2\ 3)\sigma = (3\ 4), \quad \sigma^{-1}(3\ 4)\sigma = (4\ 5)\cdots$

Συνεχίζοντας διαπιστώνουμε ότι όλες οι μεταθέσεις του τύπου $(m, m+1)$ ανήκουν στην $< \sigma, \tau >=: G$

Επίσης $(1\ 2)(2\ 3)(1\ 2) = (1\ 3) \in G, \quad (1\ 3)(3\ 4)(1\ 3) = (1\ 4) \in G\cdots$ δηλαδή και όλες οι μεταθέσεις του τύπου $(1\ m) \in G$

Τέλος, η τυχούσα μετάθεση $(a\ \beta)$, γράφεται, $(1\ a)(1\ \beta)(1\ a) = (a\ \beta) \in G$

Επειδή, κάθε στοιχείο της S_n είναι γινόμενο αντιμεταθέσεων έπεται ότι $S_n =< \sigma, \tau >$.

Πρόταση 14η:

Η (πεπερασμένη) ομάδα G είναι επιλύσιμη και απλή $\Leftrightarrow$ (Είναι κυκλική τάξεως πρώτου αριθμού)

Απόδειξη:

Υποθέτουμε ότι η G είναι επιλύσιμη.

Επομένως υπάρχει μια αλυσίδα υποομάδων H_i τ.ω. $\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_n = G$

Υποθέτουμε ότι έχουμε διαγράψει επαναλήψεις, και επομένως ισχύει:

$H_{i+1} \neq H_i \quad \forall i = 0, 1, 2, \cdots, (n-1)$

Συνεπώς η $H_{n-1} \trianglelefteq G$, γνήσια υποομάδα της G

$(H_{n-1} \neq H_n = G)$

Η G είναι και απλή, δηλαδή δεν έχει γνήσιες κανονικές υποομάδες, άρα $H_{n-1} = \{1\}$.

Τώρα G επιλύσιμη $\Rightarrow {}^{G}/_{H_{n-1}} = {}^{G}/_{\{1\}} = G$ κυκλική.

Αν η τάξη της G ήταν κάποιος σύνθετος αριθμός $n = m \cdot r$, $(m, r > 1)$ τότε η G δεν θα ήταν απλή αφού θα είχε γνήσια κανονική υποομάδα.

(Αν $|G| = n = m \cdot r \quad (m, r > 1), \quad G =< a >$ η $< a^m >$ είναι μια τέτοια)

Επομένως η G κυκλική τάξης πρώτου αριθμού.

Αντίστροφα: Αν η G κυκλική τάξης πρώτου αριθμού $\Rightarrow$ είναι απλή.

(δεν περιέχει γνήσιες κανονικές υποομάδες, αφού αν $H \leq G, \quad |H||G| = p \Rightarrow H = \{1\}$ ή $H = G$)

Είναι κυκλική, άρα αβελιανή και συνεπώς, Πρόταση 6, επιλύσιμη.

Θεώρημα:

$\forall n \geq 5$ η S_n δεν είναι επιλύσιμη.

Απόδειξη:

Αν η S_n επιλύσιμη, θα ήταν επιλύσιμη και η A_n (Πρόταση $8(i)$

Όμως, η A_n είναι απλή (για $n \geq 5$)

Συνεπώς, Πρόταση 14, θα ήταν κυκλική τάξεως πρώτου αριθμού.

Αυτό βέβαια είναι αδύνατο, αφού για $n \geq 5$ $|A_n| = \frac{n!}{2} \notin \mathbb{P}$

5.2 Ομάδες και εξισώσεις

Στην παράγραφο αυτή υποθέτουμε ότι πάντοτε $chK = 0$.
(Έτσι έχουμε την διαχωρισιμότητα «από χέρι»)
Έστω, λοιπόν ένα σώμα K και $f(X) \in K[X]$, όχι κατ΄ ανάγκη ανάγωγο.
Αν L ένα σώμα ανάλυσης του $f(X)$ υπέρ το K, από Πρόταση 8 Κεφάλαιο 4, έπεται ότι η επέκταση ${}^{L}/_{K}$ είναι κανονική.
Επειδή $chK = 0$, έπεται ότι η ${}^{L}/_{K}$ είναι και διαχωρίσιμη.
Συνεπώς είναι επέκταση $Galois$.

Ορισμός:

Η ομάδα $Galois$ της ${}^{L}/_{K}$ $\quad Gal({}^{L}/_{K})$ θα λέγεται ομάδα $Galois$ του πολυωνύμου $f(X) \in K[X]$

Συμβολισμός: $Gal(f(X)) := Gal({}^{L}/_{K})$

Ορισμός:

Η επέκταση σωμάτων ${}^{L}/_{K}$ θα λέγεται επέκταση με ριζικά ή ριζική επέκταση :$\Leftrightarrow$ υπάρχει μια αλυσίδα σωμάτων $L = L_0 \leq L_1 \leq L_2 \leq \cdots \leq L_m = L$ με την ιδιότητα, για κάθε $j = 0, 1, 2, \cdots, m-1 \quad L_{j+1} = L_j(a_j)$ όπου a_j ρίζα ενός πολυωνύμου της μορφής $X^{m_j} - a_j \in L_j[X]$

Παρατήρηση: Ο ορισμός μας δίνει μια έκφραση της έννοιας ότι τα στοιχεία του L προκύπτουν από αυτά του K μέσω ρητών πράξεων και εξαγωγής m_j-ριζών $(j = 1, 2, \cdots, m)$.

Παράδειγμα:

Έστω $K = \mathbb{Q}$, τότε το στοιχείο $(3 + \sqrt{2})^{\frac{1}{5}} + 2\sqrt[3]{5}$ ανήκει σε ένα σώμα L_3, όπου
$K = L_0 = \mathbb{Q}$,
$L_1 = \mathbb{Q}$ / $a_0^2 = \sqrt{2}$
$L_2 = L_1(a_1)$ / $a_1^5 = 3 + \sqrt{2}$

$L_3 = L_2(a_2)$ / $a_2^3 = 5$

Ορισμός:

Το πολυώνυμο $f(X) \in K[X]$ θα λέγεται επιλύσιμο με ριζικά όταν (ένα) σώμα ανάλυσης αυτού, έστω L, περιέχεται σε ένα σώμα Μ τ.ω. η επέκταση ${}^{M}/_{K}$ να είναι επέκταση με ριζικά.

Παρατηρήσεις:

1. Στον ορισμό δεν απαιτούμε η ${}^{L}/_{K}$ να είναι επέκταση με ριζικά.

2. Είναι δυνατόν μια ρίζα ενός πολυωνύμου να είναι εκφράσιμη με ριζικά και μια άλλη όχι (π.χ. αν $h(X) = f(X)g(X)$ και το ένα από αυτά είναι επιλύσιμο με ριζικά ενώ το άλλο όχι.)
   Όμως, αν το $f(X) \in K[X]$ είναι ανάγωγο υπέρ το Κ τότε αν μια ρίζα του εκφράζεται μέσω ριζικών, το ίδιο ισχύει για όλες τις ρίζες.
   (Για την απόδειξη, χρησιμοποιούμε το Θεώρημα Επέκτασης των ισομορφισμών, Πρόταση 19_1 Κεφάλαιο 3 και επαγωγή)

Πρόταση 15η:

Αν η επέκταση ${}^{L}/_{K}$ είναι επέκταση με ριζικά και Ν η κανονική θήκη του L υπέρ το Κ, τότε και η ${}^{N}/_{K}$ είναι επέκταση με ριζικά.

Απόδειξη:

Η ${}^{L}/_{K}$ είναι επέκταση με ριζικά συνεπάγεται: $L = K(a_1, a_2, \cdots, a_m)$ τ.ω.
$\forall i = 1, 2, \cdots, m \quad \exists m_i \in \mathbb{N}$ τ.ω $a_i^{m_i} \in K(a_1, a_2, \cdots, a_{i-1})$.
Έστωσαν, $f_i(X) = Irr(a_i, K) \in K[X] \quad i = 1, 2, \cdots, m$ και
$f(X) = f_1(X)f_2(X)\cdots f_m(X)$.
Αφού Ν η κανονική θήκη του L υπέρ το Κ το Ν είναι σώμα ανάλυσης του $f(X)$ υπέρ το Κ.
Σύμφωνα με το Θεώρημα επέκτασης των ισομορφισμών (Πρόταση 19_1, Κεφάλαιο 3)(ή Πρόταση 15) για κάθε ρίζα β_{i_j} του $f_i(X)$ υπάρχει ένας Κ-ισομορφισμός σωμάτων
$K(a_i) \cong K(\beta_{i_j})$ τ.ω. $\Psi(a_i) = \beta_{i_j}$

Αφού το a_i είναι εκφράσιμο με ριζικά, και το β_{i_j} είναι εκφράσιμο με ριζικά και συνεπώς και η ${}^{N}/_{K}$ είναι επέκταση με ριζικά.
$(N = K(\beta_{1_1}, \beta_{1_2}, \cdots, \beta_{1_{k_1}}, \beta_{2_1}, \beta_{2_2}, \cdots))$

Πρόταση 16η:

Αν $p \in \mathbb{P}$ και L ένα σώμα ανάλυσης του $f(X) = X^p - 1 \in K[X]$, τότε η ομάδα $Galois$ της επέκτασης ${}^{L}/_{K}$ είναι αβελιανή. (Μάλιστα είναι κυκλική.)

Απόδειξη:

(Διάλεξη της Ανθής Ζερβού)

Πρόταση 17η:

Αν στο K ανήκει μια πρωταρχική n-ρίζα της μονάδας $a \in K$, και L ένα σώμα ανάλυσης του πολυωνύμου $f(X) = X^n - a \in K[X]$ τότε η ομάδα $Galois$ της επέκτασης ${}^{L}/_{K}$ είναι αβελιανή.

Απόδειξη:

(Διάλεξη της Ιωσήφ Μαυραλεξάκη και Ευάγγελου Κουλουκουσίδη)

Πρόταση 18η:

Αν η ${}^{L}/_{K}$ είναι κανονική και επέκταση με ριζικά τότε η $Gal({}^{L}/_{K})$ είναι επιλύσιμη.

Απόδειξη:

Η ${}^{L}/_{K}$ επέκταση με ριζικά, άρα $L = K(a_1, a_2, \cdots, a_m)$, όπου, $\forall j = 2, 3, \cdots, m \quad \exists m_j \in \mathbb{N}$ τ.ω. $a_j^{m_j} \in K(a_1, a_1, \cdots, a_{j-1})$

Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $m_j =: p_j \in \mathbb{P}$, πρώτοι αριθμοί.

Θα εφαρμόσουμε επαγωγή, ως προς m.

Για $m = 0, \quad L = K \Rightarrow Gal({}^{L}/_{K}) = \{Id_K\}$ η οποία είναι επιλύσιμη.

Υποθέτουμε ότι η πρόταση ισχύει για κάθε $i < m$, δηλαδή ότι, $\forall i < m$ η
$Gal({}^{K(a_1,a_2,\cdots,a_i)}/_{K})$ είναι επιλύσιμη.

Το $L := K(a_1, a_2, \cdots, a_m)$

Υποθέτουμε ότι ισχύει: $a_1 \notin K(a_2, \cdots, a_m)$

(Αλλιώς $L = K(a_2, \cdots, a_m)$ και λόγω της υπόθεσης της μαθηματικής επαγωγής θα είχαμε τελειώσει: ${}^{L}/_{K}$ θα ήταν επιλύσιμη).

Επομένως $deg\ Irr(a_1, K) \geq 2$.

(Αν ήταν $= 1, \quad a_1 \in K \ \Rightarrow \ a_1 \in K(a_2, \cdots, a_m)$)

Τώρα, $[\exists p \in \mathbb{P}$ τ.ω. $a_1^p \in K]$.

Επομένως, το $f(X) := X^p - a_1^p \in K[X]$

Άρα, $Irr(a_1, K) \mid_{K[X]} f(X)$

Επειδή $chK = 0$ και $deg\ Irr(a_1, K) \geq 2$, έπεται ότι το $Irr(a_1, K)$ έχει μια ακόμη τουλάχιστον ρίζα, έστω $\beta, \quad \beta \neq a_1\ \beta \in L$ αφού ${}^{L}/_{K}$ κανονική.

Επειδή $Irr(a_1, X) \mid f(X) = X^p - a_1^p$ έπεται ότι το β είναι ρίζα του $X^p - a_1^p$, δηλαδή $\beta^p = a_1^p \ \Rightarrow \ (\frac{\beta}{a_1})^p = 1$

Το $\varepsilon := \frac{\beta}{a_1} \in L$ και $\varepsilon \neq a_1$.

Επειδή $\varepsilon^p = 1$, έπεται ότι $ord(\varepsilon) = p$ στην L^* και συνεπώς τα στοιχεία $1, \varepsilon, \varepsilon^2, \cdots, \varepsilon^{p-1}$ είναι p-στές ρίζες της μονάδας στο L, δηλαδή το $X^p - 1$ αναλύεται πλήρως στο L.

Έστω Ε το σώμα ανάλυσης του $X^p - 1 \in K[X]$ υπέρ το Κ.

Το $E = K(\varepsilon)$ και $K \leq E = K(\varepsilon) \leq E(a_1) \leq L$

Το $E(a_1)$ είναι το σώμα ανάλυσης του $f(X) = X^p - a_1^p \in K[X]$.

Επομένως:

$$
\begin{array}{ccc}
L & \leftrightarrow & \{Id_L\} \\
| & & | \\
E(a_1) & \leftrightarrow & Gal({}^{L}/_{E(a_1)}) \\
| & & | \qquad \} : Gal({}^{E(a_1)}/_{E}) \\
E = K(\epsilon) & \leftrightarrow & Gal({}^{L}/_{E}) \\
| & & | \qquad \} : Gal({}^{E}/_{K}) \\
K & \leftrightarrow & Gal({}^{L}/_{E})
\end{array}
$$

Η ${}^{L}/_{E(a_1)}$ είναι πάντοτε $Galois$ και μάλιστα η $Gal({}^{L}/_{E(a_1)})$ επιλύσιμη λόγω της επαγωγικής υπόθεσης.

Η ${}^{E(a_1)}/_{E}$ είναι κανονική (και διαχωρίσιμη) αφού το $E(a_1)$ είναι σώμα ανάλυσης του $X^p - a_1 \in E[X]$.

$\xRightarrow{\text{Πρόταση17}}$ Η $Gal({}^{E(a_1)}/_{E})$ είναι αβελιανή (και συνεπώς ,Πρόταση 6 Καφάλαιο 5, επιλύσιμη)

Η ${}^{E}/_{K}$ είναι $Galois$, αφού Ε σώμα ανάλυσης του $X^p - 1 \in K[X]$ και, από Πρόταση 16,

Κεφάλαιο 5, αβελιανή.

Υπόθεση της προς απόδειξη πρότασης: ${}^{L}/_{K}$ κανονική. Συνεπώς ${}^{L}/_{E}$ κανονική.

Επομένως, $Gal({}^{E(a_1)}/_{E}) \cong {}^{Gal({}^{L}/_{E})}/_{Gal({}^{L}/_{E(a_1)})}$

Το $L = E(a_1)(a_1, \cdots, a_m)$ είναι επέκταση με ριζικά και κανονική $\Rightarrow$ ${}^{L}/_{E(a_1)}$ είναι επιλύσιμη $\xRightarrow{\text{επαγωγική υπόθεση}}$ $Gal({}^{L}/_{E})$ επιλύσιμη.

Επίσης, $Gal({}^{E}/_{K}) \cong {}^{Gal({}^{L}/_{K})}/_{Gal({}^{L}/_{E})}$

($Gal({}^{E}/_{K})$ Αβελιανή $\Rightarrow$ επιλύσιμη)

$\Rightarrow$ $Gal({}^{L}/_{K})$ επιλύσιμη.

Θεώρημα:

Αν $K \leq L \leq M$ και ${}^{M}/_{K}$ επέκταση με ριζικά, τότε η $Aut({}^{L}/_{K})$ είναι επιλύσιμη.

Απόδειξη:

Έστω $K_0 = \Phi(Aut({}^{L}/_{K}))$

Η επέκταση ${}^{L}/_{K_0}$ είναι κανονική, (αφού $K_0 = \Phi(Aut({}^{L}/_{K}))$, δες Πρόταση 7 Κεφάλαιο 4) και διαχωρίσιμη (αφού $chK = 0$).

Έστω N η κανονική θήκη του M υπέρ το K.

Στον πύργο σωμάτων $K \leq K_0 \leq L \leq M \leq N$, η ${}^{M}/_{K}$ είναι επέκταση με ριζικά,άρα και η ${}^{M}/_{K_0}$ είναι επέκταση με ριζικά, οπότε, Πρόταση 15, και η ${}^{N}/_{K_0}$ είναι επέκταση με ριζικά.

Η ${}^{N}/_{K}$ είναι κανονική, άρα και η ${}^{N}/_{K_0}$ είναι επίσης κανονική.

Τελικά η ${}^{N}/_{K_0}$ είναι κανονική και επέκταση με ριζικά, οπότε (Πρόταση 18) η $Gal({}^{N}/_{K_0})$ είναι επιλύσιμη.

Τώρα,

$$\begin{array}{ccc} & N & \\ & | \quad \diagdown & \\ \diagup & L \qquad & Galois \\ Gal({}^{L}/_{K_0}) & | \quad \diagup & \\ \diagdown & K_0 & \end{array}$$

Η ${}^{N}/_{K_0}$ είναι κανονική άρα $Galois \Rightarrow$ η ${}^{N}/_{L}$ είναι $Galois$.

Επίσης η ${}^{L}/_{K_0}$ είναι $Galois$.

Επομένως από το Θεμελιώδες Θεώρημα της Θεωρίας $Galois$, $Gal({}^{L}/_{K_0}) \cong \frac{Gal({}^{N}/_{K_0})}{Gal({}^{N}/_{L})}$.

Η $Gal({}^{N}/_{K_0})$ επιλύσιμη, Πρόταση $8(ii)$ Κεφάλαιο 4, και η $Gal({}^{L}/_{K_0})$ είναι επιλύσιμη.

Έστω $H := Aut(^{L}/_{K})$.

Ισχύει $H = Gal(^{L}/_{\Phi(H)})$ $(*)$

Αλλά η $\Phi(H) = \Phi(Aut(^{L}/_{K})) = K_0$.

Συνεπώς από το $(*)$ $H = Gal(^{L}/_{K_0})$, επιλύσιμη

Πόρισμα:

Έστω $f(X) \in K[X]$.

Αν το $f(X)$ είναι επιλύσιμο με ριζικά τότε η $Gal(^{f(X)}/_{K})$ είναι επιλύσιμη.

Απόδειξη:

Έστω L ένα σώμα ανάλυσης του $f(X)$ υπέρ το K.

Η $^{L}/_{K}$ είναι επέκταση $Galois$ και το $L \leq M$ τ.ω. $^{M}/_{K}$ επέκταση με ριζικά.

Επομένως, Θεώρημα, η $Aut(^{L}/_{K}) = Gal(^{L}/_{K}) = Gal(^{f(X)}/_{K})$ είναι επιλύσιμη.

Άμεση συνέπεια του Πορίσματος είναι ότι αν η $Gal(^{f(X)}/_{K})$ δεν είναι επιλύσιμη, τότε το $f(X) \in K[X]$ δεν είναι επιλύσιμο με ριζικά.

Ας ψάξουμε λοιπόν να βρούμε κάποιο πολυώνυμο με ομάδα $Galois$ π.χ. την S_5.

Πρώτα απ΄ όλα θα αποδείξουμε την ακόλουθη πρόταση:

Πρόταση 19η:

Έστω $p \in \mathbb{P}$ και $f(X) \in \mathbb{Q}[X]$ μονικό και ανάγωγο με $deg(f(X)) = p$

Υποθέτουμε ότι το f έχει ακριβώς δύο ρίζες στο $\mathbb{C} \setminus \mathbb{R}$.

Τότε, $Gal(^{f(X)}/_{\mathbb{Q}}) \cong S_p$

Απόδειξη:

Από το Θεμελιώδες Θεώρημα της Άλγεβρας, το $f(X)$ έχει ένα σώμα ανάλυσης $L \leq \mathbb{C}$.

$^{L}/_{\mathbb{Q}}$ κανονική και διαχωρίσιμη $\Rightarrow$ $^{L}/_{\mathbb{Q}}$, $Galois$.

Επομένως $\#G = \#Gal(^{L}/_{\mathbb{Q}}) = [L : \mathbb{Q}]$

Το πολυώνυμο $f(X)$ είναι ανάγωγο $|_{\mathbb{Q}}$ και διαχωρίσιμο, άρα έχει απλές ρίζες.

Οι ρίζες του είναι p.

Επομένως, Θεώρημα του $Gayley$, η $G \leq S_p$.

Αν a ρίζα του $f(X)$ τότε $[\mathbb{Q}(a) : \mathbb{Q}] = deg\ Irr(a, \mathbb{Q}) = deg\ f(X) = p$

$[L : \mathbb{Q}] = [L : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}] \Rightarrow p \mid [L : \mathbb{Q}] = \#G$

Σύμφωνα με το Θεώρημα του $Cauchy$ η G έχει ένα τουλάχιστο στοιχείο τάξης p.

Τα μοναδικά όμως στοιχεία της S_p τάξης p είναι οι p-κύκλοι.

Άρα η G περιέχει ένα τουλάχιστο p-κύκλο.

Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι αυτός ο είναι ο $(1\ 2\ \cdots\ p)$.

Ο $\mathbb{Q}$-αυτομορφισμός του L, που αφήνει σταθερές τις πραγματικές ρίζες και αντιμεταθέτει τις μιγαδικές αντιστοιχεί σε μια αντιμετάθεση, έστω την $(1\ 2)$.

Επομένως $\left.\begin{matrix}(1\ 2\ \cdots\ p)\in G\\ (1\ 2)\in G\end{matrix}\right\} \Rightarrow <(1\ 2\ \cdots\ p),(1\ 2)>\leq G \Rightarrow S_p\leq G$

Τελικά $G=S_p$

Παράδειγμα:

$f(X)=X^5-8X+2\in\mathbb{Q}[X]$

Το $f(X)$ ανάγωγο υπέρ το $\mathbb{Q}$ $(Eisenstein.$ για $p=2)$

x	-2	-1	0	1	2
$f(X)$	-14	9	2	-5	8

Θεώρημα ενδιάμεσης τιμής.

Υπάρχει μια πραγματική ρίζα σε κάθε ένα από τα διαστήματα (-2,-1),(0,1),(1,2)

$f'(X)=5X^4-8$

Η $f'(X)>0$, εκτός ίσως αν $-\sqrt[4]{\frac{8}{5}}<X<\sqrt[4]{\frac{8}{5}}$ (όπου $-\sqrt[4]{\frac{8}{5}}\ -1.1247$ και $\sqrt[4]{\frac{8}{5}}\ 1.1247$)

Σύμφωνα με το Θεώρημα του $Rolle$ υπάρχει μια τουλάχιστον ρίζα του $f'(X)$ ανάμεσα σε δύο ρίζες της $f(X)$.

Η $f'(X)$ όμως έχει ακριβώς δύο ρίζες.

Άρα η $f(X)$ θα έχει το πολύ 3-πραγματικές.

Δηλαδή, τελικά η $f(X)$ έχει ακριβώς 3 πραγματικές ρίζες, δηλαδή ακριβώς 2 στο $\mathbb{C}\setminus\mathbb{R}$.

Συνεπώς, $Gal(^{f(X)}/_{\mathbb{Q}})\ \cong\ S_5$, η οποία δεν είναι επιλύσιμη και συνεπώς $f(X)$ όχι επιλύσιμο με ριζικά.

5.3 Κατασκευή κανονικού n-γώνου με κανόνα και διαβήτη

Στην αρχή αυτής της παραγράφου θα επιστρέψουμε στην κατασκευασιμότητα των σημείων του $\mathbb{R}^2$.

Υπενθυμίζουμε ότι το $(a,b) \in \mathbb{R}^2$ είναι κατασκευάσιμο $:\Leftrightarrow$ Μπορούμε να κατασκευάσουμε το σημείο αυτό ξεκινώντας από το $O=(0,0)$ και $I=(1,0)$ και κάνοντας χρήση κανόνα και διαβήτη.

Ισχύουν: Έστω $a,b \in \mathbb{R}$

(ι) Το $(a,0)$ είναι κατασκευάσιμο $\Leftrightarrow$ $(0,a)$ είναι κατασκευάσιμο.

(ιι) Το (a,b) είναι κατασκευάσιμο $\Leftrightarrow$ $(0,a)$ και $(b,0)$ είναι κατασκευάσιμα.

(ιιι) Αν $(a,0),(b,0)$ είναι κατασκευάσιμο, τότε και τα $(a+b,0),(a-b,0),(ab,0)$ είναι κατασκευάσιμα.

Επιπλέον αν $b \neq 0$ και το $\frac{a}{b}$ είναι κατασκευάσιμο.

Παρατήρηση: Αν $a,b \in \mathbb{Q}$ τότε το σημείο (a,b) είναι κατασκευάσιμο.

Απόδειξη:

Το (1,0) είναι κατασκευάσιμο $\overset{(iii)}{\Longrightarrow}$ $(m,0)$ για κάθε $m \in \mathbb{Z}$ είναι κατασκευάσιμο.

Το (1,0) είναι κατασκευάσιμο, άρα και το (i) (0,1) και συνεπώς (iii) και το $(0,m)|n \in \mathbb{Z}$ είναι κατασκευάσιμο.

Επομένως, (iii) το $(\frac{m}{n},0)$ για $m \in \mathbb{Z},\ n \in \mathbb{Z},\ n \neq 0$ είναι κατασκευάσιμο και $\overset{(i)}{\Rightarrow}$ $(0,\frac{m}{n})$ είναι κατασκευάσιμο, δηλαδή $(a,0)$ και $(0,b) \mid a,b \in \mathbb{Q}$ είναι κατασκευάσιμο, πάλι από $(iii) \Rightarrow (a,b)$ κατασκευάσιμο.

Πρόταση 20η:

Το $B_0 := \{O=(0,0),\ I=(1,0)\}$

Αν $\mathbb{Q} = K_0 \leq K_1 \leq \cdots \leq K_n = L \leq \mathbb{R}$ αλυσίδα σωμάτων, (υποσωμάτων του $\mathbb{R}$) τ.ω. $[K_i : K_{i-1}] = 2 \quad (i=1,2,\cdots,n)$ τότε κάθε σημείο $(a,b) \in L \times L$ είναι κατασκευάσιμο.

Απόδειξη:

Σύμφωνα με την παρατήρηση όλα τα σημεία του $\mathbb{Q}$ είναι κατασκευάσιμα, δηλαδή η Πρόταση ισχύει για $n = 0$.

Υποθέτουμε ότι ισχύει για $i \geq 1$, δηλαδή όλα τα σημεία του K_{i-1} είναι κατασκευάσιμα.

Από $[K_i : K_{i-1}] = 2 \Rightarrow \exists \beta \in K_i$ τ.ω $K_i = K_{i-1}(\beta)$

Το $Irr(\beta, K_{i-1}) = X^2 + bX + c \mid b, c \in K_{i-1}$ και $\Delta = b^2 - 4c \geq 0, \quad \Delta \in K_{i-1}$

Το $\beta = \frac{1}{2}(b \pm \sqrt{\Delta})$.

Επομένως $K_i = K_{i-1}(\sqrt{\Delta})$.

Το σημείο $(\sqrt{\Delta}, 0)$ είναι κατασκευάσιμο.

(Αυτό το έχουμε κάνει στις ασκήσεις)

Από τις εισαγωγικές παρατηρήσεις $(i), (ii), (iii)$ έπεται ότι κάθε στοιχείο του

$K_i, \quad a + b\sqrt{\Delta} \ / a, b \in K_{i-1}$ είναι κατασκευάσιμο.

Πρόταση 21η:

Αν η επέκταση ${}^{K}/_{\mathbb{Q}}$ είναι $Galois$ και $[K : \mathbb{Q}] = 2^m \quad (m > 0)$, τότε κάθε σημείο $(a, b) \in K \times K$ είναι κατασκευάσιμο.

Απόδειξη:

$\#Gal({}^{K}/_{\mathbb{Q}}) = 2^m$, είναι μια p-ομάδα (για $p = 2$).

Επομένως, Πρόταση 5 Κεφάλαιο 4, υπάρχει μια αλυσίδα κανονικών υποομάδων της G

$\{1\} = H_0 \leq H_1 \leq \cdots \leq H_{m-1} \leq H_m = G$ τ.ω. $|H_i| = 2^i, \quad i = 0, 1, 2, \cdots, m$

Από το Θεμελιώδες Θεώρημα της Θεωρίας $Galois$ έχουμε:

$K = \Phi(H_0) \geq \Phi(H_1) \geq \cdots \geq \Phi(H_{m-1}) \geq \Phi(H_m) = \mathbb{Q}$ και

$[K : \Phi(H_i)] = 2^i \quad (i = 0, 1, 2, \cdots, m)$ δηλαδή ότι

$[\Phi(H_i) : \Phi(H_{i+1})] = 2 \quad (i = 0, 1, 2, \cdots, m-1)$, οπότε το συμπέρασμα είναι άμεση συνέπεια της Πρότασης 20.

Επιστρέφουμε στο κύριο θέμα της παραγράφου που είναι η κατασκευή κανονικού n-γώνου, με κανόνα και διαβήτη.

Για κάθε $n \geq 3$ η κατασκευή κανονικού n-γώνου εξαρτάται από την κατασκευή της γωνίας $\Theta_n := \frac{2\pi}{n}$ (Κεντρική γωνία του κανονικού n-γώνου).

Αν δύο γωνίες Θ_m και Θ_n είναι κατασκευάσιμες, τότε και οι γωνίες $\Theta_m + \Theta_n, \ \ \Theta_m - \Theta_n$ είναι κατασκευάσιμες και συνεπώς και οι γωνίες $s\Theta_m + t\Theta_n \mid s, t \in \mathbb{Z}$ είναι κατασκευάσιμες.

Πρόταση 22η:

Οι παρακάτω προτάσεις είναι μεταξύ τους ισοδύναμες:

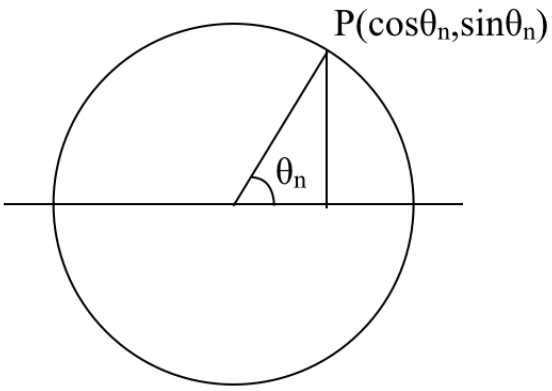
(ι) Η γωνία $\Theta_n = \frac{2\pi}{n}$ είναι κατασκευάσιμη.

(ιι) Το σημείο $(cos(\Theta_n), sin(\Theta_n))$ είναι κατασκευάσιμο.

(ιιι) Το σημείο $(cos(\Theta_n), 0)$ είναι κατασκευάσιμο.

Απόδειξη:

$(i) \Rightarrow (ii)$

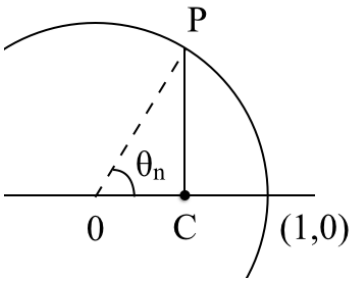


$(ii) \Rightarrow (iii)$

(Σελίδα 103 το (ii))

$(iii) \Rightarrow (i)$

Κατασκευάζουμε το $C = (cos(\Theta_n), 0)$



Η κάθετος στο C τέμνει τον μοναδιαίο κύκλο στο $P = (cos\theta_n, sin\theta_n)$

Συνδέουμε το P με το 0.

Πρόταση 23η:

Αν ΜΚΔ$(m,n)=1$, τότε το ($\Pi_{m\cdot n}$ είναι κατασκευάσιμο) $\Leftrightarrow$ (Π_m και Π_n είναι κατασκευάσιμα)

Απόδειξη:

" $\Rightarrow$ " Αν $A_0, A_1, \cdots, A_{m\cdot n-1}$ οι κορυφές του $\pi_{m\cdot n}$, τότε οι κορυφές $A_0, A_n, A_{2n}, \cdots, A_{(m-1)n}, A_0$ σχηματίζουν το π_m. Όμοια και το π_n.
(Εδώ, δεν χρησιμοποιούμε την υπόθεση $(m,n)=1$)

" $\Leftarrow$ " Υποθέτουμε ότι τα π_m, π_n είναι κατασκευάσιμα.
Επειδή $(m,n)=1 \Rightarrow [\exists \quad s,t\in\mathbb{Z} \quad \text{τ.ω} \quad sm+tn=1]$
Οι γωνίες θ_m και θ_n είναι κατασκευάσιμες.
Επομένως και η γωνία $s\theta_n + t\theta_m = \frac{2\pi s}{n} + \frac{2\pi t}{m} = \frac{2\pi(sm+tn)}{mn} = \frac{2\pi}{mn} = \theta_{mn}$ κατασκευάσιμη.

Λήμμα:

Έστω $\zeta_p := e^{\Theta_p} = e^{\frac{2\pi i}{p}} \quad (p\in\mathbb{P})$
Η γωνία $\Theta_p = \frac{2\pi}{p}$ είναι κατασκευάσιμη $\Leftrightarrow$ $[\mathbb{Q}(\zeta_p):\mathbb{Q}] = 2^m, \quad (m>0)$
Απόδειξη:
Το $Irr(\zeta_p,\mathbb{Q}) = X^{p-1}+\cdots+X+1 \in \mathbb{Q}[X]$
Επομένως $[\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1$.
Επίσης, η επέκταση ${}^{\mathbb{Q}(\zeta_p)}/_{\mathbb{Q}}$ έχει ομάδα *Galois* ισόμορφη με την $\mathbb{Z}_p^*$, άρα είναι αβελιανή. (μάλιστα είναι κυκλική.)
Θεωρούμε το σώμα $K := \mathbb{Q}(\zeta_p+\zeta_p^{-1})$.
Είναι προφανές ότι $\zeta_p+\zeta_p^{-1} = 2cos\frac{2\pi}{\pi} \in \mathbb{R}$, δηλαδή ότι $K\leq\mathbb{R}$ και ότι $\zeta_p \notin K$.
Το ζ_p είναι ρίζα του $X^2 = (\zeta_p+\zeta_p^{-1})X - 1 \in K[X]$
Επομένως, αυτό είναι ανάγωγο, δηλαδή $[\mathbb{Q}(\zeta_p):K]=2$.
Η ${}^{\mathbb{Q}(\zeta_p)}/_K$ είναι *Galois* και μάλιστα $Gal({}^{\mathbb{Q}(\zeta_p)}/_K) \trianglelefteq Gal({}^{\mathbb{Q}(\zeta_p)}/_{\mathbb{Q}})$, αφού η ${}^{\mathbb{Q}(\zeta_p)}/_{\mathbb{Q}}$ αβελιανή.
Επομένως, Θεμελιώδες Θεώρημα Θεωρίας *Galois*, ${}^K/_{\mathbb{Q}}$ *Galois*.
Επομένως, σύμφωνα με την Πρόταση 21, [ο $\frac{2\pi}{p}$ είναι κατασκευάσιμος]
$\Leftrightarrow$ [$[K:\mathbb{Q}] =$ δύναμη του 2], δηλαδή [η γωνία $\theta_p := \frac{2\pi}{\pi}$ κατασκευάσιμη]

$\Leftrightarrow$ ($[\mathbb{Q}(\zeta_p) : \mathbb{Q}] =$ δύναμη του 2)
(εδώ $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = [\mathbb{Q}(\zeta_p) : K][K : \mathbb{Q}] = 2 \cdot [K : \mathbb{Q}]$)

Θεώρημα:

(Το Π_n είναι κατασκευάσιμο) $\Leftrightarrow$ ($n = 2^k p_1 p_2 \cdots p_r \mid k \geq 0, r \geq 0$ και p_i (διακεκριμένοι) πρώτοι αριθμοί της μορφής $2^{2^m} + 1$)

Απόδειξη:

Έστω $n = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s} \mid p_i \in \mathbb{P} \quad p_i \neq p_j \quad \forall i \neq j \quad m_i \geq 1$

Αν το κανονικό πολύγωνο Π_n είναι κατασκευάσιμο, τότε Πρόταση 23, κάθε Π_q, όπου $q \in \{p_1^{m_1}, p_2^{m_2}, \cdots, p_s^{m_s}\}$ είναι επίσης κατασκευάσιμο. Επομένως $(cos\theta_q, sin\theta_q)$ είναι κατασκευάσιμο. ($\theta_q := \frac{2\pi}{q}$)

Από Πρόταση 16 Κεφάλαιο 3, έπεται ότι $[\mathbb{Q}(cos\theta_q, sin\theta_q) : \mathbb{Q}] =$ δύναμη του 2.

Το $\zeta_q := cos\theta_q, +i\ sin\theta_q$, έπεται ότι $\mathbb{Q}(\zeta_q) \leq \mathbb{Q}(cos\theta_q, sin\theta_q, i) = K(i)$ και $[K(i) : K] = 2$ όπου $K = \mathbb{Q}(cos\theta_q, sin\theta_q)$ και ότι $[\mathbb{Q}(\zeta_q) : K] = [K(i) : K] = 2$

Επομένως, $[\mathbb{Q}(\zeta_q) : \mathbb{Q}] =$ δύναμη του 2.

Τώρα, ζ_q είναι μια πρωταρχική q-ρίζα της μονάδας.

Το $q = p^m, \quad [\mathbb{Q}(\zeta_q) : K\mathbb{Q}] = 2^l$

Όμως κατ΄ αναλογία, προς το ανάγωγο του ζ_p, ισχύει:

$Irr(\zeta_{p^m}, \mathbb{Q}) = X^{(p-1)p^{m-1}} + \cdots + X^{2p^{m-1}} + X^{p^{m-1}} + 1$

(χωρίς απόδειξη)

Επομένως, $[\mathbb{Q}(\zeta_q) : \mathbb{Q}] = p^{m-1}(p-1)$

(Αν $p = 2$, δεν έχουμε κάποια αντίφαση στους δύο τύπους του βαθμού επεκτάσεων.)

Αν $p \in \mathbb{P}, \quad p \neq 2$, τότε πρέπει $m = 1$ και $p - 1 =$ δύναμη του 2, έστω $p - 1 = 2^k$, δηλαδή $p = 2^k + 1$.

Γράφουμε το $k = 2^a \cdot b$ με $b > 1, \quad 2 \nmid b$.

Αν

$w := 2^{2^a} \quad p = 2^k + 1 = 2^{2^a b} + 1 = (2^{2^a})^b + 1 = w^b + 1 = (w+1)(w^{b-1} - w^{b-2} + \cdots - w + 1)$,

και $(w^{b-1} - w^{b-2} + \cdots - w + 1) > 1$, άτοπο.

Επομένως $b = 1$, δηλαδή $k = 2^a, \Rightarrow p = 2^{2^a} + 1$

Ορισμός:

Οι πρώτοι αριθμοί της μορφής $p = 2^{2^a} + 1, \quad a \geq 0$, λέγονται πρώτοι αριθμοί $Fermat$.

Επομένως, αν π_n κατασκευάσιμο $\Rightarrow\ n = 2^l \cdot p_1 \cdot p_2 \cdots p_r$, όπου p_i πρώτοι αριθμοί $Fermat$.

Αντίστροφα

Έστω $= 2^l \cdot p_1 \cdot p_2 \cdots p_r\ \mid$ με p_j πρώτους αριθμούς $Fermat\ \ p_j = 2^{2^{m_j}} + 1$

Το (π_n είναι κατασκευάσιμο) $\Leftrightarrow$ Το (π_{2^e} κατασκευάσιμο και π_{p_j} κατασκευάσιμο $\forall j = 1, 2, \cdots, r$)

Το π_{2^e} κατασκευάσιμο.

(Διχοτομούμε διαδοχικά τη γωνία $\frac{\pi}{2}$).

Αρκεί να δείξουμε ότι τα π_{p_j} είναι $(j = 1, 2, \cdots, r)$ κατασκευάσιμα.

Αν $\zeta_{p_j} := e^{\frac{2\pi i}{p_j}}$, τότε $\forall j = 1, 2, \cdots, r$ η $^{\mathbb{Q}(\zeta_{p_j})}/_{\mathbb{Q}}$ είναι $Galois$ και

$[\mathbb{Q}(\zeta_{p_j}) : \mathbb{Q}] = p_j - 1 = 2^{2^{m_j}}$, δύναμη του 2, Πρόταση 21, $\Rightarrow$ οι γωνίες $\zeta_{p_j} = \frac{2\pi}{p_j}$ κατασκευάσιμες $\Rightarrow\ \pi_{p_j}\ \ (\forall j = 1, 2, \cdots, r)$ είναι κατασκευάσιμα.

Πρώτοι αριθμοί Fermat

m	0	1	2	3	4
F_m	3	5	17	257	65537

Ο F_5 όχι πρώτος $(641 \mid F_5)$

Ο $F_5 = 641, 6700417$

Απόδειξη ότι $641 | F_5$:

$641 = 2^7 \cdot 5 + 1\ \Rightarrow\ 2^7 \cdot 5 \equiv -1(641)\ \Rightarrow\ (2^7 \cdot 5)^4 \equiv +1(64)\ \Rightarrow\ 2^{28} \cdot 5^4 \equiv +1(64)$

$641 = 2^4 + 5^4\ \Rightarrow\ 5^4 \equiv -2^4(641)$

$\Rightarrow\ \ 2^{28}(-2^4) \equiv\neq 1(641)$

$\Rightarrow\ \ -2^{32} \equiv 1(641)$

$\Rightarrow\ \ 2^{32} + 1 \equiv 0(641)$

Μέχρι το 2014 είναι γνωστό ότι η F_n είναι σύνθετος για $5 \leq n \leq 32$. Δεν έχει βρεθεί άλλος πρώτος. Αν αυτό ισχύει, τότε το συμπέρασμα θα είναι ότι, ένα κανονικό n-γωνο είναι κατασκευάσιμο με κανόνα και διαβήτη. $\Leftrightarrow\ n = 2^s \cdot 3^a \cdot 5^b \cdot 17^c \cdot 257^a \cdot 65537^e$ όπου $s \geq 0$ και $a, b, c, d, e \in \{0, 1\}$

Ο *Gauss*, στις 30 Μαρτίου 1796 ένα μήνα πριν κλείσει το 19^{ο} έτος της ζωής του ανακάλυψε τη σύνδεση μεταξύ πρώτων αριθμών $Fermat$ και κατασκευάσιμων κανονικών πολυγώνων. Στο άρθρο 365 του έργου του "$DisquisitionesArcthmeeicae$" απέδειξε ότι όταν ο p είναι πρώτος αριθμός $Fermat$, τότε ο ζ_p είναι κατασκευάσιμος με κανόνα και διαβήτη.
Ο ίδιος ισχυρίστηκε ότι και το αντίστροφο ισχύει αλλά η πρώτη δημοσιευμένη απόδειξη οφείλεται στον $Wantzel$ (1837).
Η κατασκευή ισόπλευρου τριγώνου και κανονικού 5-γώνου ήταν γνωστή από την εποχή του Ευκλείδη.
Ο *Gauss* υπολόγισε:
$cos\frac{2\pi}{17} = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{7}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17}} - \sqrt{34 + 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}$
και αυτό οδήγησε στην κατασκευή του κανονικού 17-γώνου.
Ο *Richelot* (1832) παρουσίασε μια μέθοδο κατασκευής 257-γώνου.
Τέλη του 19^{ου}-αιώνα οι $Hermes\ Von\ Linger$ εργάστηκε για 10-χρόνια για την κατασκευή κανονικού 65537-γώνου.

5.4 Η γενική εξίσωση $\mathbf{n}^{\sigma\tau ου}$ - βαθμού

Και στην παράγραφο αυτή υποθέτουμε ότι $chK = 0$.
Έστω ${}^{L}/_{K}$ επέκταση σωμάτων.

Ορισμός:

Το υποσύνολο $\{a_1, a_2, \cdots, a_n\} \leq L$ θα λέγεται αλγεβρικά ανεξάρτητο υπέρ το K :$\Leftrightarrow$ (για κάθε πολυώνυμο $f(X_1, X_2 \cdots, X_n) \in K[X_1, X_2, \cdots, X_n]$ ισχύει
$f(a_1, a_2, \cdots, a_n) = 0 \ \Leftrightarrow \ f = 0$)
Αποδεικνύεται ότι ένας ισοδύναμος ορισμός είναι: Το (a_1 είναι υπερβατικό υπέρ το K και $\forall \ r = 2, 3, \cdots, n$ το a_r είναι υπερβατικό υπέρ το $K(a_1, a_2, \cdots, a_{r-1})$
Επίσης, όπως και στην περίπτωση μιας μεταβλητής ισχύει:
Το σύνολο $\{a_1, a_2, \cdots, a_n\}$ είναι αλγεβρικά ανεξάρτητο $|_K$
$\Leftrightarrow \ K(a_1, a_2, \cdots, a_n) \ \cong \ K(X_1, X_2, \cdots, X_n)$.

Παρατήρηση: Η έννοια της αλγεβρικής ανεξαρτησίας είναι πολύ ισχυρή έναντι αυτής της γραμμικής ανεξαρτησίας.
π.χ. $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$ είναι $\mathbb{Q}$-γραμμικά ανεξάρτητο σύνολο αλλά όχι αλγεβρικά ανεξάρτητο, αφού, αν $f(X_1, X_2, X_3, X_4) = X_2X_3 - X_4$
$f(1, \sqrt{3}, \sqrt{5}, \sqrt{15}) = 0$

Έστω τώρα K σώμα, και $\{s_1, s_2, \cdots, s_n\} \subseteqq L$ ένα αλγεβρικά ανεξάρτητο $|_K$ σύνολο στοιχείων κάποιου σώματος L, $\quad K \subseteqq L$.

Ορισμός:

Το πολυώνυμο $g(X) := X^n - s_1X^{n-1} + s_2X^{n-1} - \cdots + (-1)^n s_n \in K(s_1, s_2, \cdots, s_n)[X]$ θα λέγεται γενικό πολυώνυμο n-στού βαθμού υπέρ το K.

Πρόταση 24η:

Έστω Μ ένα σώμα ανάλυσης του $g(X)$ ως προς το $K(s_1, s_2, \cdots, s_n)$
Αν $t_1, t_2, \cdots, t_n$ οι ρίζες του $g(X)$ τότε αυτές είναι αλγεβρικά ανεξάρτητες υπέρ το Κ και η ομάδα $Galois \quad Gal(^M/_{K(s_1,s_2,\cdots,s_n)}) \cong S_n$.
(χωρίς απόδειξη)

Παρατηρήσεις: Ισχύουν:
$s_1 = t_1 + t_2 + \cdots + t_n$
$s_2 = t_1t_2 + t_1t_3 + \cdots + t_1t_n + t_2t_3 + \cdots + t_2t_n + \cdots + t_{n-1}t_n$
$s_n = t_1t_2 \cdots t_n$
Τα s_i, σαν συναρτήσεις τ.ω. $t_1, t_2, \cdots, t_n$ λέγονται στοιχειώδεις συμμετρικές συναρτήσεις των $t_1, t_2, \cdots, t_n$.
Ισχύει:
Όλες οι ρητές συμμετρικές συναρτήσεις των $t_1, t_2, \cdots, t_n$ υπέρ το Κ εκφράζονται σαν ρητές συναρτήσεις των $s_1, s_2, \cdots, s_n$ υπέρ το Κ, δηλαδή ανήκουν στο $K(s_1, s_2, \cdots, s_n)$.
(Η πρόταση αυτή λέγεται Θεμελιώδες Θεώρημα των Ρητών συμμετρικών συναρτήσεων)

Παράδειγμα:

(i) $n = 2 \quad X_1^2 + X_2^2 = (X_1 + X_2)^2 - 2X_1X_2 = s_1^2 - 2s_2$

(i) $X_1^3 + X_2^3 = (X_1 + X_2)^3 - 3X_1X_2(X_1 + X_2) = s_1^3 - 3s_2s_1$

Από τα παραπάνω προκύπτει το

Θεώρημα ($Abel$):

Για $n \geq 5$, η γενική εξίσωση n-στού βαθμού, δεν είναι επιλύσιμη με ριζικά.

Ερώτημα: Μας δίνεται μα πεπερασμένη ομάδα, έστω G.

Υπάρχει επέκταση $Galois \quad {}^{L}/_{K}$ τ.ω. $Gal({}^{L}/_{K}) \cong G$;

Η απάντηση είναι θετική.

. Βήμα 1^0

(Θεώρημα $Cayley$)

Αν G πεπερασμένη ομάδα τάξης n τότε και η G περιέχεται, ισόμορφα, στην S_n,

δηλαδή μπορούμε να θεωρήσουμε ότι $G \leq S_n$

Απόδειξη:

$\forall a \in G$, ορίζουμε: $\sigma_a : G \ni x \longmapsto ax \in G$

Η σ_a είναι αμφιμονοσήμαντη, δηλαδή $\sigma_a \in S_n$.

Τώρα, η $\phi : G \to S_n$ όπου $a \longmapsto \sigma_a$ είναι μονομορφισμός ομάδων.

Επομένως $G \leq S_n$.

. Βήμα 2^0

Έστω ότι $\#G = n$.

Θεωρούμε την επέκταση $Galois \quad {}^{L}/_{F}$

$L = K(t_1, t_2, \cdots, t_n)$ και

$F := K(s_1, s_2, \cdots, s_n)$,

Σύμφωνα με τα προηγούμενα: $Gal({}^{L}/_{F}) \cong S_n$.

Σύμφωνα με το Θεμελιώδες Θεώρημα της Θεωρίας $Galois$:

$$\begin{array}{ccc} L & \longleftrightarrow & \{Id_L\} \\ | & & | \\ E & \longleftrightarrow & G \\ | & & | \\ F & \longleftrightarrow & Gal({}^{L}/_{F}) \\ & & \cong S_n \end{array}$$

αν $E = \Phi(G)$ η ${}^{L}/_{E}$ είναι $Galois$ και $Gal({}^{L}/_{E}) \cong G$

Ερώτημα: Τι γίνεται όμως, αν περιορίσουμε το πρόβλημα:

Δίνεται η πεπερασμένη ομάδα G.

Υπάρχει επέκταση $Galois \quad {}^{L}/_{\mathbb{Q}}$ (Εδώ το ότι ζητούμε να είναι ομάδα $Galois$ υπέρ το $\mathbb{Q}$ είναι το σημαντικό, δηλαδή κρατούμε το σώμα $\mathbb{Q}$, σταθερό.) τ.ω. $Gal({}^{L}/_{\mathbb{Q}}) \cong G$;

Το πρόβλημα είναι μέχρι σήμερα ανοιχτό και η προσπάθεια επίλυσης του βρίσκεται υπό εξέλιξη.

Λέγεται, αντίστροφο πρόβλημα της Θεωρίας του *Galois*.

5.5 Επίλυση της γενικής εξίσωσης $2^{ου}$, $3^{ου}$ και $4^{ου}$ βαθμού

Η S_n για $n = 2, 3$ και 4 είναι επιλύσιμη, συνεπώς κάθε υποομάδα της είναι επιλύσιμη.
Συνεπώς, η γενική εξίσωση $2^{ου}$, $3^{ου}$ και $4^{ου}$ βαθμού είναι επιλύσιμη με ριζικά.
(Υπενθυμίζω ότι $chK = 0$)

- Η γενική εξίσωση $2^{ου}$ βαθμού.
  $f(X) = X^2 + s_1X + s_2 \in K[X]$
  Η $f(X) = 0$, έχει δύο ρίζες, έστω x_1, x_2.
  Η ομάδα $S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix} \right\}$
  Η αντιμετάθεση (1 2) εναλλάσσει τις ρίζες x_1 και x_2.
  Επομένως, η $(x_1 - x_2)^2$ παραμένει αναλλοίωτη κάτω από τη δράση της S_2.
  Επομένως, Θεμελιώδες Θεώρημα των συμμετρικών συναρτήσεων,
  $(x_1 - x_2)^2 \in K(s_1, s_2)$.
  Πράγματι, $(x_1 - x_2)^2 = x_1^2 + x_2^2 - x_1x_2 = (x_1 - x_2)^2 - 4x_1x_2 = s_1^2 - 4s_2^2$.
  Από αυτό, προκύπτει ότι $x_1 - x_2 = \pm\sqrt{s_1^2 - 4s_2}$.
  Επειδή και $x_1 + x_2 = s_1 \ \Rightarrow \ X_{1,2} = \frac{s_1 \pm \sqrt{s_1^2 - 4s_2}}{2}$.

- Η γενική εξίσωση $3^{ου}$ βαθμού
  $f(X) = X^3 - s_1X^2 + s_2X - s_3 \in K(s_1, s_2, s_3)[X]$
  Η εξίσωση $f(X) = 0$, έχει 3-ρίζες, έστω x_1, x_2, x_3.
  Η S_3 είναι επιλύσιμη
  (υπενθυμίζουμε ότι $\{1\} \trianglelefteq A_3 \trianglelefteq S_3$ και $\#(\frac{S_3}{A_3}) = 2, \quad \#(\frac{A_3}{\{1\}}) = 3$)
  Επισυνάπτουμε, αν χρειαστεί, στο K μια πρωταρχική 3-ρίζα του 1, έστω ω.
  Θεωρούμε το στοιχείο $y = x_1 + \omega x_2 + \omega^2 x_3$.
  Η
  $A_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix} \right\}$
  Η μετάθεση $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ μεταθέτει τις ρίζες $x_1, x_2, x_3, \quad (x_1 \longrightarrow x_2 \longrightarrow x_3 \longrightarrow x_1)$,

δηλαδή $\begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}$

$\left(\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, y\right) = x_2+\omega x_3+\omega^2 x_1 = \omega^3 x_2+\omega^4 x_3+\omega^2 x_1 = \omega^2(x_1+\omega x_2+\omega^2 x_3) = \omega^2 y$

$\left(\begin{pmatrix} 1 & 3 & 2 \end{pmatrix}, y\right) = x_3+x_1\omega+x_2\omega^2 = x_3\omega^3+x_1\omega+x_2\omega^2 = \omega(x_1+x_2\omega+x_3\omega^2) = \omega y$

Επομένως, το y^3 παραμένει σταθερό (αναλλοίωτο) κάτω από την δράση της A_3.

($\forall \sigma \in A_3, \quad \sigma(y^3) = y^3$,

- Α, αν $\sigma = (1)$ προφανές
- αν $\sigma = (1\ 2\ 3), \quad (\sigma, y^3) = (\sigma, y)^3 = (\omega^2 y)^3 = y^3$
- αν $\sigma = (1\ 3\ 2), \quad (\sigma, y^3) = (\omega y)^3 = y^3$)

Ομοίως, αν $z = x_1 + \omega^2 x_2 + \omega x_3$ το z^3 παραμένει σταθερό από την A_3.

Τώρα αν τ περιττή μετάθεση της S_3, $\tau \in \{(1\ 2), (1\ 3), (2\ 3)\}$

π.χ. ας πάρουμε $\tau = (1\ 2)$

$\tau y = x_2 + x_1\omega + x_3\omega^2 = A_2\omega^3 + x_1\omega + x_3\omega^2 = \omega(x_1 + x_2\omega^2 + x_3\omega) = \omega z$

$\Rightarrow \ \tau(y^3) = \tau(y)^3 = (\omega z)^3 = \omega^3 z^3 = z^3$

Το ίδιο ισχύει και για την δράση των $(1\ 3)$ και $(2\ 3)$.

Επομένως και οι $y^3 + z^3$ και $y^3 z^3$ παραμένουν αναλλοίωτες από την δράση της S_3.

Συνεπώς, $y^3 + z^3 \in K(s_1, s_2, s_3)$ και $y^3 z^3 \in K(s_1, s_2, s_3)$.

Τα $y^3,\ z^3$ είναι ρίζες δευτεροβάθμιας εξίσωσης.

Συνεπώς μπορούμε να υπολογίσουμε τα $y,\ z$.

Έτσι έχουμε:

$$\left\{ \begin{array}{l} s_1 = x_1 + x_2 + x_3 \\ y = x_1 + \omega x_2 + \omega^2 x_3 \\ z = x_1 + \omega^2 x_2 + \omega x_3 \end{array} \right\}$$

Προσθέτουμε κατά μέλη:

$X_1 = \frac{1}{3}(s_1 + y + z)$,

$s_1 + \omega^2 y + \omega z = (x_1 + x_2 + x_3) + (\omega^2 x_1 + x_2 + \omega x_3) + (\omega x_1 + x_2 + \omega^2 x_3) = 3x_2$

$$\text{Δηλαδή} \quad \left. \begin{array}{l} x_1 = \frac{1}{3}(s_1 + y + z) \\ x_2 = \frac{1}{3}(s_1 + \omega^2 y + \omega z) \\ x_3 = \frac{1}{3}(s_1 + \omega y + \omega^2 z) \end{array} \right\} \quad (*)$$

Τώρα, για μια μικρή απλοποίηση η $f(X) = X^3 - s_1 X^2 + s_2 X - s_3 = 0$ μπορεί, με $X := \frac{s_1}{3} + y$, να μας δώσει ισοδύναμη εξίσωση, χωρίς δευτεροβάθμιο όρο, που θα

έχει την μορφή

$X^3 + pX + q = 0 \quad (p \neq 0)$ (Αν $p = 0$ απλή!)

Για $X = y - \frac{p}{3y}$ η εξίσωση γίνεται

$y^3 - \frac{p^3}{27y^3} + q = 0$

Αν θέσουμε $\phi := y^3$, έχουμε $\phi^2 + q\phi - \frac{p^3}{27} = 0$ (λέγεται επιλύουσα της αρχικής)

Εδώ οι ρίζες της επιλύουσας είναι τα y^3 και z^3 τ.ω. $y \cdot z = -\frac{p}{3}$ και οι λύσεις είναι οι λύσεις της $(*)$ για $s_1 = 0$.

Οι ρίζες της επιλύουσας είναι:

$y^3 = \phi_1 = -\frac{q}{2} + \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}$ και

$z^3 = \phi_2 = -\frac{q}{2} - \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}$

Επομένως

$y = \sqrt[3]{-\frac{q}{2} + \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}}$ και

$z = \sqrt[3]{-\frac{q}{2} - \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}}$

τ.ω. $(y \cdot z = -\frac{p}{3})$

Η λύση είναι πλέον αυτή της $(*)$ για $s_1 = 0$ και y, z τα παραπάνω.

Παράδειγμα: $X^3 + 6X + 2 = 0$

$p = 6, \quad q = 2, \Rightarrow \quad \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3} = \sqrt{1 + 8} = 3$

$y = \sqrt[3]{-1 + 3} = \sqrt[3]{2}$

$z = \sqrt[3]{-1 - 3} = \sqrt[3]{-4}$

$y \cdot z = \sqrt[3]{2} \cdot \sqrt[3]{-4} = -2 = -\frac{p}{3}$

και οι τρεις λύσεις δίνονται από $(*)$ για $s_1 = 0$.

- Ανάλογη μελέτη επιδέχεται η γενική εξίσωση $4^{ου}$-βαθμού.

5.6 Η ομάδα *Galois* πολυωνύμων $3^{ου}$ και $4^{ου}$ βαθμού

Έστω $f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in \mathbb{Q}[X]$

Σε κάποιο σώμα ανάλυσης το $f(X)$ γράφεται:

$f(X) = (X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n)$.

Έστω $\Delta(f) = \prod_{1\le i<j\le n} (\alpha_i - \alpha_j)$ και $D(f) = \Delta(f)^2 = \prod_{1\le i<j\le n} (\alpha_i - \alpha_j)^2$.

Ορισμός:

Ο αριθμός $D(f)$ λέγεται διακρίνουσα του $f(X)$.

Ιδιότητες:

1. Αν $\sigma \in Gal(^{f(X)}/_{\mathbb{Q}}) \le S_n$
   τότε $\sigma(D(f)) = D(f)$, δηλαδή
   $\sigma(\Delta(f)^2) = \Delta(f)^2, \quad \sigma(\Delta(f)) = \pm\Delta(f)$
2. Ισχύει $\sigma(\Delta(f)) = \Delta(f) \Leftrightarrow \sigma \in A_n$ και $\sigma(\Delta(f)) = -\Delta(f) \Leftrightarrow \sigma \in S_n \setminus A_n$
3. $Gal(^{f(X)}/_{\mathbb{Q}}) \le A_n \Leftrightarrow D(f) \in \mathbb{Q}^2$

Τώρα, αν $f(X) = X^3 + pX + q \in \mathbb{Q}[X]$ η $D(f) = -4p^3 - 27q^2$.

Πρόταση $25^{η}$:

Αν $f(X) = X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$ ανάγωγο, $G := Gal(^{f(X)}/_{\mathbb{Q}})$ και $D(f)$ η διακρίνουσα αυτού.

Ισχύουν:

$G \cong A_3 \Leftrightarrow D(f) \in \mathbb{Q}^2$

$G \cong S_3 \Leftrightarrow D(f) \notin \mathbb{Q}^2$

Παραδείγματα:

1. $f(X) = X^3 - 3X + 1 \in \mathbb{Q}[X]$ ανάγωγο $|_{\mathbb{Q}}$,
   $D(f(X)) = 81 = 9^2 \Rightarrow Gal(^{f(X)}/_{\mathbb{Q}}) \cong A_3$

2. $f(X) = X^3 + 3X + 1 \in \mathbb{Q}[X]$ ανάγωγο $|_{\mathbb{Q}}$
   $D(f(X)) = -135 \notin \mathbb{Q}^2 \Rightarrow Gal(^{f(X)}/_{\mathbb{Q}}) \cong S_3$.

Έστω τώρα $f(X) = X^4 + aX^3 + bX^2 + cX + d \in \mathbb{Q}[X]$,ανάγωγο $|_{\mathbb{Q}}$.
Επομένως $Gal(^{f(X)}/_{\mathbb{Q}}) \leq S_4$
Αν $f(X) := (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)(X - \alpha_4)$

$\beta_1 := \alpha_1\alpha_2 + \alpha_3\alpha_4$

$\beta_2 := \alpha_1\alpha_3 + \alpha_2\alpha_4$

$\beta_3 := \alpha_1\alpha_4 + \alpha_2\alpha_3$

Το πολυώνυμο $r(X) := (X - \beta_1)(X - \beta_2)(X - \beta_3)$ λέγεται επιλύουσα του $f(X)$
Απόδεικνύεται ότι: $r(X) = X^3 - bX^2 + (ac - 4d)X + 4bd - a^2d - c^2 \in \mathbb{Q}[X]$.
Η ομάδα $Gal(^{f(X)}/_{\mathbb{Q}})$ είναι ισόμορφη με κάποια μεταβατική $(transitive)$ υποομάδα της S_4.
Έστω $L = \mathbb{Q}(\beta_1, \beta_2, \beta_3)$ και $m := [L : \mathbb{Q}]$

Θεώρημα του Kaplansky:

Έστω $f(X) = X^4 + aX^2 + b \in \mathbb{Q}[X]$, ανάγωγο $|_{\mathbb{Q}}$.

(i) Αν $b = \square$ στο $\mathbb{Q}$, τότε $Gal(^{f(X)}/_{\mathbb{Q}}) \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}/_{2\mathbb{Z}} \cong V$

(ii) Αν $b \neq \square$ και $b(a^2 - 4b) = \square$ στο $\mathbb{Q}$, τότε $Gal(^{f(X)}/_{\mathbb{Q}(Q)}) \cong \mathbb{Z}_4 = {}^{\mathbb{Z}}/_{4\mathbb{Z}}$

(iii) Αν $b \neq 0$ και $b(a^2 - 4b) \neq \square$ στο $\mathbb{Q}$, τότε $Gal(^{f(X)}/_{\mathbb{Q}}) \cong D_4$

Παραδείγματα:

1. Έστω $f(X) = X^4 + 1 \in \mathbb{Q}[X]$
   Το $b = 1 = \square = 1^2$ στο $\mathbb{Q} \Rightarrow Gal(^{f(X)}/_{\mathbb{Q}}) \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}/_{2\mathbb{Z}}$

2. Αν $f(X) = X^4 + 4X + 2 \in \mathbb{Q}[X]$,
   το $b = 2 \neq \square$ στο $\mathbb{Q}$,
   $b(a^2 - 4b) = 2(16 - 8) = 16 = \square$ στο $\mathbb{Q} \Rightarrow Gal(^{f(X)}/_{\mathbb{Q}(Q)}) \cong {}^{\mathbb{Z}}/_{4\mathbb{Z}}$

3. Αν $f(X) = X^4 + 2X^2 + 2 \in \mathbb{Q}$.
   Εδώ $b = 2 \neq \square$ στο $\mathbb{Q}$
   $b(a^2 - 4b) = 2(4 - 8) = -8 \neq \square$ στο $\mathbb{Q}$.

Συνεπώς $Gal(^{f(X)}/_{\mathbb{Q}}) \cong D_4$

5.7 Πεπερασμένα σώματα

Θεώρημα 1ο:

(*i*) Αν Κ πεπερασμένο σώμα, τότε $\exists p \in \mathbb{P}$ και $n \geq 1$ τ.ω. $|K| = p^n$.
Κάθε στοιχείο του Κ είναι μια ρίζα του πολυωνύμου $X^{p^n} - X$ και το Κ είναι ένα σώμα ανάλυσης του πολυωνύμου αυτού υπέρ το $\mathbb{F}_p = {}^{\mathbb{Z}}/_{p\mathbb{Z}}$

(*ii*) Έστω $p \in \mathbb{P}$ και $n \geq 1$.
Υπάρχει (*modulo* ισομορφία) ακριβώς ένα σώμα με p^n-στοιχεία.
(χωρίς απόδειξη)

Πρόταση 26η:

Η ομάδα $\mathbb{F}^*_{pn}$ είναι κυκλική.
(χωρίς απόδειξη)

Θεώρημα 2ο:

Αν $q = p^l$, $p \in \mathbb{P}$, $\mathbb{F}_q$ το σώμα με q στοιχεία και $\begin{matrix} \mathbb{F}_{q^n} \\ | \\ \mathbb{F}_q \end{matrix}$
τότε η επέκταση ${}^{\mathbb{F}_{q^n}}/_{\mathbb{F}_q}$ είναι *Galois* (προφανώς $[\mathbb{F}_{qn} : \mathbb{F}_q] = n$) και μάλιστα κυκλική.
Η ομάδα *Galois* της επέκτασης αυτής παράγεται από τον $\mathbb{F}_q$-αυτομορφισμό του $\mathbb{F}_{qn}$

$$\sigma_q : \left\{ \begin{array}{c} \mathbb{F}_{qn} \longrightarrow \mathbb{F}_{q^n} \\ x \longmapsto x^q \end{array} \right\}$$

(χωρίς απόδειξη)

Πρόταση 27η:

Το $X^4 + 1 \in \mathbb{Z}[X]$ είναι ανάγωγο $|_{\mathbb{Q}}$, ενώ $\forall p \in \mathbb{P}$ το $X^4 + 1 \in \mathbb{F}_p[X]$ δεν είναι ανάγωγο στο $\mathbb{F}_p$.

Απόδειξη:

Για $p = 2$, προφανώς $(X^4 + 1) = (X + 1)^4$ όχι ανάγωγο.

Αν τώρα $p \neq 2$, τότε $p \equiv 1, 3, 5, 7 (mod 8)$, δηλαδή $p^2 - 1 = 8 \cdot k$.

Συνεπώς $p \equiv 1, 3, 5, 7 (mod 8)$, οπότε $p^2 - 1 \equiv 0 (mod 8)$.

Επομένως

$X^{p^2-1} - 1 = (X^8)^k - 1 = (X^8 - 1)((X^8)^{k-1} + \cdots + 1) \Rightarrow (X^8 - 1) \mid (X^{p^2-1} - 1)$

Τώρα $X^8 - 1 = (X^4 - 1)(X^4 + 1) \Rightarrow (X^4 + 1) \mid (X^8 - 1)$

Επίσης $X^{p^2-1} - 1 \mid X(X^{p^2-1} - 1) = X^{p^2} - X$

Τελικά $[(X^4 + 1) \mid (X^{p^2} - X), \quad \forall p \in \mathbb{P} \setminus \{2\}]$

Επομένως, όλες οι ρίζες του $X^4 + 1$ είναι και ρίζες του $X^{p^2} - X$, δηλαδή στοιχεία του σώματος $\mathbb{F}_{p^2}$.

Αυτό σημαίνει ότι η επέκταση του προκύπτει από οποιαδήποτε ρίζα του $X^4 + 1$ έχει βαθμό το πολύ 2 υπέρ το $\mathbb{F}_p$, αφού ανήκουν στο $\mathbb{F}_{p^2}$, ενώ $deg(X^4 + 1) = 4$.

Άρα το $X^4 + 1$ δεν μπορεί να είναι ανάγωγο.

— Τέλος. —