Θέματα Άλγεβρας και Γεωμετρίας Ι

Άπειρη Θεωρία Galois.

Ονομ/νο: Νούλας Δημήτριος
ΑΜ:
email:

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών
ΙΔΡΥΘΕΝ ΤΟ 1837

Περιεχόμενα

1 Κλασική Θεωρία Galois

Ορισμός. *Έστω $F \subseteq K$ εγκλεισμός σωμάτων. Το K θα λέγεται επέκταση του F και θα συμβολίζεται με K/F.*

Παρατηρούμε ότι με τις πράξεις:

$$K \times K \longrightarrow K \qquad F \times K \longrightarrow K$$

$$(x, y) \longmapsto x + y \qquad (\lambda, x) \longmapsto \lambda x$$

Το K είναι διανυσματικός χώρος υπεράνω του F και συμβολίζουμε την διάσταση του με $[K : F]$. Αν $[K : F] < \infty$ θα λέμε ότι η επέκταση K/F είναι πεπερασμένη.

Για παράδειγμα, έχουμε $[\mathbb{C} : \mathbb{R}] = 2$ και αν $K = \mathbb{Z}_2[x]/(x^2 + x + 1)$ τότε $[K : \mathbb{Z}_2] = 2$.

Ορισμός. *Έστω K/F και $a \in K$. Το a θα λέγεται αλγεβρικό υπεράνω του F αν υπάρχει $f(x) \in F[x]$ τέτοιο ώστε $f(a) = 0$. Αν αυτό ισχύει για κάθε $a \in K$ τότε λέμε ότι η επέκταση είναι αλγεβρική.*

Πρόταση 1. *Έστω K/F με $[K : F] < \infty$. Τότε K/F αλγεβρική.*

Απόδειξη.

Έστω $b \in K$. Θεωρούμε το σύνολο των δυνάμεων $\{1, x, x^2, \ldots, x^n\}$, όπου $n = [K : F]$. Αυτό το σύνολο περιέχει $n + 1$ στοιχεία σε έναν διανυσματικό χώρο διάστασης n, άρα τα στοιχεία είναι γραμμικά εξαρτημένα. Συνεπώς, υπάρχουν $a_i \in F$ όχι όλα μηδέν ώστε:

$$a_0 + a_1 b + \ldots + a_n b^n = 0$$

δηλαδή το b είναι ρίζα του πολυωνύμου $f(x) = a_0 + a_1 x + \ldots a_n x^n \in F[x]$. Το τυχόν $b \in K$ ειναι αλγεβρικό υπεράνω του F, συνεπώς η επέκταση K/F είναι αλγεβρική. □

Θεώρημα 1 (Κανόνας Πύργων)**.** *Άν K/E και E/F πεπερασμένες επεκτάσεις τότε K/F πεπερασμένη και επιπλέον:*

$$[K : F] = [K : E][E : F]$$

Απόδειξη.

Έστω $\{a_1, \ldots a_n\}$ μια βάση του E ως F-διανυσματικός χώρος και $\{b_1, \ldots, b_m\}$ μια βάση του K ως E-διανυσματικός χώρος. Τα στοιχεία $a_i b_j$ για $i = 1, \ldots, n$ και $j = 1, \ldots, m$ θα αποτελούν βάση του K ως F-διανυσματικού χώρου. Πράγματι, έστω $c \in K$. Τότε υπάρχουν $r_i \in E$ τέτοια ώστε:

$$c = r_1 b_1 + r_2 b_2 + \ldots r_m b_m$$

Για κάθε i υπάρχουν $s_{i1}, \ldots s_{in} \in F$ με $r_i = s_{i1} a_1 + \ldots + s_{in} a_n$. Δηλαδή έχουμε:

$$c = s_{11} a_1 b_1 + \ldots + s_{1n} a_n b_n + s_{21} a_1 b_2 + \ldots s_{2n} a_n b_2 + \ldots + s_{m1} a_1 b_m + \ldots + s_{mn} a_n b_m$$

άρα τα στοιχεία $a_i b_j$ παράγουν τον διανυσματικό χώρο K υπεράνω του F. Έστω $r_{ij} \in F$ με $\sum_{i=1,j=1}^{n,m} r_{ij} a_i b_j = 0$. Τότε

$$\sum_{j=1}^{m} \left(\sum_{i=1}^{n} r_{ij} a_i \right) b_j = 0$$

Από την γραμμική ανεξαρτησία των b_j τα αθροίσματα που είναι συντελεστές των b_j είναι 0. Στη συνέχεια, από την ανεξαρτησία των a_j επεται ότι τα r_{ij} είναι όλα 0. Άρα τα στοιχεία $a_i b_j$ είναι γραμμικά ανεξάρτηκτα πάνω από το F. □

Ορισμός. *Έστω K/F. Ονομάζουμε αλγεβρική κλειστότητα του F στο K το σώμα:*

$$\overline{F} = \{a \in K : \text{ το } a \text{ είναι αλγεβρικό υπεράνω του } F\}$$

Ορισμός. *Έστω K/F και $S \subseteq K$ με $F(S)$ συμβολίζουμε την τομή όλων των υποσωμάτων του K που περιέχουν το F και το S. Το $F(S)$ είναι σώμα και $F \subseteq F(S) \subseteq K$. Αν $S = \{a_1, \ldots, a_n\}$ τότε γράφουμε $F(a_1, \ldots, a_n)$.*

Πρόταση 2. *Έστω K/F και $a_1, \ldots a_n \in K$. Έχουμε ότι το $F(a_1, \ldots, a_n)$ είναι ίσο με:*

$$\left\{ \frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} \in K : \quad f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n], g(a_1, \ldots, a_n) \neq 0 \right\}$$

Απόδειξη.

Το παραπάνω σύνολο, έστω E, είναι σώμα με $F \subseteq E \subseteq K$ και περιέχει τα $a_1, \ldots, a_n$. Από τον παραπάνω ορισμό έχουμε $F(a_1, \ldots, a_n) \subseteq E$. Αν L σώμα με $F \subseteq L$ και $a_1, \ldots a_n \in L$ τότε

$$\frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} = f(a_1, \ldots, a_n) g(a_1, \ldots, a_n)^{-1} \in L$$

από τον ορισμό του σώματος, για κάθε $f, g \in F[x_1, \ldots, x_n]$ με $g(a_1, \ldots, a_n) \neq 0$. Άρα $E \subseteq L$. Σαν L μπορούμε να θεωρήσουμε το $F(a_1, \ldots, a_n)$, από όπου έπεται το ζητούμενο. □

Έστω a αλγεβρικό στοιχείο υπεράνω κάποιου σώματος F. Θεωρούμε το πολυώνυμο $p(x) \in F[x]$ ελαχίστου βαθμού που έχει ρίζα το a. Εφόσον το F είναι σώμα μπορούμε να υποθέσουμε ότι το p είναι μονικό καθώς μπορούμε να το πολλαπλασιάσουμε με τον αντίστροφο του μεγιστοβάθμιου συντελεστή. Επιπλέον, αυτό το πολυώνυμο είναι μοναδικό. Αν δεν είναι και έχουμε $p(x), g(x)$ με αυτές τις ιδιότητες, τότε το $p(x) - g(x) \in F[x]$ θα έχει ρίζα το a και θα είναι βαθμού μικρότερου του $p(x)$ δηλαδή θα είναι βαθμού 0 από την υπόθεσή μας.

Ορισμός. *Για ένα a που ανήκει σε κάποια επέκταση και είναι αλγεβρικό στοιχείο υπεράνω ενός σώματος F λέμε το παραπάνω πολυώνυμο $p(x)$ ως ελάχιστο πολυώνυμο του a υπεράνω του F και το συμβολίζουμε με $Irr(a, F)$.*

Πρόταση 3. *Έστω K/F με a αλγεβρικό στοιχείο υπεράνω του F. Τότε:*

(1) *$Irr(a, F)$ είναι ανάγωγο στο $F[x]$.*

(2) *Αν $g(x) \in F[x]$ τότε $g(a) = 0 \iff Irr(a, F) | g(x)$.*

(3) *Αν $n = deg(Irr(a, F))$ τότε τα $1, a, a^2, \ldots, a^{n-1}$ αποτελούν βάση του $F(a)$ υπεράνω του F.*

Απόδειξη.

(1) Έχουμε από ορισμό $deg(Irr(a, F)) \geq 1$. Αν το $Irr(a, F)$ δεν ήταν ανάγωγο υπεράνω του F, τότε το a θα ήταν ρίζα κάποιου μονικού γνήσιου παράγοντα του $Irr(a, F)$, πράγμα αδύνατο από τον ορισμό ελαχίστου πολυωνύμου.

(2) Αν $Irr(a, F) | g(x)$ τότε εφόσον το $Irr(a, F)$ έχει ρίζα το a παίρνουμε ότι

$$g(a) = h(a) Irr(a, F)(a) = 0$$

Αντίστροφα, αν $g(a) = 0$ τότε

$$g(x) = h(x) Irr(a, F)(x) + r(x)$$

με $deg(r(x)) < deg Irr(a, F)$. Άρα $r(a) = Irr(a, F)(a) = 0$ και άρα από ορισμό ελαχίστου πολυωνύμου το $r(x)$ είναι το μηδενικό πολυώνυμο.

(3) Αν υπάρχουν $c_i \in F$, όχι όλα μηδέν, τέτοια ώστε $c_0 + c_1 a + \ldots + c_{n-1}a^{n-1}$ τότε αυτά ορίζουν πολυώνυμο στο $F[x]$ βαθμού $n-1$ με ρίζα το a το οποίο είναι άτοπο. Άρα τα $\{1, \ldots, a^{n-1}\}$ είναι γραμμικά ανεξάρτητα. Για να δείξουμε ότι παράγουν και τον χώρο θα αποδείξουμε πρώτα ότι $F(a) = \{f(a) : f(x) \in F[x]\}$.

Πράγματι, αν $p(x) = Irr(a, F)$ τότε ο δακτύλιος $F[x]/(p(x))$ είναι σώμα. Θεωρούμε τον ομομορφισμό εκτίμησης $\phi_a : F[x] \to F(a), f(x) \mapsto f(a)$. Με βάση το πρώτο θεωήρημα ισομορφισμών δακτυλίων παίρνουμε ότι οι δακτύλιοι, δηλαδή τα σώματα σε αυτή την περίπτωση, $F[x]/(p(x))$ και $im\phi_a$ είναι ισόμορφα. Θα δείξουμε ότι $im\phi_a = F(a)$. Έχουμε $im\phi_a = \{f(a) : f(x) \in F[x]\}$ και άρα $im\phi_a \subseteq F(a)$ από την προηγούμενη πρόταση. Από την άλλη μεριά, θεωρώντας σταθερά πολυώνυμα έχουμε $F \subseteq im\phi_a$ και $a \in im\phi_a$. Επειδή $im\phi_a$ είναι σώμα παίρνουμε $F(a) \subseteq im\phi_a$ και συνεπώς $im\phi_a = F(a)$.

Άρα έστω $b \in F(a)$, τότε υπάρχει $f(x) \in F[x]$ με $b = f(a)$. Από Ευκλείδεια διαίρεση του $f(x)$ με το $p(x)$ έχουμε ότι $f(a) = r(a)$ όπου r το υπόλοιπο της διαίρεσης και $deg(r(x)) < n$. Δηλαδή

$$b = r(a) = r_0 + r_1 a + \ldots + r_{n-1}a^{n-1}$$

δηλαδή παράγουν τον χώρο $F(a)$.

□

Πόρισμα 1. *$[F(a) : F] < \infty$ αν και μόνο αν το a είναι αλγεβρικό υπεράνω του F.*

Απόδειξη.

Αν η επέκταση $F(a)/F$ είναι πεπερασμένη έχουμε δείξει ότι είναι αλγεβρική και περιέχει το a, άρα το a είναι αλγεβρικό υπεράνω του F. Αντίστροφα, αν το a είναι αλγεβρικό υπεράνω του F στο 3) της προηγούμενη πρόταση δείξαμε ότι $[F(a) : F] = deg(Irr(a, F)) < \infty$.

□

Θεώρημα 2. *Αν K/E και E/F είναι αλγεβρικές επεκτάσεις τότε και η επέκταση K/F είναι αλγεβρική.*

Απόδειξη.

Έστω $a \in K$ και $f(x) = Irr(a, E) = a_0 + a_1 x + \ldots x^n$ το ελάχιστο πολυώνυμο του a υπεράνω του E. Καθώς η επέκταση E/F είναι αλγεβρική τότε και η επέκταση E_0/F είναι αλγεβρική ως πεπερασμένη, όπου $E_0 = F(a_0, \ldots, a_{n-1})$. Επιπλέον, το $f(x)$ ανήκει και στο $E_0[x]$ και άρα το a είναι αλγεβρικό υπεράνω του $E_0[x]$. Επομένως:

$$[E_0(a) : F] = [E_0(a) : E_0][E_0 : F] < \infty$$

Καθώς $F(a) \subseteq E_0(a)$ έχουμε ότι $[F(a) : F] < \infty$, δηλαδή το τυχόν $a \in K$ είναι αλγεβρικό υπεράνω του F. Άρα η επέκταση K/F είναι αλγεβρική. □

1.1 Αυτομορφισμοί

Έστω K ένα σώμα. Ένας ισομορφισμός δακτυλιών $K \to K$ ονομάζεται αυτομορφισμός του K και η ομάδα των αυτομορφισμών με πράξη την σύνθεση συμβολίζεται με $Aut(K)$. Καθώς ασχολούμαστε με επεκτάσεις πρέπει να θεωρήσουμε απεικονίσεις επεκτάσεων. Έστω K, L επεκτάσεις ενός σώματος F. Ένας F-ομομορφισμός $\tau : K \to L$ είναι ένας ομομορφισμός δακτυλίων τέτοιος ώστε $\tau(a) = a$ για κάθε $a \in F$. Δηλαδή, $\tau|_F = id_F$. Αν ο τ είναι 1-1 και επί τότε λέγεται F-ισομορφισμός. Αν επιπλέον $K = L$, τότε λέγεται F-αυτομορφισμός του K.

Ορισμός (Ομάδα Galois)**.** *Έστω K/F. Ορίζουμε $Gal(K/F)$ να είναι οι F-αυτομορφισμοί του K με πράξη την σύνθεση.*

Λήμμα 1. *Έστω $K = F(X)$ με $X \subseteq K$. Αν $\sigma, \tau \in Gal(K/F)$ με $\sigma|_X = \tau|_X$ τότε $\sigma = \tau$. Συνεπώς, οι F-αυτομορφισμοί του K καθορίζονται πλήρως από τις εικόνες τους στο σύνολο X που επισυνάπτουμε.*

Απόδειξη.

Έστω $b \in F(X)$, τότε υπάρχουν $\{a_1, \ldots, a_n\} \subseteq X$ με $b \in F(a_1, \ldots, a_n)$ και άρα αυτό γράφεται ως

$$b = \frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)}$$

Επειδή τα σ, τ διατηρούν την πρόσθεση και τον πολλαπλασιασμό στο σώμα, καθώς και κρατάνε σταθερό το F έχουμε ότι το $\sigma(b)$ είναι ίσο με:

$$\sigma\left(\frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)}\right) = \frac{f(\sigma(a_1), \ldots, \sigma(a_n))}{g(\sigma(a_1), \ldots, \sigma(a_n))} = \frac{f(\tau(a_1), \ldots, \tau(a_n))}{g(\tau(a_1), \ldots, \tau(a_n))} = \tau\left(\frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)}\right)$$

το οποίο είναι ίσο με $\tau(b)$. Άρα οι αυτομορφισμοί του K που κρατάνε το F σταθερό καθορίζονται πλήρως από τις εικόνες τους στο X. □

Λήμμα 2. *Έστω $\tau : K \to L$ ένας F-ομομορφισμός και $a \in K$ αλγεβρικό υπεράνω του F. Αν $f(x) \in F[x]$ με $f(a) = 0$ τότε $f(\tau(a)) = 0$. Δηλαδή το τ μεταθέτει τις ρίζες του $Irr(a, F)$. Συνεπώς $Irr(a, F) = Irr(\tau(a), F)$.*

Απόδειξη.

Έστω $f(x) = a_0 + a_1 x + \ldots + a_n x^n$. Τότε

$$\sum_i \tau(a_i)\tau(a)^i = \tau(f(a)) = \tau(0) = 0$$

ωστόσο, έχουμε $a_i \in F$ και άρα $\tau(a_i) = a_i$. Επομένως, $0 = \sum_i a_i \tau(a)^i$, άρα $f(\tau(a)) = 0$. Συγκεκριμένα, αν $p(x) = Irr(a, F)$ τότε $p(\tau(a)) = 0$. Επομένως το $Irr(\tau(a), F)$ διαιρεί το $p(x)$. Καθώς το $p(x)$ είναι ανάγωγο, $Irr(\tau(a), F) = p(x) = Irr(a, F)$.

□

Πόρισμα 2. *Αν K/F επέκταση με $[K : F] < \infty$ τότε $|Gal(K/F)| < \infty$.*

Απόδειξη.

Γράφουμε το K ως $F(a_1, \ldots, a_n)$ για κάποιοα $a_i \in K$. Έχουμε δείξει ότι κάθε αυτομορφισμός του K που κρατάει σταθερό το F καθορίζεται πλήρως από την δράση του στα a_i. Από το προηγούμενο λήμμα υπάρχουν πεπερασμένες επιλογές για την εικόνα του κάθε a_i, δηλαδή οι ρίζες του $Irr(a_i, F)$. Άρα για πεπερασμένα a_i έχουμε πεπερασμένες επιλογές για τις εικόνες, συνεπώς πεπερασμένους F-αυτομορφισμούς του K. □

Ορισμός (Σταθερό σώμα)**.** *Έστω K/F και $S \subseteq Aut(K)$. Τότε το σύνολο:*

$$F^S = \{a \in K : \quad \tau(a) = a \quad \forall \tau \in S\}$$

λέγεται σταθερό σώμα του S και είναι πράγματι σώμα και μάλιστα υπόσωμα του K.

Λέμε ένα σώμα L τέτοιο ώστε $F \subseteq L \subseteq K$ ενδιάμεση επέκταση της K/F ή αλλιώς $K/L/F$. Αν $S \subseteq Gal(K/F)$ τότε F^S είναι ενδιάμεση επέκταση της K/F.

Λήμμα 3. *Έστω K ένα σώμα. Τότε:*

(1) *Αν $L_1 \subseteq L_2$ υποσώματα του K τότε $Gal(K/L_2) \subseteq Gal(K/L_1)$.*

(2) *Αν $L \subseteq K$ τότε $L \subseteq F^{Gal(K/L)}$.*

(3) *Αν $S_1 \subseteq S_2$ υποσύνολα του $Aut(K)$ τότε $F^{S_2} \subseteq F^{S_1}$.*

(4) *Αν $S \subseteq Aut(K)$ τότε $S \subseteq Gal(K/F^S)$.*

(5) *Αν $L = F^S$ για κάποιο $S \subseteq Aut(K)$ τότε $L = F^{Gal(K/F)}$.*

(6) *Αν $H = Gal(K/L)$ για κάποιο σώμα $L \subseteq K$ τότε $H = Gal(K/F^H)$.*

Απόδειξη.

(1) Έστω $\sigma \in Gal(K/L_2)$. Το σ κρατάει σταθερό το L_2 και άρα και το υπόσωμα L_1, άρα $\sigma \in Gal(K/L1)$.

(2) Έστω $x \in L$ και $\sigma \in Gal(K/L)$, τότε $\sigma(x) = x$ και άρα $x \in F^{Gal(K/L)}$.

(3) Έστω $x \in F^{S_2}$, τότε κάθε αυτομορφισμός που βρίσκεται στο S_2 κρατάει σταθερό το x, άρα και κάθε αυτομορφισμός που βρίσκεται στο S_1 κάνει το ίδιο. Δηλαδή, $x \in F^{S_1}$.

(4) Έστω $\sigma \in S$, το σ τότε κρατάει σταθερό το σταθερό σώμα F^S από τον ορισμό του σταθερό σώματος. Άρα $\sigma \in Gal(K/F^S)$.

(5) Έχουμε $S \subseteq Gal(K/L)$ από το 4) συνεπώς $F^{Gal(K/L)} \subseteq F^S = L$ από το 3). Από το 2) επίσης έχουμε ότι $L \subseteq F^{Gal(K/L)}$ από όπου έπεται το ζητούμενο.

(6) Όμοια, έχουμε $L \subseteq F^{Gal(K/L)}$ οπότε $Gal(K/F^{Gal(K/L)}) \subseteq Gal(K/L) = H$. Επιπλέον, $H \subseteq Gal(K/F^H)$ και άρα $H = Gal(K/F^H)$.

□

Πόρισμα 3. *Αν K/F τότε υπάρχει 1-1 αντιστοιχία που αλλάζει την φορά μεταξύ των υποομάδων της $Gal(K/F)$ της μορφής $Gal(K/L)$ για κάποιο υπόσωμα L του K που περιέχει το F και των υποσωμάτων του K που περιέχουν το F και είναι της μορφής F^S για κάποιο $S \subseteq Aut(K)$. Η αντιστοιχία δίνεται από την απεικόνιση $L \mapsto Gal(K/L)$ και την αντίστροφή της $H \mapsto F^H$*

Απόδειξη.

Αν θεωρήσουμε ως $\mathcal{G}, \mathcal{F}$ τα σύνολα των ομάδων και των σωμάτων αντίστοιχα από την εκφώνηση, τότε η απεικόνιση που στέλνει το $L \subseteq K$ στο $Gal(K/L)$ έχει πεδίο ορισμού το $\mathcal{F}$ και πεδίο τιμών το $\mathcal{G}$. Από το 5) του προηγούμενου λήμματος είναι 1-1 και επί. Από το 6) παίρνουμε ότι έχει αντίστροφη την $H \mapsto F^H$.

□

Ορισμός. *Έστω G μια ομάδα και K ένα σώμα, τότε ονομάζουμε χαρακτήρα κάθε ομομορφισμό ομάδων από το G στο K^*. Αν θεωρήσουμε και $G = K^*$, μπορούμε να βλέπουμε τους F-αυτομορφισμούς του K ως χαρακτήρες από το G στο K^*.*

Λήμμα 4 (Dedekind)**.** *Έστω $\tau_1, \ldots, \tau_n$ διακεκριμένοι χαρακτήρες από μια ομάδα G στην πολλαπλασιαστική ομάδα ενός σώματος K^*. Τότε τα τ_i είναι γραμμικά ανεξάρτητα υπεράνω του K. Δηλαδή, αν $\sum_i c_i\tau_i(g) = 0$ για κάθε $g \in G$ με $c_i \in K$ τότε $c_i = 0$ για όλα τα $i = 1, \ldots, n$.*

Απόδειξη.

Θα χρησιμοποιήσουμε επαγωγή στον αριθμό n των διακεκριμένων χαρακτήρων. Για $n = 1$ αν $c_1\tau_1(g) = 0$ τότε $c_1 = 0$ καθώς από τον ορισμό $\tau_1(g) \neq 0$ για κάθε $g \in G$. Υποθέτουμε ότι $n > 1$ και ότι έχουμε την σχέση:

$$c_1\tau_1(g) + \ldots + c_n\tau_n(g) = 0 \tag{1}$$

όπου δεν είναι όλα τα $c_i = 0$. Από αυτό μπορούμε να υποθέσουμε ότι κανένα από τα c_i δεν είναι 0 καθώς τότε θα ίσχυε η επαγωγική υπόθεση για τους υπόλοιπους $n - 1$ όρους. Υποθέτουμε επιπλέον ότι $c_n = 1$, αλλιώς πολλαπλάσιάζουμε ολόκληρη την σχέση με τον αντίστροφο. Έχουμε υποθέσει ότι οι χαρακτήρες είναι διακεκριμένοι, δηλαδή $\tau_n \neq \tau_1$. Άρα θεωρούμε ένα $y \in G$ τέτοιο ώστε $\tau_n(y) \neq \tau_1(y)$. Αντικαθιστούμε στην σχέση 1 το τυχόν $g \in G$ με $yg \in G$.

$$c_1\tau_1(y)\tau_1(g) + \ldots c_{n-1}\tau_{n-1}(y)\tau_{n-1}(x) + \tau_n(y)\tau_n(g)$$

στην συνέχεια πολλαπλασιάζουμε αυτήν την σχέση με $\tau_n(y)^{-1}$ και την αφαιρούμε από την 1. Η σχέση που μένει είναι:

$$c_1[1 - \tau_n(y)^{-1}\tau_1(y)]\tau_1(g) + \ldots + c_{n-1}[1 - \tau_n(y)^{-1}\tau_{n-1}(y)]\tau_{n-1}(g) = 0$$

και από την επαγωγική υπόθεση, καθένας από τους συντελεστές είναι ίσος με 0. Έχουμε $c_1 \neq 0$ και άρα $1 = \tau_n(y)^{-1}\tau_1(y)$, δηλαδή $\tau_1(y) = \tau_n(y)$ το οποίο είναι άτοπο.

□

Πρόταση 4. *Εστω K/F πεπερασμένη επέκταση. Τότε $|Gal(K/F)| \leq [K : F]$*

Απόδειξη.

Έχουμε δείξει ότι η ομάδα $Gal(K/F)$ είναι πεπερασμένη. Έστω $Gal(K/F) = \{\tau_1, \ldots \tau_n\}$ και υποθέτουμε προς άτοπο ότι $[K : F] < n$. Έστω $a_1, \ldots a_m$ μια βάση του K ως F-διανυσματικού χώρου με $m < n$. Ο πίνακας

$$A = \begin{pmatrix} \tau_1(a_1) & \tau_1(a_2) & \ldots & \tau_1(a_m) \\ \tau_2(a_1) & \tau_2(a_2) & \ldots & \tau_2(a_m) \\ \vdots & \vdots & \ddots & \vdots \\ \tau_n(a_1) & \tau_n(a_2) & \ldots & \tau_n(a_m) \end{pmatrix}$$

υπεράνω του K έχει $rank(A) \leq m < n$ και άρα οι γραμμές του είναι γραμμικά εξαρτημένες πάνω από το K. Έτσι, υπάρχουν c_i στο K όχι όλα 0, τέτοια ώστε $\sum_i c_i\tau_i(a_j) = 0$ για κάθε $j = 1, \ldots m$. Αν θεωρήσουμε $G = K*$, τότε για κάθε $g \in G$ υπάρχουν $b_i \in F$ με $g = \sum_j b_j a_j$. Επομένως:

$$\sum_i c_i\tau_i(g) = \sum_i c_i\tau_i\left(\sum_j b_j a_j\right) = \sum_i c_i\left(b_j \sum_j \tau_j(a_j)\right)$$

$$= \sum_j b_j\left(\sum_i c_i\tau_i(a_j)\right) = 0$$

και άρα κάθε c_i είναι 0 από το λήμμα του Dedekind, το οποίο είναι άτοπο. □

Πρόταση 5. *Έστω G πεπερασμένη ομάδα αυτομορφισμών του K με $F = F^G$. Τότε $|G| = [K : F]$ και $G = Gal(K/F)$.*

Απόδειξη.

Από την προηγούμενη πρόταση έχουμε $|G| \leq [K : F]$ καθώς $G \subseteq Gal(K/F)$. Ας υποθέσουμε ότι $|G| < [K : F]$. Έστω $n = |G|$ και $a_1, \dots a_{n+1}$ γραμμικά εξαρτημένα στοιχεία του K. Αν $G = \{\tau_1, \dots \tau_n\}$ θεωρούμε τον πίνακα

$$A = \begin{pmatrix} \tau_1(a_1) & \tau_1(a_2) & \dots & \tau_1(a_{n+1}) \\ \tau_2(a_1) & \tau_2(a_2) & \dots & \tau_2(a_{n+1}) \\ \vdots & \vdots & \ddots & \vdots \\ \tau_n(a_1) & \tau_n(a_2) & \dots & \tau_n(a_{n+1}) \end{pmatrix}$$

τότε οι στήλες του A είναι γραμμικά εξαρτημένες υπεράνω του K. Διαλέγουμε k ελάχιστο φυσικό τέτοιο ώστε οι πρώτες k στήλες είναι γραμμικά εξαρτημένες (με πιθανή αναδιάταξη των τ_i). Τότε υπάρχουν $c_i \in K$ όχι όλα μηδέν με $\sum_{i=1}^{k} c_i \tau_j(a_i) = 0$ για κάθε $j = 1, \dots, n$. Το ότι το k είναι ελάχιστο μας δίνει ότι όλα τα c_i είναι διάφορα του 0. Έτσι μπορούμε να υποθέσουμε ότι $c_1 = 1$, διαφορετικά πολλαπλασιάζουμε με τον αντίστροφο. Αν κάθε c_i περιέχεται στο F, τότε $0 = \tau_j \left(\sum_{i=1}^{k} c_i a_i \right)$ για κάθε j, οπότε $\sum_{i=1}^{k} c_i a_i = 0$.

Αυτό είναι άτοπο από την γραμμική ανεξαρτησία των a_i υπεράνω του F. Έστω ένα τυχόν $\sigma \in G$. Καθώς το σ μεταθέτει τα στοιχεία του G, παίρνουμε $\sum_{i=1}^{k} \sigma(c_i)\tau_j(a_i) = 0$ για κάθε j. Αφαιρώντας τα δύο αθροίσματα, μαζί με ότι $c_1 = 1$ παίρνουμε:

$$\sum_{i=2}^{k} (c_i - \sigma(c_i))\tau_j(a_i) = 0$$

για κάθε $j = 1, \dots n$. Επειδή το k είναι ελάχιστο, παίρνουμε $c_i - \sigma(c_i) = 0$ για κάθε i. Καθώς το σ ήταν τυχόν παίρνουμε $c_i \in F^G = F$ το οποίο δείξαμε ότι δεν μπορεί να συμβαίνει. Άρα $|G| \geq [K : F]$ από το άτοπο και λόγω της προηγούμενης πρότασης παίρνουμε $|G| = [K : F]$. Επιπλέον $G \subseteq Gal(K/F)$ και $|G| = [K : F] \geq |Gal(K/F)|$ άρα $G = Gal(K/F)$. □

Ορισμός (Επέκταση Galois)**.** *Έστω K/F αλγεβρική επέκταση. Τότε λέμε ότι η K/F είναι Galois αν $F = F^{Gal(K/F)}$.*

Πόρισμα 4. *Έστω K/F πεπερασμένη επέκταση. Τότε K/F είναι Galois αν και μόνο αν $|Gal(K/F)| = [K : F]$.*

Απόδειξη.

Αν η επέκταση K/F είναι Galois τότε $F = F^{Gal(K/F)}$ και από την προηγούμενη πρόταση $|Gal(K/F)| = [K : F]$. Αντίστροφα, αν $|Gal(K/F)| = [K : F]$, θέτουμε $L = F^{Gal(K/F)}$. Τότε πάλι από την προηγούμενη πρόταση $Gal(K/L) = Gal(K/F)$. Άρα $|Gal(K/F)| = [K : L] \leq [K : F]$. Από την υπόθεση παίρνουμε την ισότητα $[K : L] = [K : F]$, δηλαδή $L = F$.

□

Πόρισμα 5. *Έστω K/F και $a \in K$ αλγεβρικό υπεράνω του F. Τότε $|Gal(F(a)/F)|$ είναι ο αριθμός των διακεκριμένων ριζών του $Irr(a, F)$ στο $F(a)$. Συνεπώς, $F(a)/F$ είναι Galois αν και μόνο αν $Irr(a, F)$ έχει διακεκριμένες ρίζες όσες είναι ο βαθμός του.*

Απόδειξη.

Έστω $\tau \in Gal(F(a), F)$, γνωρίζουμε ότι το $\tau(a)$ είναι ρίζα του $Irr(a, F)$. Επιπλέον, αν $\sigma, \tau \in Gal(F(a)/F)$ με $\sigma \neq \tau$, τότε $\sigma(a) \neq \tau(a)$ καθώς αυτοί οι αυτομορφισμοί του $F(a)$ καθορίζονται πλήρως από την δράση τους στο a. Άρα $|Gal(F(a)/F) \leq deg\,(Irr(a, F))$.

Αντίστροφα, έστω b μια ρίζα του $Irr(a, F)$ στο $F(a)$. Ορίζουμε $\tau : F(a) \to F(a)$ με $\tau(f(a)) = f(b)$ για κάθε $f(x) \in F[x]$. Η απεικόνιση είναι καλά ορισμένη εφόσον έχουμε υποθέσει ότι το b είναι ρίζα του $Irr(a, F)$ και άρα πράγματι μεταθέτουμε ρίζες. Το τ είναι F-αυτομορφισμός και από τον ορισμό του $\tau(a) = b$. Έτσι η τάξη $|Gal(F(a)/F)|$ είναι ίση με τον αριθμο των διακεκριμένων ριζών του $Irr(a, F)$ στο $F(a)$. Καθώς $[F(a) : F] = deg(Irr(a, f))$, βλέπουμε ότι η επέκταση $F(a)/F$ είναι Galois αν και μόνο αν το $Irr(a, F)$ έχει απλές διακεκριμένες ρίζες όσες είναι ο βαθμός του. □

Παράδειγμα 1. *Η επέκταση $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ δεν είναι Galois. Το $Irr(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$ έχει 3 διακεκριμένες ρίζες και $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ αλλά μόνο μια ανήκει στο πραγματικό σώμα $\mathbb{Q}(\sqrt[3]{2})$, δηλαδή $|Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1$.*

Αν επισυνάψουμε και την $\omega = e^{2\pi i/3}$, έχουμε $x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega)(x - \sqrt[3]{2}\omega^2)$. Όλες οι ρίζες ανήκουν στο $\mathbb{Q}(\sqrt[3]{2}, \omega)$ και εφόσον $Irr(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$ και $Irr(\omega, \mathbb{Q}) = x^2 + x + 1$ έχουμε από κανόνα των πύργων ότι $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6$. Ταυτόχρονα έχουμε τους 6 ισομορφισμούς:

	$\sqrt[3]{2}$	ω
$\sigma_1 = id$	$\sqrt[3]{2}$	ω
σ_2	$\omega\sqrt[3]{2}$	ω
σ_3	$\sqrt[3]{2}$	ω^2
σ_4	$\omega\sqrt[3]{2}$	ω^2
σ_5	$\omega^2\sqrt[3]{2}$	ω
σ_6	$\omega^2\sqrt[3]{2}$	ω^2

επομένως $|Gal(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})| = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}]$ και άρα αυτή η επέκταση είναι Galois.

1.2 Κανονικές Επεκτάσεις

Υπενθυμίζουμε εδώ ότι, με βάση τον αλγόριθμο διαίρεσης, $a \in F$ είναι ρίζα του $f(x) \in F[x]$ αν και μόνο αν $x - a | f(x)$.

Λήμμα 5. *Έστω $f(x) \in F[x]$. Τότε το πολυώνυμο f έχει το πολύ $deg(f)$ ρίζες σε οποιαδήποτε επέκταση του F.*

Απόδειξη.

Θα κάνουμε επαγωγή στον βαθμό n του f. Για $n = 1$ τότε $f(x) = ax + b$ για κάποια $a, b \in F$. Η μόνη ρίζα είναι η $-ba^{-1}$ και ισύει το λήμμα. Υποθέτουμε ότι κάθε πολυώνυμο βαθμού $n-1$ έχει το πολύ $n-1$ ρίζες σε οποιαδήποτε επέκταση K/F. Αν το f δεν έχει ρίζες στο K δεν έχουμε να δείξουμε κάτι. Αν έχουμε $a \in K$ ρίζα του f τότε $f(x) = (x - a)g(x)$ και για το $g(x)$ ισχύει η επαγωγική υπόθεση. Άρα το f έχει το πολύ n ρίζες. □

Ορισμός. *Έστω K/F και $f(x) \in F[x]$. Λέμε ότι το f διασπάται πλήρως στο K αν υπάρχουν $a_1, \ldots a_n \in K$ και $a \in F$ τέτοια ώστε:*

$$f(x) = a(x - a_1) \cdots (x - a_n) \in K[x]$$

Ορισμός (Σώμα ριζών)**.** *Έστω K/F και $f(x) \in F[x]$. Λέμε ότι το K είναι σώμα ριζών του $f(x) \in F[x]$ αν το f διασπάται πλήρως στο K και $K = F(a_1, \ldots, a_n)$ όπου $a_1, \ldots, a_n$ είναι οι ρίζες του f. Μπορούμε να λέμε ότι το K είναι και σώμα ριζών ενός συνόλου πολυωνύμων αν καθένα από αυτά διασπάται πλήρως στο K και $K = F(X)$ όπου X οι ρίζες των πολυωνύμων.*

Αν $X = \{f_1, \ldots f_n\}$ ουσιαστικά μιλάμε για το σώμα ριζών του πολυωνύμου $f = f_1 \cdots f_n$.

Θεώρημα 3 (Ύπαρξη ρίζας σε επέκταση)**.** *Έστω $f(x) \in F[x]$ βαθμού $n > 1$. Τότε υπάρχει επέκταση K του F στην οποία το f έχει ρίζα και $[K : F] \leq n$.*

Απόδειξη.

Έστω $p(x)$ ένας ανάγωγος παράγοντας του $f(x)$ στο $F[x]$. Θέτουμε $K = F[x]/(p(x))$. Τότε η απεικόνιση $F \to K, a \mapsto a + (p(x))$ είναι μονομορφισμός σωμάτων και μπορούμε να ταυτίσουμε κάθε $a \in F$ με την εικόνα $a+(p(x))$. Έστω $b = x+(p(x)) \in K$. Τότε αν $f(x) = a_n x^n + \ldots + a_0$ έχουμε:

$$f(b) = a_n b^n + \ldots a_0 = a_n(x + (p(x)))^n + \ldots + a_1(x + (p(x))) + a_0$$
$$= a_n x^n + \ldots a_1 x + a_0 + (p(x)) = f(x) + (p(x)) = 0 + (p(x)) = 0_K$$

αφού το $p(x)$ διαιρεί το $f(x)$. Καθώς $[K : F] = deg(p(x))$ έχουμε $[K : F] < n$. □

Θεώρημα 4 (Ύπαρξη σώματος ριζών για πεπερασμένα πολυώνυμα)**.** *Έστω $f(x) \in F[x]$ βαθμού $n > 1$. Τότε υπάρχει επέκταση K του F με $[K : F] \leq n!$ και το f διασπάται πλήρως στο K.*

Απόδειξη.

Χρησιμοποιούμε επαγωγή στον βαθμό n. Από το θεώρημα ύπαρξης ρίζας έχουμε ότι υπάρχει επέκταση E/F με $[E : F] \leq n$ όπου το E περιέχει ρίζα a του $f(x)$. Δηλαδή $f(x) = (x-a)g(x)$ με $g(x) \in E[x]$. Από την επαγωγική υπόθεση υπάρχει σώμα ριζών $K \supseteq E$ του $g(x)$ με $[K : E] \leq (n-1)!$. Τότε το $f(x)$ διασπάται πλήρως στο K και από θεώρημα πύργων $[K : F] \leq n!$. □

Λήμμα 6. *Αν K είναι σώμα τότε τα επόμενα είναι ισοδύναμα:*

(1) *Δεν υπάρχουν αλγεβρικές επεκτάσεις του K εκτός από το ίδιο το K.*

(2) *Δεν υπάρχουν πεπερασμένες επεκτάσεις του K εκτός από το ίδιο το K.*

(3) *Αν L είναι επέκταση του K, τότε $K = \{a \in L : a$ αλγεβρικό υπεράνω του $K\}$.*

(4) *Κάθε $f(x) \in K[x]$ διασπάται πλήρως στο K.*

(5) *Κάθε $f(x) \in K[x]$ έχει ρίζα στο K.*

(6) *Κάθε ανάγωγο πολυώνυμο υπεράνω του K έχει βαθμό 1.*

Απόδειξη.

(1) $\implies$ (2) Άμεσο, καθώς κάθε πεπερασμένη επέκταση είναι αλγεβρική.
(2) $\implies$ (3) Έστω $a \in L$ αλγεβρικό υπεράνω του K. Τότε το $K(a)$ είναι πεπερασμένη επέκταση του K βαθμού $deg(Irr(a, K))$, άρα από υπόθεση $K(a) = K$.
(3) $\implies$ (4) Έστω $f(x) \in K[x]$ και L σώμα ριζών του f υπεράνω του K. Καθώς το L είναι αλγεβρική επέκταση του K, η υπόθεση μας δίνει ότι $L = K$. Δηλαδή, το f διασπάται πλήρως στο K.

(4) $\implies$ (5) Άμεσο.
(5) $\implies$ (6) Έστω $f(x) \in K[x]$ ανάγωγο. Από την υπόθεση, το f έχει ρίζα στο K και άρα καθώς είναι ανάγωγο με ρίζα είναι βαθμού 1.
(6) $\implies$ (1) Έστω L αλγεβρική επέκταση του K. Έστω $a \in L$ και $p(x) = Irr(a, F)$. Από υπόθεση $deg(p(x)) = 1$ δηλαδή $a \in K$ και άρα $L = K$.

□

Ορισμός. *Αν κάποιο K ικανοποιεί κάποια από τις συνθήκες του λήμματος 6 τότε λέμε ότι το K είναι αλγεβρικά κλειστό. Αν K/F είναι αλγεβρική επέκταση και το K είναι αλγεβρικά κλειστό, λέμε ότι το K είναι αλγεβρική κλειστότητα του F.*

Λήμμα 7. *Αν K/F αλγεβρική επέκταση, τότε $|K| \leq max\{|F|, |\mathbb{N}|\}$.*

Απόδειξη.

Έστω $a \in K$ και $a_1, \dots a_n$ οι ρίζες του $Irr(a, F)$ στο K. Έστω $\mathcal{M}$ το σύνολο όλων των μονικών πολυωνύμων υπεράνω του F. Ορίζουμε $f : K \to \mathcal{M} \times \mathbb{N}$ με $f(a) = (p(x), r)$ αν $p(x) = Irr(a, F)$ και $a = a_r$. Η απεικόνιση είναι 1-1 καθώς αν $a \in F$ τότε $f(a) = (x - a, 1)$, δηλαδή η πρώτη συντεταγμένη θα διαφέρει πάντα και αν $a \notin F$ τότε $f(a) = (Irr(a, F), r)$, δηλαδή αν μιλάμε για το ίδιο ελάχιστο πολυώνυμο, θα έχουμε διαφορετικό δείκτη της κάθε ρίζας. Επομένως:

$$|K| \leq |\mathcal{M} \times \mathbb{N}| = max\{|\mathcal{M}|, |\mathbb{N}|\}$$

Για να ολοκληρωθεί η απόδειξη θα δείξουμε ότι $|\mathcal{M}| \leq max\{|F|, |\mathbb{N}|\}$. Θεωρούμε $\mathcal{M}_n$ το σύνολο των μονικών πολυωνύμων βαθμού n. Τότε $|\mathcal{M}_n| = |F^n|$ καθώς η απεικόνιση $(a_0, \dots, a_{n-1}) \mapsto x^n + \sum_{i=0}^{n-1} a_i x^i$ είναι μια 1-1 και επί απεικόνιση μεταξύ των $\mathcal{M}_n, F^n$. Αν το F είναι πεπερασμένο έχουμε $|F^n| = |F|^n$, διαφορετικά $|F^n| = |F|$. Καθώς το $\mathcal{M}$ είναι ξένη ένωση των $\mathcal{M}_n$. Έχουμε

$$|\mathcal{M}| = |\cup_n \mathcal{M}_n| = max\{|F|, |\mathbb{N}|\}$$

εφόσον αν το F είναι πεπερασμένο θα είναι και το $|F|^n$ πεπερασμένο, αλλά ενώνουμε για όλα τα n συνεπώς θα έχουμε πληθικότητα $|\mathbb{N}|$. Διαφορετικά, παίρνουμε την πληθικότητα του $|F|$. □

Θεώρημα 5 (Ύπαρξη αλγεβρικής κλειστότητας)**.** *Έστω F ένα σώμα. Τότε υπάρχει αλγεβρική κλειστότητα του F*

Απόδειξη.

Έστω S ένα σύνολο που περιέχει το F με $|S| > max\{|F|, |\mathbb{N}|\}$. Εστω $\mathcal{A}$ το σύνολο των αλγεβρικών επεκτάσεων του F που περιέχονται στο S. Ορίζουμε διάταξη στο $\mathcal{A}$ με $K \leq L$ αν το L είναι επέκταση του K. Τότε από το λήμμα του Zorn, υπάρχει μεγιστικό στοιχείο M στο $\mathcal{A}$ ως προς την διάταξη αυτή. Θα δείξουμε ότι το M είναι αλγεβρικά κλειστό και ότι είναι η αλγεβρική κλειστότητα του F.

Έστω L μια αλγεβρική επέκταση του M. Από το προηγούμενο λήμμα έχουμε

$$|L| \leq max\{|M|, |\mathbb{N}|\} \leq max\{|F|, |\mathbb{N}|\} \leq |S|$$

άρα υπάρχει 1-1 απεικόνιση $f : L \to S$ με $f|_M = 1$. Αν ορίσουμε τις πράξεις $+, \cdot$ στο $f(L)$ με $f(a) + f(b) = f(a + b)$ και $f(a)f(b) = f(ab)$, τότε το $f(L)$ είναι επέκταση του M, αφού $f(M) = M$ και το f ομομορφισμός σωμάτων. Η μεγιστικότητα του M μας δίνει ότι $f(L) = M$. Άρα εφόσον η f είναι 1-1 έχουμε $L = M$. Συνεπώς M αλγεβρικά κλειστό σώμα. Καθώς το M είναι αλγεβρικό υπεράνω του F έχουμε ότι είναι και αλγεβρική κλειστότητα του F. □

Πόρισμα 6 (Υπαρξη σώματος ριζών)**.** *Έστω S ένα σύνολο μη σταθερών πολυωνύμων υπεράνω ενός σώματος F. Τότε υπάρχει σώμα ριζών του S υπεράνω του F.*

Απόδειξη.

Έστω K μια αλγεβρική κλειστότητα του F, Τότε κάθε $f(x) \in S$ διασπάται πλήρως στο K. Έστω $X \subseteq K$ το σύνολο των ριζών των πολυωνύμων του S. Τότε $F(X) \subseteq K$ είναι ένα σώμα ριζών του S υπεράνω του F καθώς κάθε $f \in S$ διασπάται πλήρως στο $F(X)$ μαζί με το ότι αυτό το σώμα είναι παραγόμενο από τις ρίζες των πολυωνύμων του S, όπως έχει οριστεί δηλαδή το σώμα ριζών. □

Λήμμα 8. *Έστω $\sigma : F \to F'$ ένας ισομορφισμός σωμάτων. Έστω $f(x) \in F[x]$ ανάγωγο και a μια ρίζα του σε κάποια επέκταση K/F. Επιπλέον, έστω a' μια ρίζα του $\sigma(f)$ σε μια επέκταση K'/F'. Τότε, υπάρχει ισομορφισμός $\tau : F(a) \to F'(a')$ με $\tau(a) = a'$ και $\tau|_F = \sigma$.*

Απόδειξη.

Καθώς το f είναι ανάγωγο και έχει ρίζα το a τότε το $Irr(a, F)$ θα είναι το f πολλαπλασιασμένο με μια σταθερά. Έτσι, τα $f, Irr(a, F)$ παράγουν το ίδιο κύριο ιδεώδες του $F[x]$. Ορίζουμε

$$\phi : F[x]/(f(x)) \longrightarrow F(a)$$

$$g(x) + (f(x)) \longmapsto g(a)$$

και επιπλέον

$$\psi : F'[x](f'(x)) \longmapsto F'(a')$$

$$g(x) + (f'(x)) \longmapsto g(a')$$

Οι ϕ, ψ είναι F, F'-αυτομορφισμοί των αντίστοιχων επεκτάσεων. Καθώς $\sigma(f) = f'$, η απεικόνιση

$$\nu : F[x]/(f(x)) \longrightarrow F'[x]/(f'(x))$$

$$g(x) + (f(x)) \longmapsto \sigma(g(x)) + (f'(x))$$

είναι ένας καλά ορισμένος ισομορφισμός που επεκτείνει τον σ. Επιπλέον έχουμε μια ακολουθία ισομορφισμών σωμάτων:

$$F(a) \xrightarrow{\phi^{-1}} F[x]/(f(x)) \xrightarrow{\nu} F'[x]/(f'(x)) \xrightarrow{\psi} F'(a')$$

δηλαδή η σύνθεση $\phi^{-1} \circ \nu \circ \psi : F(a) \to F'(a')$ είναι ένας ισομορφισμός που επεκτείνει τον σ με $a \mapsto a'$. □

Λήμμα 9. *Έστω $\sigma : F \to F'$ ένας ισομορφισμός σωμάτων και οι επεκτάσεις K/F και K'/F'. Υποθέτουμε ότι το K είναι σώμα ριζών μιας οικογένειας $\{f_i\}$ υπεράνω του F και ότι $\tau : K \to K'$ είναι ένας ομομορφισμός με $\tau|_F = \sigma$. Τότε το $\tau(K)$ είναι σώμα ριζών της οικογένειας $\{\sigma(f_i)\}$ υπεράνω του F'.*

Απόδειξη.

Εφόσον το K είναι σώμα ριζών της οικογένειας $\{f_i\}$ υπεράνω του F, για σταθερό i υπάρχουν a και οι ρίζες του $a_1, \ldots, a_n$ στο K έτσι ώστε

$$f_i(x) = a(x - a_1)(x - a_2) \cdots (x - a_n)$$

Επομένως, αν εφαρμόσουμε το τ έχουμε

$$\tau(f_i(x)) = \tau(a)(x - \tau(a_1)) \cdots (x - \tau(a_n))$$

Άρα κάθε $f_i' = \sigma(f_i) = \tau(f_i)$ διασπάται πλήρως στο $\tau(K)$. Επιπλέον, το K παράγεται από το F επισυνάπτοντας τις ρίζες των $\{f_i\}$ και άρα το $\tau(K)$ παράγεται από το F' επισυνάπτοντας τις εικόνες των ριζών των $\{f_i\}$ μέσω του τ. Δηλαδή, παράγεται από το F' επισυνάπτοντας τις ρίζες των $\{f_i'\}$. Άρα πράγματι το $\tau(K)$ είναι σώμα ριζών υπεράνω του F' του συνόλου $\{f_i'\}$. □

Θεώρημα 6. *Έστω $\sigma : F \to F'$ ενας ισομορφισμός σωμάτων και θεωρούμε τα πολυώνυμα $f(x) \in F[x], \sigma(f) \in F'[x]$. Έστω K το σώμα ριζών του f υπεράνω του F και K' το σώμα ριζών του $\sigma(f)$ υπεράνω του F'. Τότε υπάρχει ισομορφισμός $\tau : K \to K'$ με $\tau|_F = \sigma$. Επιπλέον, αν $a \in K$ και το $a' \in K'$ είναι ρίζα του $\sigma(Irr(a, F))$ στο K' τότε ο ισομορφισμός τ μπορεί να επιλεχθεί έτσι ώστε $\tau(a) = a'$.*

Απόδειξη.

Καθώς έχουμε σώματα ριζών ενός πολυωνύμου, οι επεκτάσεις θα είναι πεπερασμένες και έτσι μπορούμε να εφαρμόσουμε επαγωγή στο $n = [K : F]$. Αν $n = 1$ το αποτέλεσμα είναι άμεσο, εφόσον $F = K$ και $\tau = \sigma$. Για $n > 1$, υποθέτουμε ότι το αποτέλεσμα ισχύει για επεκτάσεις με δείκτη μικρότερο του n. Αν τώρα το f διασπάται πλήρως στο F πάλι $\tau = \sigma$. Αν δεν ισχύει αυτό, έστω $p(x)$ ένας ανάγωγος παράγοντας του f βαθμού μεγαλύτερου του 1. Έστω a μια ρίζα του $p(x)$ και a' ρίζα του $\sigma(p(x))$.

Έστω $L = F(a)$ και $L' = F(a)$. Τότε από επιλογή του $p(x)$ έχουμε $[L : F] > 1$ και άρα $[K : L] < n$. Από το λήμμα 8 υπάρχει ισομορφισμός $g : L \to L'$ με $g(a) = a'$. Καθώς το K είναι σώμα ριζών του $f(x)$ υπεράνω του L και το K' είναι σώμα ριζών του $\sigma(f)$ υπεράνω του L', από την επαγωγική υπόθεση επεκτείνουμε τον ισομορφισμό g σε έναν ισομορφισμό $\tau : K \to K'$.

Έχουμε $g|_F = \sigma$ όπως ορίζεται ο g από το λήμμα 8 και από την επαγωγική υπόθεση για την K/L ότι $\tau|_L = g$. Δηλαδή, $\tau|_F = \sigma$ και $\tau(a) = g(a) = a'$. □

Θεώρημα 7 (Θεώρημα Επέκτασης Ισομορφισμών)**.** *Έστω $\sigma : F \to F'$ ένας ισομορφισμός σωμάτων. Έστω $S = \{f_i(x)\}$ ένα σύνολο πολυωνύμων με συντελεστές από το F και $S' = \{\sigma(f_i)\}$. Έστω K ένα σώμα ριζών του S υπεράνω του F και K' ένα σώμα ριζών του S' υπεράνω του F'. Τότε υπάρχει ισομορφισμός $\tau : K \to K'$ με $\tau|_F = \sigma$. Επιπλέον, αν $a \in K$ και το a' είναι οποιαδήποτε ρίζα του $\sigma(Irr(a, F))$ στο K' τότε ο ισομορφισμός τ μπορεί να επιλεγεί έτσι ώστε $\tau(a) = a'$.*

Απόδειξη.

Για αυτή την απόδειξη θα χρησιμοποιήσουμε το λήμμα του Zorn. Έστω $\mathcal{A}$ το σύνολο των (L, ϕ) όπου L είναι οι ενδιάμεσες επεκτάσεις της K/F και $phi : L \to K'$ οι ομομορφισμοί που επεκτείνουν το σ. Το $\mathcal{A}$ είναι μη κενό καθώς $(F, \sigma) \in \mathcal{A}$.

Ορίζουμε την μερική διάταξη στο $\mathcal{A}$ με $(L, \phi) \leq (L', \phi')$ αν $L \subseteq L'$ και $\phi'|_L = \phi$. Υπενθυμίζουμε ότι μια αλυσίδα είναι ένα υποσύνολο στο οποίο ισχύει πλήρης διάταξη, δηλαδή κάθε στοιχείο μπορεί να συγκριθεί με οποιοδήποτε άλλο.

Έστω $\{(L_i, \phi_i)\}$ μια αλυσίδα στο $\mathcal{A}$. Αν $L = \cup_i L_i$ και $\phi : L \to K'$ με $\phi(a) = \phi_i(a)$ αν $a \in L_i$ τότε το L είναι σώμα που επεκτείνει τα L_i. Πράγματι, αν διαλέξουμε δύο στοιχεία του x, y για να επαληθεύσουμε τις ιδιότητες, τότε θα υπάρχουν i_1, i_2 με $x \in L_{i_1}$ και $y \in L_{i_2}$ και αν δίχως βλάβη γενικότητας $L_{i_1} \subseteq L_{i_2}$ οι πράξεις των x, y θα γίνονται αποκλειστικά στο σώμα L_{i_2}.

Επιπλέον, ο ϕ είναι ομομορφισμός που επεκτείνει τον σ αφού έχουμε $\phi_i|_F = \sigma$ για κάθε

i. Συνεπώς, το (L, ϕ) είναι ένα άνω φράγμα της αλυσίδας στο $\mathcal{A}$. Από το λήμμα του Zorn υπάρχει μεγιστικό στοιχείο $(M, \tau) \in \mathcal{A}$.

Θα δείξουμε ότι $M = K$ και $\tau(M) = K'$. Αν $M \neq K$ υπάρχει $f \in S$ το οποίο δεν διασπάται πλήρως στο M. Έστω $a \in K$ μια ρίζα του f που δεν ανήκει στο M και $p(x) = Irr(a, F)$. Θέτουμε $p' = \sigma(p) \in F'[x]$ και $a' \in K'$ μια ρίζα του p'. Μια τέτοια ρίζα υπάρχει καθώς το p' διαιρεί το f' το οποίο διασπάται πλήρως στο K'. Αν περιορίσουμε το πεδίο τιμών του τ στο $\tau(M)$, δηλαδή σαν ομομορφισμό τον θεωρήσουμε επί, θα έχουμε και ισομορφισμό. Πράγματι, αν $y \in ker\tau$ και $y \notin F$ τότε υπάρχει το $h(x) = Irr(y, F)$ και ο τ ως ομομορφισμός θα στέλνει μια ρίζα του $h(x)$ σε μια άλλη. Ωστόσο, $\tau(y) = 0$ άρα το 0 είναι ρίζα του αναγώγου $h(x)$, δηλαδή $h(x) = x$ και άρα $y = 0 \in F$ άτοπο. Άρα $ker\tau = \ker\sigma = 0$.

Τώρα χρησιμοποιούμε το λήμμα 8 για αυτόν τον ισομορφισμό και παίρνουμε $g : M(a) \to \tau(M)(a')$ ισομορφισμό που επεκτείνει τον τ. Τότε το $(M(a), g) \in \mathcal{A}$ είναι μεγαλύτερο του (M, τ), το οποίο είναι άτοπο. Άρα $M = K$ και το $\tau(K) = K'$ έπεται από το λήμμα 9 καθώς το $\tau(K) \subseteq K'$ είναι σώμα ριζών του S' υπεράνω του F'. □

Πόρισμα 7. *Έστω F ένα σώμα και $S \subseteq F[x]$. Τότε οποιαδήποτε δύο σώματα ριζών του S είναι ισόμορφα μέσω ενός F-ισομορφισμού. Ειδικότερα το ίδιο ισχύει για αλγεβρικές κλειστότητες.*

Απόδειξη.

Για το πρώτο επιχείρημα επεκτείνουμε με βάση το θεώρημα τον ισομορφισμό $id : F \to F$ μεταξύ των δύο σωμάτων ριζών του S. Από αυτό έπεται και το επόμενο επειχείρημα, εφόσον κάθε αλγεβρική κλειστότητα του F είναι το σώμα ριζών όλων των μη σταθερών πολυωνύμων του $F[x]$.

□

Πόρισμα 8. *Έστω F ένα σώμα και N μια αλγεβρική κλειστότητα του F. Αν K είναι αλγεβρική επέκταση του F τότε το K είναι ισόμορφο με ένα υπόσωμα του N.*

Απόδειξη.

Έστω M μια αλγεβρική κλειστότητα του K. Τότε η επέκταση M/F είναι και αυτή αλγεβρική από την αλγεβρικότητα των $K/F, M/K$. Άρα το M είναι και αυτό μια αλγεβρική κλειστότα του F και συνεπώς, από το προηγούμενο πόρισμα, ισόμορφο με το N. Αν $f : M \to N$ είναι ένας F-ισομορφισμός, τότε το $f(K)$ είναι υπόσωμα του N ισόμορφο με το K. □

Ορισμός (Κανονική Επέκταση)**.** *Έστω K/F. Τότε λέμε ότι η επέκταση K/F είναι κανονική αν το K είναι σώμα ριζών για κάποιο σύνολο πολυωνύμων υπεράνω του F.*

Πρόταση 6. *Έστω $K/L/F$ και K/F κανονική επέκταση. Τότε η επέκταση K/L είναι κανονική.*

Απόδειξη. Το K είναι σώμα ριζών ενός συνόλου πολυωνύμων $S \subseteq F[x]$. Δηλαδή, το K είναι το F με επισύναψη των ριζών των πολυωνύμων του S. Λόγω της επέκτασης $K/L/F$ το K θα είναι το L με επισύναψη τις ρίζες των πολυωνύμων του S (πιθανότατα κάποιες από αυτές θα ανήκουν ήδη στο L). Άρα το K είναι σώμα ριζών του S υπεράνω του L και συνεπώς κανονική επέκταση του L. □

Πρόταση 7. *Έστω K/F αλγεβρική επέκταση. Τότε τα ακόλουθα είνα ισοδύναμα:*

(1) *K/F κανονική επέκταση.*

(2) *Αν M είναι αλγεβρική κλειστότητα του K και αν $\tau : K \to M$ είναι ένας F-ισομορφισμός, τότε $\tau(K) = K$.*

(3) *Αν $N/K/L/F$ και $\sigma : L \to N$ είναι ένας F-ομομορφισμός, τότε $\sigma(L) \subseteq K$ και υπάρχει $\tau \in Gal(K/F)$ με $\tau|_L = \sigma$.*

(4) *Για κάθε ανάγωγο $f(x) \in F[x]$, αν f έχει ρίζα στο K τότε διασπάται πλήρως στο K.*

Απόδειξη.

(1) $\implies$ (2) Έστω M μια αλγεβρική επέκταση του K και $\tau : K \to M$ ενας F-ομομορφισμός. Έστω S το σύνολο των πολυωνύμων για το οποίο το K είναι σώμα ριζών υπεράνω του F ως κανονική επέκταση. Τότε, όμοια με την απόδειξη του θεωρήματος ισομορφισμών, αν περιορίσουμε το πεδίο τιμών του τ στο $\tau(K)$ έχουμε ισομορφισμό που επεκτείνει τον $id : F \to F$ και μπορούμε να χρησιμοποιήσουμε το λήμμα 8 ώστε να πάρουμε ότι και το $\tau(K)$ είναι σώμα ριζών του S υπεράνω του F. Άρα καθώς τα $K, \tau(K)$ περιέχουν το F και παράγονται από τις ίδιες ρίζες πολυωνύμων έχουμε $\tau(K) = K$.

(2) $\implies$ (3) Έστω $F \subseteq L \subseteq K \subseteq N$ σώματα και $\sigma : L \to N$ ένας F-ισομορφισμός. Καθώς $L \subseteq K$, η επέκταση L/F είναι αλγεβρική και άρα είναι και η $\sigma(L)/F$. Έστω M' η αλγεβρική κλειστότητα του F που περιέχεται στο N και M μια αλγεβρική κλειστότητα του M'. Τότε και το M είναι αλγεβρική κλειστότητα του K. Από το θεώρημα επέκτασης ισομορφισμών, υπάρχει $g : M \to M$ ισομορφισμός που επεκτείνει το σ. Έστω $\tau = g|_K$, από την υπόθεση έχουμε $\tau(K) = K$ και άρα $\sigma(L) = \tau(L) \subseteq \tau(K) = K$. Άρα $\tau \in Gal(K/F)$.

(3) $\implies$ (4) Έστω $f(x) \in F[x]$ ανάγωγο και $a \in K$ μια ρίζα του f. Θέτουμε $L = F(a) \subseteq K$ και N μια αλγεβρική κλειστότητα του K. Αν $b \in N$ είναι ρίζα του f, τότε υπάρχει F-ομομορφισμός $\sigma : L \to N$ που ορίζεται ως $\sigma|_F = id$ και $\sigma(a) = b$. Από την υπόθεση $\sigma(L) \subseteq K$ και άρα $b \in K$. Άρα αν μια ρίζα περιέχεται στο K τότε περιέχονται και οι υπόλοιπες, δηλαδή το f διασπάται πλήρως στο K.

(4) $\implies$ (1) Έστω $a \in K$, τότε από την υπόθεση το ανάγωγο $Irr(a, F)$ διασπάται πλήρως στο K. Δηλαδή, το K είναι σώμα ριζών των πολυωνύμων $\{Irr(a, F) : a \in K\}$ υπεράνω του F και άρα η επέκταση K/F είναι κανονική.

□

1.3 Διαχωρίσιμες Επεκτάσεις

Ορισμός (Διαχωρίσιμο πολυώνυμο)**.** *Έστω F ένα σώμα. Ένα ανάγωγο πολυώνυμο $f(x) \in F[x]$ είναι διαχωρίσιμο υπεράνω του F αν οι ρίζες του είναι απλές σε οποιοδήποτε σώμα ριζών. Ένα πολυώνυμο $g(x) \in F[x]$ είναι διαχωρίσιμο υπεράνω του F αν όλοι οι ανάγωγοι παράγοντες του είναι διαχωρίσιμοι υπεράνω του F.*

Παράδειγμα 2. *Τα πολυώνυμα $x^2 - 2$ και $(x-1)^5$ είναι διαχωρίσιμα υπεράνω του $\mathbb{Q}$. Για να βρούμε μη διαχωρίσιμο πολυώνυμο πρέπει να κοιτάξουμε σε σώματα θετικής χαρακτηριστικής λόγω αποτελέσματος που θα ακολουθήσει. Έστω σώμα F χαρακτηριστικής p και ένα στοιχείο $a \in F \setminus F^p$. Έστω y ρίζα του $x^p - a$ σε κάποια επέκταση L/F. Έχουμε ότι η χαρακτηριστικη του L θα είναι p και επομένως $(x-y)^p = x^p - y^p = x^p - a$ αφού $a = y^p$ στο $L[x]$. Από αυτή τη σχέση, αν το $x^p - a$ δεν είναι ανάγωγο στο F τότε κάποιος παράγοντας $(x-y)^r, 1 \leq r < p$ θα ανήκει στο $F[x]$. Έστω λοιπόν:*

$$x^p - a = g(x)h(x) \quad g(x), h(x) \in F[x] \text{ μη σταθερά}$$

αν δούμε την εξίσωση στο μεγάλο σώμα L έχουμε:

$$(x-y)^p = g(x)h(x)$$

δηλαδή, εφόσον έχουμε ότι το L είναι σώμα και άρα το $L[x]$ περιοχή μοναδικής παραγοντοποίησης, $g(x) = (x-y)^r$ και $h(x) = (x-y)^{p-r}$ για κάποιο $1 \leq r < p$. Καθώς $g(x) \in F[x]$ τότε ο συντελεστής $-ry$ του x^{r-1} ανήκει στο F. Ωστόσο, το $r \neq 0_F$ από την επιλογή του άρα $y \in F$. Αυτό είναι άτοπο καθώς $a = y^p \notin F^p$. Άρα το $x^p - a$ είναι ανάγωγο στο $F[x]$. Όπως είδαμε παραπάνω, αν έχει ρίζα y σε επέκταση το $x^p - a$ θα γράφεται ως $(x-y)^p$ και άρα δεν είναι διαχωρίσιμο υπεράνω του F.

Λήμμα 10. *Έστω $f(x)$ και $g(x)$ πολυώνυμα υπεράνω ενός σώματος F. Τότε:*

(1) *Αν το f έχει μόνο απλές ρίζες σε οποιοδήποτε σώμα ριζών, τότε είναι διαχωρίσιμο.*

(2) *Αν $g(x)|f(x)$ και το f είναι διαχωρίσιμο υπεράνω του F, τότε και το g είναι διαχωρίσιμο υπεράνω του F.*

(3) *Αν $f_1, \dots f_n$ είναι διαχωρίσιμα πολυώνυμα υπεράνω του F τότε το γινόμενο τους είναι διαχωρίσιμο υπεράνω του F*

(4) *Αν το f είναι διαχωρίσιμο υπεράνω του F, τότε το F είναι διαχωρίσιμο υπεράνω οποιασδήποτε επέκτασης του F.*

Απόδειξη.

(1) Αν το f έχει μόνο απλές ρίζες σε οποιοδήποτε σώμα ριζών τότε το ίδιο θα ισχύει και για τους ανάγωγους παράγοντές του. Άρα το f είναι διαχωρίσιμο.

(2) Εφόσον το f είναι διαχωρίσιμο, οι ανάγωγοι παράγοντές του θα έχουν απλές ρίζες σε οποιοδήποτε σώμα ριζών και άρα το ίδιο θα ισχύει και για τους ανάγωγους παράγοντες του g.

(3) Ο κάθε ανάγωγος παράγοντας του $f_1 \cdots f_n$ θα είναι ανάγωγος παράγοντας κάποιου από τα f_i και άρα θα είναι διαχωρίσιμος, συνεπώς το $f_1 \cdots f_n$ είναι διαχωρίσιμο.

(4) Έστω K μια επέκταση του F. Θεωρούμε $p(x)$ έναν ανάγωγο παράγοντα του f στο $K[x]$ που έχει ρίζα a σε κάποια αλγεβρική κλειστότητα του K. Θέτουμε $q(x) = Irr(a, F)$. Τότε $q(x) \in F[x] \subseteq K[x]$ και άρα $p(x)|q(x)$ στο $K[x]$. Ωστόσο, το $q(x)$ είναι ανάγωγος παράγοντας του f στο $F[x]$ και άρα δεν έχει πολλαπλές ρίζες. Επομένως, ούτε το p έχει πολλαπλές ρίζες και άρα το f είναι διαχωρίσιμο υπεράνω του K.

□

Πρόταση 8. *Έστω $f(x) \in F[x]$ μη σταθερό πολυώνυμο. Τότε το f έχει μόνο απλές ρίζες σε ένα σώμα ριζών αν και μόνο αν $(f, f') = 1$ στο $F[x]$, όπου f' είναι η τυπική παράγωγος του πολυωνύμου f.*

Απόδειξη.

Έστω K ενα σώμα ριζών του f υπεράνω του F. Τα f, f' είναι σχετικά πρώτα στο $F[x]$ αν και μόνο αν είναι σχετικά πρώτα στο $K[x]$. Πράγματι, αν μκδ$(f, f') = 1$ στο $F[x]$ τότε υπάρχουν πολυώνυμα $g, h \in F[x]$ τέτοια ώστε

$$fg + hf' = 1$$

αυτή η εξίσωση όμως ισχύει και στο $K[x]$ άρα μκδ$(f, f') = 1$ στο $K[x]$. Αντίστροφα, αν μκδ$(f, f') = 1$ στο $K[x]$ και d ο μέγιστος κοινός διαιρέτης των f, f' στο $F[x]$, τότε $d \in K[x]$ και άρα $d|1$. Αρα τα f, f' είναι σχετικά πρώτα στο $F[x]$.

Υποθέτουμε ότι τα f, f' είναι σχετικά πρώτα στο $F[x]$ και θεωρούμε K το σώμα ριζών των f, f' υπεράνω του F. Αν υπάρχει κοινή ρίζα $a \in K$ τότε το $x - a$ θα διαιρεί τον μέγιστο κοινό διαιρέτη στο K, αλλά όπως έχουμε υποθέσει αυτός προκύπτει να είναι 1. Άρα δεν υπάρχει κοινή ρίζα μεταξύ των f, f', δηλαδη το f έχει μόνο απλές ρίζες.

Αντίστροφα, αν f, f' δεν έχουν κοινές ρίζες σε ένα σώμα ριζών, θεωρούμε το σώμα ριζών K του συνόλου $\{f, f'\}$ υπεράνω του F. Αν d ο μέγιστος κοινός διαιρέτης των $f(x), f'(x)$ στο $K[x]$, τότε το d διασπάται πλήρως στο K καθώς το f διασπάται πλήρως και $d|f$. Επιπλέον, κάθε ρίζα του d είναι κοινή ρίζα εφόσον $d|f'$. Άρα το d δεν έχει ρίζες και επειδή είναι μονικό ως μέγιστος κοινός διαιρέτης έχουμε $d = 1$. Άρα τα f, f' είναι σχετικά πρώτα στο $K[x]$, δηλαδή και στο $F[x]$. □

Πρόταση 9. *Έστω $f(x) \in F[x]$ ανάγωγο. Τότε:*

(1) *Αν η χαρακτηριστική του F είναι 0, τότε το f είναι διαχωρίσιμο υπεράνω του F. Αν η χαρακτηριστική είναι $p > 0$ τότε το f είναι διαχωρίσιμο αν και μόνο αν $f' \neq 0$ και αυτό συμβαίνει μόνο όταν $f(x) \notin F[x^p]$.*

(2) *Αν η χαρακτηριστική του F ειναι $p > 0$, τότε $f(x) = g(x^{p^m})$ για κάποιον ακέραιο $m \geq 0$ και κάποιο $g(x) \in F[x]$ το οποίο είναι ανάγωγο και διαχωρίσιμο υπεράνω του F.*

Απόδειξη.

(1) Εφόσον το f είναι ανάγωγο, έχουμε μκδ$(f, f') = 1$ ή f. Αν η χαρακτηριστική του F είναι 0 έχουμε $deg(f') = deg(f) - 1$ συνεπώς το f δεν διαιρεί το f' και άρα παίρνουμε το 1 για μέγιστο κοινό διαιρέτη. Από την προηγούμενη πρόταση παίρνουμε ότι το f δεν έχει πολλαπλές ρίζες και άρα είναι διαχωρίσιμο.

Αν η χαρακτηριστική του F είναι $p > 0$, όμοια έχουμε μκδ$(f, f') = f$ αν και μόνο αν το f διαιρεί το f' αν και μόνο αν $f' = 0$. Δηλαδή, θα πρέπει $f(x) \in F[x^p]$.

(2) Θεωρούμε μέγιστο m τέτοιο ώστε $f(x) \in F[x^{p^m}]$. Τέτοιο m υπάρχει καθώς $f(x) \in F[x^{p^0}] = F[x]$ και ισχύει ότι $f(x) \in F[x^{p^r}]$ για πεπερασμένα r γιατί κάθε μη σταθερό πολυώνυμο στο $F[x^{p^r}]$ έχει βαθμό τουλάχιστον p^r.

Έστω $f(x) = g(x^{p^m})$. Τότε, $g(x) \not\in F[x^p]$. Πράγματι, αν $g(x) \in F[x^p]$ τότε $f(x) \in F[x^{p^{m+1}}]$ το οποίο αντικρούει το ότι το m είναι μέγιστο. Επιπλέον, το $g(x)$ είναι ανάγωγο στο F. Αν δεν ήταν και είχαμε μια παραγοντοποίηση $g(x) = h(x)k(x)$, τότε

$$f(x) = h(x^{p^m})k(x^{p^m})$$

δηλαδή το f δεν θα ήταν ανάγωγο στο $F[x]$. Από το (1) της πρότασης, το $g(x)$ είναι διαχωρίσιμο υπεράνω του F.

□

Τώρα θα επεκτείνουμε την ιδέα της διαχωρισιμότητας στα στοιχεία ενός σώματος και γενικότερα στις επεκτάσεις.

Ορισμός (Διαχωρίσιμο Στοιχείο και Επέκταση)**.** *Έστω K/F επέκταση και $a \in K$. Τότε το a είναι διαχωρίσιμο υπεράνω του F αν το $Irr(a, F)$ είναι διαχωρίσιμο υπεράνω του F. Αν αυτό ισχύει για κάθε $a \in K$ λέμε την επέκταση K/F διαχωρίσιμη.*

Με βάση τα παραπάνω, Θα δώσουμε στην συνέχεια έναν χρήσιμο χαρακτηρισμό για τις επεκτάσεις Galois.

Θεώρημα 8. *Έστω K/F αλγεβρική επέκταση. Τότε τα ακόλουθα είναι ισοδύναμα:*

(1) *η επέκταση K/F είναι Galois.*

(2) *η επέκταση K/F είναι κανονική και διαχωρίσιμη.*

(3) *το K είναι σώμα ριζών ενός συνόλου διαχωρίσιμων πολυωνύμων υπεράνω του F.*

Απόδειξη.

(1) $\implies$ (2) Έστω K/F Galois και $a \in K$. Καθώς το a είναι αλγεβρικό υπεράνω του F, θεωρούμε $a_1, \dots a_n$ τα διακεκριμένα στοιχεία του συνόλου $A = \{\sigma(a) : \sigma \in Gal(K/F)\}$. Αυτό το σύνολο είναι πεπερασμένο, καθώς κάθε F-αυτομορφισμός του K πάει το a σε μια άλλη ρίζα του $Irr(a, F)$. Επιπλέον, κάθε $\tau \in Gal(K/F)$ μεταθέτει τα a_i μεταξύ τους. Πράγματι, αν $\tau(a_i) = b \notin A$ το a_i θα γράφεται ως $\sigma(a)$ για κάποιο $\sigma \in Gal(K/F)$ και έτσι $(\tau\sigma)(a) = b \notin A$, το οποίο είναι άτοπο από τον ορισμό του A. Θέτουμε:

$$f(x) = \prod_{i=1}^{n}(x - a_i) \in K[x]$$

και για κάθε $\tau \in Gal(K/F)$ έχουμε

$$\tau(f)(x) = \prod_{i=1}^{n}(x - \tau(a_i)) = \prod_{i=1}^{n}(x - a_i) = f(x)$$

Άρα οι συντελεστές του f παραμένουν σταθεροί υπό την δράση του τυχόν $\tau \in Gal(K/F)$. Έχουμε υποθέσει ότι K/F Galois, δηλαδή $F^{Gal(K/F)} = F$ και άρα $f(x) \in F[x]$.

Αφού το $f(x)$ έχει ρίζα το a, παίρνουμε ότι $Irr(a, F)|f(x)$ και άρα το $Irr(a, F)$ διασπάται πλήρως στο K και δεν έχει πολλαπλές ρίζες. Αυτό ισχύει για το τυχόν $a \in K$. Δηλαδή, το K είναι σώμα ριζών του συνόλου $\{Irr(a, F) : a \in K\}$ υπεράνω του F, το οποίο αποτελείται από διαχωρίσιμα πολυώνυμα. Άρα K/F κανονική και διαχωρίσιμη.

(2) $\implies$ (3) Έστω K/F κανονική και διαχωρίσιμη. Από το (4) της πρότασης 7 το K είναι σώμα ριζών των διαχωρίσιμων πολυωνύμων $\{Irr(a, F) : a \in K\}$ υπεράνω του F.

(3) $\implies$ (1) Έστω K ένα σώμα ριζών ενός συνόλου $\{f_i(x)\}$ διαχωρίσιμων πολυωνύμων υπεράνω του F. Αποδεικνύουμε αρχικά την περίπτωση για πεπερασμένες επεκτάσεις με επαγωγή στον βαθμό $[K : F] = n$. Για $n = 1$ έχουμε την τετριμμένη επέκταση Galois $K = F$. Έστω $n > 1$ και υποθέτουμε ότι ισχύει το αποτέλεσμα για τους φυσικούς μικρότερους του n.

Εφόσον $n > 1$ υπάρχει a ρίζα κάποιου f_i που δεν περιέχεται στο F. Θέτουμε $L = F(a)$ και έχουμε $[L : F] > 1$, δηλαδή $[K : L] < n$. Καθώς το K είναι σώμα ριζών των $\{f_i(x)\}$ υπεράνω του F, είναι και σώμα ριζών των ίδιων πολυωνύμων υπεράνω του L. Έχουμε δείξει επίσης ότι η διαχωρισιμότητα ενός πολυωνύμου μεταφέρεται στην επέκταση, άρα από την επαγωγική υπόθεση έχουμε ότι η επέκταση K/L είναι Galois.

Θέτουμε $H = Gal(K/L) \leq Gal(K/F)$ και θεωρούμε $a_1, \dots a_r \in K$ τις διακεκριμένες ρίζες του $Irr(a, F)$. Αυτές περιέχονται όλες στο K αφού το K είναι κανονική επέκταση και περιέχει την μια ρίζα a. Επίσης, το a είναι διαχωρίσιμο και άρα έχουμε $deg(Irr(a, F)) = r$ από όπου παίρνουμε $[L : F] = r$.

Από θεώρημα επέκτασης ισομορφισμών υπάρχουν $\tau_i \in Gal(K/F)$ έτσι ώστε $\tau_i(a) = a_i$. Έχουμε ότι τα σύμπλοκα $\tau_i H$ είναι ξένα μεταξύ τους. Αν αυτό δεν ίσχυε θα είχαμε

$$\tau_i H = \tau_j H \iff \tau_i^{-1}\tau_j H = H \iff \tau_i^{-1}\tau_j \in H = Gal(K/L)$$

δηλαδή $(\tau_i^{-1}\tau_j)(a) = a$ αφού κρατάμε σταθερό το L και παίρνουμε

$$\tau_i(a) = \tau_j(a) \implies a_i = a_j$$

το οποίο είναι άτοπο αφού οι ρίζες a_i, a_j είναι διακεκριμένες. Έτσι παίρνουμε ότι $[G : H] \geq r$.

Γράφουμε $G = Gal(K/F)$. Επιπλέον έχουμε ότι η K/L είναι Galois, δηλαδή $|H| = [K : L]$. Άρα παίρνουμε

$$|G| = [G : H]|H| \geq r|H| = [L : F][K : L] = [K : F]$$

και επειδή έχουμε δείξει ότι ισχύει γενικά $|G| \leq [K : F]$, καταλήγουμε στο $|G| = [K : F]$. Άρα K/F Galois.

Τώρα θα το αποδείξουμε για αυθαίρετη επέκταση K/F ως προς τον βαθμό. Έστω ότι το K είναι σώμα ριζών ενός συνόλου διαχωρίσιμων πολυωνύμων S υπεράνω του F και X το σύνολο των ριζών των πολυωνύμων του S. Δηλαδή, έχουμε $K = F(X)$. Έστω $a \in F^{Gal(K/F)}$. Για να δείξουμε ότι η επέκταση είναι Galois αρκεί να δείξουμε ότι $a \in F$.

Καθώς το K παράγεται από το X, έχουμε ότι υπάρχει ένα πεπερασμένο σύνολο

$$\{a_1, \ldots, a_n\} \subseteq X : \quad a \in F(a_1, \ldots a_n)$$

Θέτουμε L το σώμα ριζών του $\{Irr(a_i, F) : 1 \leq i \leq n\}$ υπεράνω του F. Τότε η επέκταση L/F είναι πεπερασμένη, κανονική και διαχωρίσιμη, άρα Galois όπως δείξαμε για την πεπερασμένη περίπτωση. Επιπλέον, $a \in F(a_1, a_2, \ldots, a_n) \subseteq L$.

Χρησιμοποιούμε το θεώρημα επέκτασης ισομορφισμών για τα στοιχεία του $Gal(L/F)$ και τα επεκτείνουμε σε F-αυτομορφισμούς του K. Έτσι, από το (3) της πρότασης 7 έχουμε

$$Gal(L/F) = \{\sigma|_L : \sigma \in Gal(K/F)\}$$

τώρα χρησιμοοποιούμε την υπόθεση $a \in F^{Gal(K/F)}$ και θεωρούμε ένα $\sigma|_L \in Gal(L/F)$, δηλαδή ένα $\sigma \in Gal(K/F)$. Τότε

$$\sigma|_L(a) = \sigma(a) = a$$

και άρα $a \in F^{Gal(L/F)}$. Όμως, η επέκταση L/F είναι Galois και άρα $a \in F$. □

Πόρισμα 9. *Έστω L/F πεπερασμένη επέκταση. Τότε:*

(1) *το L είναι διαχωρίσιμο υπεράνω του F αν και μόνο αν περιέχεται σε μια Galois επέκταση του F.*

(2) *Αν $L = F(a_1, \ldots, a_n)$ με τα a_i να είναι διαχωρίσιμα υπεράνω του F τότε το L είναι διαχωρίσιμο υπεράνω του F.*

Απόδειξη.

(1) Έστω $L \subseteq K$ με K/F Galois. Τότε K/F διαχωρίσιμη από το προηγούμενο θεώρημα και άρα L/F διαχωρίσιμη. Αντίστροφα, έστω L/F διαχωρίσιμη. Έχουμε $[L : F] < \infty$ και άρα μπορούμε να γράψουμε $L = F(a_1, \ldots a_n)$ με a_i διαχωρίσιμα υπεράνω του F. Έστω K το σώμα ριζών του συνόλου $\{Irr(a_i, F) : 1 \leq i \leq n\}$. Τότε $L \subseteq K$ και K/F Galois από το προηγούμενο θεώρημα.

(2) Έστω $L = F(a_1, \ldots a_n)$ με a_i διαχωρίσιμα υπεράνω του F. Τότε τα $Irr(a_i, F)$ είναι διαχωρίσμα υπεράνω του F και θεωρούμε ως K το σώμα ριζών τους. Τότε η επέκταση K/F είναι Galois αφού ικανοποιεί το (3) του προηγούμενου θεωρήματος. Δηλαδή, K/F διαχωρίσιμη επέκταση και $L \subseteq K$. Άρα και η L/F είναι διαχωρίσιμη.

□

Πρόταση 10. *Έστω K/F διαχωρίσιμη και $K/E/F$ ενδιάμεση επέκταση. Τότε η επέκταση K/E είναι και αυτή διαχωρίσιμη.*

Απόδειξη. Έστω $a \in K$. Έχουμε ότι το $Irr(a, F)$ έχει ρίζα το a και συνεπώς έχουμε:

$$Irr(a, E)|Irr(a, F) \quad \text{στο } E[x]$$

επίσης, το $Irr(a, F)$ είναι διαχωρίσιμο υπεράνω του F λόγω ότι ολόκληρη η επέκταση K/F είναι διαχωρίσιμη. Από το λήμμα 10, το τέταρτο επιχείρημα μας δίνει ότι το $Irr(a, F)$ είναι διαχωρίσιμο υπεράνω του E. Μαζί με αυτό, το δεύτερο επιχείρημα του λήμματος μας δίνει ότι το $Irr(a, E)$ είναι διαχωρίσιμο υπεράνω του E. □

1.4 Θεμελιώδες Θεώρημα της Θεωρίας Galois

Είμαστε τώρα σε θέση να αποδείξουμε το θεμελιώδες θεώρημα της θεωρίας Galois που περιγράφει την σχέση μεταξύ των ενδιάμεσων επεκτάσεων μιας επέκτασης Galois K/F με τις υποομάδες της $Gal(K/F)$.

Θεώρημα 9 (Θεμελιώδες Θεώρημα της Θεωρίας Galois)**.** *Έστω K μια πεπερασμένη επέκταση Galois ενός σώματος F και $G = Gal(K/F)$. Τότε υπάρχει μια 1-1 αντιστοιχία που αντιστρέφει την φορά μεταξύ των ενδιάμεσων επεκτάσεων της K/F και των υποομάδων της G. Αυτή η αντιστοιχία δίνεται από τις απεικονίσεις $L \mapsto Gal(K/L)$ και $H \mapsto F^H$. Επιπλέον, αν $L \leftrightarrow H$ τότε $[K : L] = |H|$ και $[L : F] = [G : H]$. Μαζί με αυτό, η H είναι κανονική υποομάδα της G αν και μόνο αν η επέκταση L/F είναι Galois. Όταν αυτό συμβαίνει έχουμε $Gal(L/F) \cong G/H$.*

Έχουμε δηλαδή τις αντοιστιχίες:

$$\begin{array}{ccc} K & & 1 \\ | & & | \\ E & \xrightarrow{E \longmapsto Gal(K,E)} & Gal(K,E) \\ | & & | \\ F & & G \end{array} \qquad \begin{array}{ccc} 1 & & K \\ | & & | \\ H & \xrightarrow{F \longmapsto F^H} & F^H \\ | & & | \\ G & & F \end{array}$$

όπου μεταξύ των πύργων που συνδέονται με μια από τις απεικονίσεις, οι βαθμοί που βρίσκονται στο ίδιο ύψος ταυτίζονται.

Απόδειξη.

Έχουμε δείξει το πρώτο μέρος της απόδειξης με το λήμμα 3. Έστω L ένα υπόσωμα του K που περιέχει το F. Καθώς το K είναι Galois υπεράνω του F έχουμε ότι είναι κανονική και διαχωρίσιμη επέκταση του F. Από τις προτάσεις $6, 10$ έχουμε ότι το K είναι διαχωρίσιμη και κανονική επέκταση υπεράνω του L. Δηλαδή η επέκταση K/L είναι Galois. Άρα, $L = F^{Gal(K/L)}$ και συνεπώς κάθε ενδιάμεσο σώμα είναι ένα σταθερό σώμα υποομάδας. Επιπλέον, αν $H \leq G$, τότε η H είναι πεπερασμένη και $H = Gal(K/F^H)$, από την πρόταση 5. Κάθε υποομάδα της G είναι λοιπόν μια ομάδα Galois και οι απεικονίσεις της εκφώνησης δίνουν την ζητούμενη αντιστοιχία. Για την Galois επέκταση K/F έχουμε $|Gal(K/F)| = [K : F]$. Αν λοιπόν $L \leftrightarrow H$ τότε $|H| = [K : L]$, καθώς το K είναι Galois επέκταση του L και $H = Gal(K/L)$. Συνεπώς:

$$[G : H] = |G|/|H| = [K : F]/[K : L] = [L : F]$$

Έστω $H \trianglelefteq G$ και $L = F^H$. Έστω $a \in L$ και b μια ρίζα του $Irr(a, F)$ που ανήκει στο K. Από το θεώρημα επέκτασης ισομορφισμών, υπάρχει $\sigma \in G$ με $\sigma(a) = b$. Αν $\tau \in H$, τότε $\tau(b) = \sigma(\sigma^{-1}\tau\sigma(a))$. Ωστόσο, έχουμε ότι $\sigma^{-1}\tau\sigma \in H$ αφού είναι κανονική υποομάδα. Άρα $\sigma^{-1}\tau\sigma(a) = a$. Συνεπώς, $\tau(b) = \sigma(a) = b$, δηλαδή $b \in F^H = L$. Καθώς το $Irr(a, F)$ διασπάται πλήρως στο K, με αυτό δείξαμε ότι διασπάται πλήρως στο L. Από την πρόταση 7 έχουμε ότι η επέκταση L/F είναι κανονική. Πράγματι, αν θεωρήσουμε τυχόν ανάγωγο $p(x) \in F[x]$ με ρίζα $a \in K$ αυτό θα ταυτίζεται με το $Irr(a, F)$ που διασπάται πλήρως στο K και όπως δείξαμε στο L. Επιπλέον, καθώς K/F είναι διαχωρίσιμη και $L \subseteq K$ έχουμε L/F διαχωρίσιμη από τον ορισμό. Άρα η επέκταση L/F είναι Galois.

Αντίστροφα, έστω ότι η επέκταση L/F είναι Galois. Έστω $\theta : G \to Gal(L/F)$ με τον κανόνα $\theta(\sigma) = \sigma|_L$. Η κανονικότητα της L/F μας δίνει ότι $\sigma|_L \in Gal(L/F)$ από την πρόταση 7, άρα ο θ είναι καλά ορισμένος ομομορφισμός ομάδων. Έχουμε:

$$ker\theta = \{\sigma \in K : \quad \sigma|_L = id\} = Gal(K/L) = H$$

και άρα η ομάδα H είναι κανονική στην G. Η απεικόνιση θ είναι επί, καθώς αν $\tau \in Gal(L/F)$ το θεώρημα επέκτασης ισομορφισμών μας δίνει $\sigma \in G$ με $\sigma|_L = \tau$. Άρα $Gal(L/F) \cong G/H$ από το πρώτο θεώρημα ισομορφισμών. □

Παράδειγμα 3. *θα μελετήσουμε τις αντιστοιχίες των υποσωμάτων του K και των υποομάδων του $G = Gal(K/\mathbb{Q})$, όπου $K \subseteq \mathbb{C}$ είναι το σώμα ριζών του $f(x) = x^4 - 2 \in \mathbb{Q}(x)$.*

Το $f(x)$ γράφεται στο $\mathbb{C}$ ως $(x-\rho)(x+\rho)(x-i\rho)(x+i\rho)$ όπου $\rho = \sqrt[4]{2}$. Δηλαδή $K = \mathbb{Q}(i, \rho)$ και η επέκταση $K/\mathbb{Q}$ είναι κανονική και διαχωρίσιμη, δηλαδή Galois. Έχουμε:

$$[\mathbb{Q}(\rho) : \mathbb{Q}] = 4$$

$$[\mathbb{Q}(\rho, i) : \mathbb{Q}(\rho)] = 2$$

επειδή $x^2 + 1$ ανάγωγο στο $\mathbb{Q}(\rho) \subseteq \mathbb{R}$ και άρα από θεώρημα πύργων μαζί με το ότι η επέκταση είναι Galois παίρνουμε:

$$[K : \mathbb{Q}] = 8 = |Gal(K/\mathbb{Q})|$$

Αν $\sigma \in G$ τότε από τις σχέσεις $\rho^4 = 2$ και $i^2 = -1$ έχουμε ότι $\sigma(\rho) \in \{\rho, -\rho, i\rho, -i\rho\}$ και $\sigma(i) \in \{i, -i\}$ και για κάθε επιλογή έχουμε τους $4 \cdot 2 = 8$ $\mathbb{Q}$-αυτομορφισμούς του K.

Έστω σ, τ που ορίζονται από:

$$\sigma(i) = i, \quad \sigma(\rho) = i\rho$$

$$\tau(i) = -i, \quad \tau(\rho) = \rho$$

Τότε με πράξεις έχουμε ότι $\sigma^4 = \tau^2 = 1_G$ και $(\sigma\tau)^2 = 1_G$. Δηλαδή έχουμε:

$$Gal(K, \mathbb{Q}) = \{1, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\} \cong D_4$$

όπου D_4 είναι η διεδρική ομάδα 8 στοιχείων.

Οι υποομάδες της D_4 εκτός από την τετριμμένη και την ίδια είναι οι:

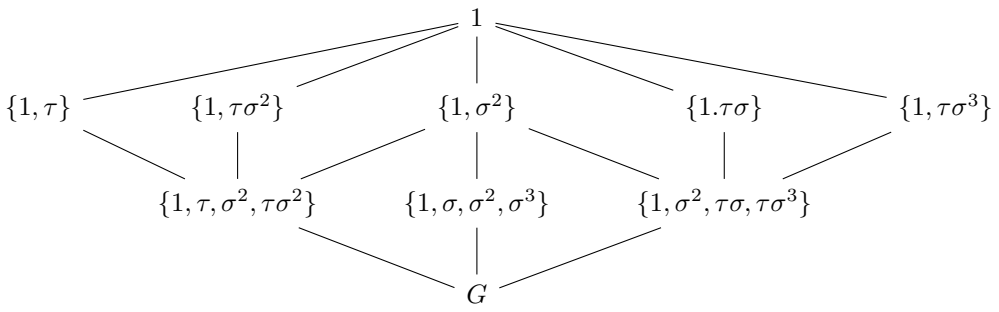
$$\{1, \tau\}, \{1, \tau\sigma^2\}, \{1, \sigma^2\}, \{1, \tau\sigma\}, \{1, \tau\sigma^3\}$$

$$\{1, \tau, \sigma^2, \tau\sigma^2\}, \{1, \sigma, \sigma^2, \sigma^3\}, \{1, \sigma^2, \tau\sigma, \tau\sigma^3\}$$

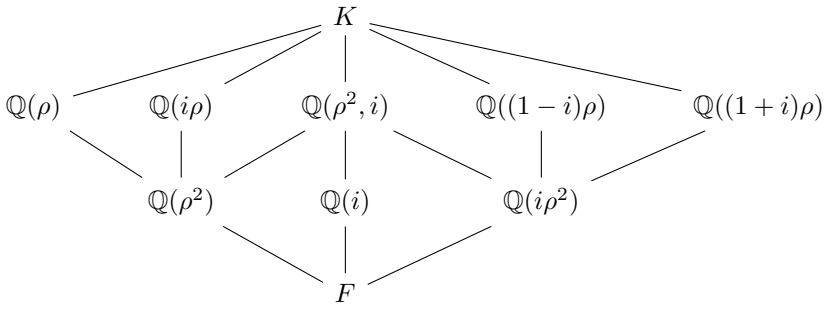
Στην συνέχεια υπολογίζοντας τα σταθερά σώματα των υποομάδων παίρνουμε το διάγραμμα υποσωμάτων από το διάγραμμα υποομάδων. Υπολογίζουμε ενδεικτικά τα σταθερά σώματα των $\{1, \sigma^2\}$ και $\{1, \tau\sigma\}$.

Έχουμε $\sigma^2(i) = i, \sigma^2(\rho) = \sigma(i\rho) = i(i\rho) = -\rho$ και άρα $\sigma^2(\rho^2) = \rho^2$. Συνεπώς $\mathbb{Q}(i, \rho^2) \subseteq F^{\{1,\sigma^2\}}$ και από θεμελιώδες θεώρημα $[F^{\{1,\sigma^2\}} : \mathbb{Q}] = [G : \{1, \sigma^2\}] = 4$. Καθώς $i \notin \mathbb{Q}(\rho^2)$ και $\rho^2 \notin \mathbb{Q}$ έχουμε $[\mathbb{Q}(i, \rho^2) : \mathbb{Q}] = 4$. Δηλαδή $F^{\{1,\sigma^2\}} = \mathbb{Q}(i, \rho^2)$.

Επιπλέον, $\tau\sigma((1-i)\rho) = \tau(\sigma(1-i)\sigma(\rho)) = \tau(1-i)\tau(i)\tau(r) = (1+i)(-i)\rho = (1-i)\rho$. Δηλαδή όμοια με πριν $F^{\{1,\tau\sigma\}} = \mathbb{Q}((1-i)\rho)$. Κάνοντας όλους τους υπολογισμούς έχουμε το διάγραμμα υποομάδων της D_4:



το οποίο το αντιστοιχούμε σε διάγραμμα υποσωμάτων του K:



2 Γενική Τοπολογία

Θα υπενθυμίσουμε όρους της τοπολογίας χωρίς να εμβαθύνουμε ιδιαίτερα, τους οποίους θα χρειαστούμε στο επόμενο κεφάλαιο.

Ορισμός (Τοπολογία). *Έστω $X \neq \varnothing$ σύνολο. Μια τοπολογία $\mathcal{T}$ στο X είναι ένα υποσύνολο $\mathcal{T} \subseteq \mathcal{P}(X)$ ώστε:*

(1) $\varnothing, X \in \mathcal{T}$.

(2) *Αν* $\{A_i : i \in I\} \subseteq \mathcal{T}$, *όπου* I *τυχόν σύνολο δεικτών, τότε* $\cup_{i\in I} A_i \in \mathcal{T}$.

(3) *Αν* $n \in \mathbb{N}$ *και* $A_1, \dots A_n \in \mathcal{T}$ *τότε* $\cap_{k=1}^{n} A_k \in \mathcal{T}$.

Το ζεύγος $(X, \mathcal{T})$ ονομάζεται τοπολογικός χώρος και τα μέλη της $\mathcal{T}$ ονομάζονται ανοικτά υποσύνολα του X. Επιπλέον, ονομάζουμε ένα υποσύνολο $F \subseteq X$ κλειστό αν F^C ανοικτό.

Αν $\mathcal{P}(x) = \mathcal{T}$ ονομάζουμε αυτήν την τοπολογία διακριτή, καθώς όλα τα υποσύνολα είναι ανοικτά και αυτό προέρχεται από την διακριτή μετρική.

Ορισμός (Κλειστή θήκη). *Έστω $(X, \mathcal{T})$ τοπολογικός χώρος και $A \subseteq X$. Η κλειστή θήκη ή κλειστότητα του A είναι το σύνολο:*

$$\overline{A} = \cap\{B : B \text{ κλειστό και } A \subseteq B\}$$

Πρόταση 11. *Έστω $(X, \mathcal{T})$ και $A \subseteq X$. Τότε $x \in \overline{A} \iff$ για κάθε ανοικτό $U \subseteq X$ με $x \in U$ ισχύει $U \cap A \neq \varnothing$.*

Ορισμός (Εσωτερικό). *Έστω $(X, \mathcal{T})$ τ.χ. και $A \subseteq X$. Τότε ορίζουμε ως εσωτερικό του A το:*

$$A^\circ = \cup\{B : B \subseteq A \text{ και } B \in \mathcal{T}\}$$

το οποίο είναι ανοικτό και τα σημεία του λέγονται εσωτερικά σημεία του A.

Επιπλέον, λέμε ότι το A είναι περιοχή του $x \in X$ αν $x \in A^\circ$. Όμοια λέμε ανοικτή περιοχή αν $A = A^\circ$ δηλαδή αν $A \in \mathcal{T}$.

Ορισμός (Βάση). *Έστω $(X, \mathcal{T})$ τοπολογικός χώρος. Μια οικογένεια $\mathcal{B} \subseteq \mathcal{T}$ λέμε ότι είναι βάση για την $\mathcal{T}$ αν κάθε ανοικτό μη κενό σύνολο είναι ένωση στοιχείων της $\mathcal{B}$.*

Ορισμός (Τοπολογία περιορισμός). *Έστω $(X, \mathcal{T})$ τ.χ. και $A \subseteq X$. Τότε η οικογένεια*

$$\mathcal{T}_A = \{A \cap U : \quad U \in \mathcal{T}\}$$

ονομάζεται τοπολογία περιορισμός στο A ή σχετική τοπολογία του A. Ο χώρος $(A, \mathcal{T}_A)$ είναι τοπολογικός υπόχωρος του X.

Ορισμός (Συνέχεια). *Εστω X, Y τοπολογικοί χώροι και $f : X \to Y$ συνάρτηση και $a \in X$. Λέμε ότι η f είναι συνεχής στο a αν για κάθε περιοχή V του $f(a)$ υπάρχει περιοχή U του a στον X ώστε $f(U) \subseteq V$.*

Πρόταση 12 (Χαρακτηρισμός συνέχειας). *Έστω X, Y τ.χ. και $f : X \to Y$ συνάρτηση. Τα ακόλουθα είναι ισοδύναμα:*

(1) *Η f είναι συνεχής.*

(2) *Για κάθε ανοικτό $V \subseteq Y$, το $f^{-1}(V)$ είναι ανοικτό στον X.*

(3) *Για κάθε κλειστό $F \subseteq Y$, το $f^{-1}(F)$ είναι κλειστό στον X.*

(4) *Για κάθε $A \subseteq X$ ισχύει ότι $f(\overline{A}) \subseteq \overline{f(A)}$.*

Ορισμός (Ομοιομορφισμός)**.** *Μια συνάρτηση f μεταξύ δύο τοπολογικών χώρων X, Y λέγεται ομοιομορφισμός αν είναι 1-1, επί και αν οι f, f^{-1} είναι συνεχείς. Τότε οι χώροι X, Y λέγονται ομοιομορφικοί και στην ουσία ταυτίζονται ως τοπολογικοί χώροι.*

Ορισμός (Καρτεσιανό Γινόμενο)**.** *Έστω $\{X_i : i \in I\}$ οικογένεια συνόλων. Το καρτεσιανό γινόμενο $\prod_{i\in I} X_i$ είναι το σύνολο όλων των συναρτήσεων $f : I \to \cup_{i\in I} X_i$ με $f(i) \in X_i$ για κάθε $i \in I$. Αν $X_i = X$ για κάθε $i \in I$ τότε συμβολίζεται το καρτεσιανό γινόμενο και ως X^I. Ένα στοιχείο $f \in \prod_{i\in I} X_i$ γράφεται ως $(x_i)_{i\in I}$ ή (x_i), δηλαδή $f(i) = x_i$ για κάθε $i \in I$. Με αυτόν τον συμβολισμό το $x_j \in X_j$ ονομάζεται j-συντεταγμένη του (x_i) και το X_j είναι ο j-παράγοντας του $\prod_{i\in I} X_i$. Επιπλέον, για κάθε $j \in I$ η απεικόνιση $\pi_j : \prod_{i\in I} X_i \to X_j$ με κανόνα $\pi_j((xi)) = x_j$ ονομάζεται η προβολή στην j-συντεταγμένη.*

Υπενθυμίζουμε και το αξιώμα επιλογής, στο οποίο βασιζόμαστε για να ορίσουμε την τοπολογία γινόμενο.

Πρόταση 13 (Αξίωμα Επιλογής)**.** *Έστω $\{X_i : i \in I\}$ μη κενή οικογένεια μη κενών συνόλων, τότε $\prod_{i\in I} X_i \neq \varnothing$. Δηλαδή, $I \neq \varnothing$ και $X_i \neq \varnothing$ για κάθε $i \in I \implies \prod_{i\in I} X_i \neq \varnothing$.*

Ορισμός (Τοπολογία γινόμενο)**.** *Έστω $(X_i, \mathcal{T}_i)$ οικογένεια τοπολογικών χώρων, η τοπολογία γινόμενο ή καρτεσιανή τοπολογία επί του $X = \prod_{i\in I} X_i$ είναι εκείνη η (μοναδική) τοπολογία η οποία έχει σαν βάση την οικογένεια:*

$$B = \Big\{ \prod_{i\in I} U_i : \quad U_i \in \mathcal{T}_i \text{ και } \{i \in I : U_i \neq X_i\} \text{ πεπερασμένο } \Big\}$$

Πρόταση 14. *Η προβολή $\pi_j : \prod_{i\in I} X_i \to X_j$ είναι συνεχής απεικόνιση και επιπλέον στέλνει τα ανοικτά σε ανοικτά, για κάθε $j \in I$.*

Ορισμός (Τοπολογία πηλίκο)**.** *Έστω $Y \neq \varnothing$ σύνολο, X τοπολογικός χώρος και $f : X \to Y$ μια απεικόνιση του X στο Y. Η τοπολογία πηλίκο στο Y η οποία ορίζεται από την f είναι η*

$$\mathcal{T}(f) = \{U \subseteq Y : f^{-1}(U) \text{ ανοικτό στον } X\}$$

μπορούμε και να ερμηνεύσουμε την f ως την κανονική απεικόνιση $x \in X \mapsto [x] \in X/\sim$ της σχέσης ισοδυναμίας του X: $x \sim y \iff f(x) = f(y)$ ταυτίζοντας το Y με τον χώρο των κλάσεων ισοδυναμίας $X/\sim$. Οι κλάσεις έχουν μορφή $[x] = f^{-1}(f(x))$ και ένα ανοικτο υποσύνολο του $X/\sim$ είναι μια οικογένεια κλάσεων ισοδυναμίας των οποίων η ένωση είναι ανοικτό υποσύνολο του X.

Ορισμός (Hausdorff)**.** *Έστω X τοπολογικός χώρος. Ο X λέγεται Hausdorff ή T_2 αν για κάθε ζεύγος $x \neq y$ του X υπάρχουν ξένα ανοικτά σύνολα U, V τέτοια ώστε $x \in U$ και $y \in V$.*

Ορισμός (Συμπάγεια)**.** *Εστω X τ.χ. και $K \subseteq X$. Ο X λέγεται συμπαγής, αν κάθε ανοικτό κάλυμμα $\{U_i : i \in I\}$ του X έχει πεπερασμένο υποκάλλυμα. Δηλαδή αν*

$$X = \bigcup_{i \in I} U_i \implies \exists F \subseteq I \text{ πεπερασμένο: } X = \bigcup_{i \in F} U_i$$

Το K λέγεται συμπαγές υποσύνολο του X αν είναι συμπαγής υπόχωρος του X με την σχετική τοπολογία.

Πρόταση 15. *Έστω $\{X_i : i \in I\}$ οικογένεια τοπολογικών χώρων. Τότε ο $X = \prod_{i \in I} X_i$ είναι Hausdorff αν και μόνο αν κάθε X_i είναι Hausdorff.*

Πρόταση 16 (Θ. Tychonoff)**.** *Έστω $\{X_i : i \in I\}$ οικογένεια τοπολογικών χώρων. Τότε ο $X = \prod_{i \in I} X_i$ είναι συμπαγής αν και μόνο αν κάθε X_i είναι συμπαγής.*

Ορισμός (Συνεκτικότητα)**.** *Ένας τοπολογικός χώρος X λέγεται συνεκτικός αν δεν είναι ένωση δύο ξένων ανοικτών μη κενών υποσυνόλων του. Δηλαδή, δεν υπάρχουν ανοικτά $U, V \neq \varnothing$ ώστε $U \cap V = \varnothing$ και $X = U \cup V$.*

Ένα υποσύνολο $A \subseteq X$ λέγεται συνεκτικό υποσύνολο αν είναι συνεκτικό ως υπόχωρος του X με την σχετική τοπολογία.

Ορισμός (Totally Disconnected)**.** *Ένας τοπολογικός χώρος X λέγεται totally disconnected αν τα μόνα συνεκτικά υποσύνολα του X είναι τα μονοσύνολα.*

3 Άπειρη θεωρία Galois

Εδώ ξεκινάμε να χτίζουμε την θεωρία για τις άπειρες επεκτάσεις που θα μας απασχολήσουν. Για όλη την ενότητα θα βασιστούμε αρκέτα στους ακόλουθους συμβολισμούς.

Έστω K/F Galois επέκταση, τότε συμβολίζουμε:

$$G = Gal(K/F)$$
$$\mathcal{I} = \{E : K/E/F, \quad [E : F] < \infty, \quad E/F \quad \text{Galois } \}$$
$$\mathcal{N} = \{N \subseteq G : N = Gal(K/E) \quad \text{για κάποιο } E \in \mathcal{I}\}$$

Υπενθύμιση: Από λήμμα 7, αν K/F κανονική επέκταση και $N/K/L/F$ σώματα με $\tau : L \mapsto N$ ένας F-ομομορφισμός, τότε $\tau(L) \subseteq K$ και υπάρχει $\sigma \in Gal(K/F)$ με $\sigma|_L = \tau$.

Λήμμα 11. *Αν $a_1, \dots a_n \in K$ τότε υπάρχει $E \in \mathcal{I}$ με $a_i \in E$ για κάθε $i \in \{1, \dots, n\}$.*

Απόδειξη.

Έστω $E \subseteq K$ το σώμα ριζών των ελαχίστων πολυωνύμων των a_i υπεράνω του F, δηλαδή το σώμα ριζών του γινομένου τους. Κάθε a_i είναι διαχωρίσιμο υπεράνω του F, εφόσον είναι στοιχείο της διαχωρίσιμης επέκτασης K/F, αρα το E είναι κανονική επέκταση του F και διαχωρίσιμη, επομένως η επέκταση E/F είναι Galois. Καθώς έχουμε πεπερασμένα a_i τότε $[E : F] < \infty$, επομένως $E \in \mathcal{I}$.

□

Λήμμα 12. *Αν $N \in \mathcal{N}$ με $N = Gal(K/E)$, $E \in \mathcal{I}$ τότε $E = F^N$ και $N \trianglelefteq G$. Τότε έχουμε τον ισομορφισμό $G/N \cong Gal(E/F)$ και επιπλέον $|G/N| = |Gal(E/F)| = [E : F] < \infty$.*

Απόδειξη.

Το σώμα K είναι κανονική και διαχωρίσιμη επέκταση υπεράνω του F το οποίο συνεπάγεται ότι είναι και υπεράνω του E. Δηλαδή K/E Galois και συνεπώς $E = F^N$. Όπως στην απόδειξη του θεμελιώδους θεωρήματος της θεωρίας Galois, η απεικόνιση $\theta : G \mapsto Gal(E/F)$ με κανόνα $\sigma \mapsto \sigma|_E$ είναι ένας ομομορφισμός ομάδων με πυρήνα $Gal(K/E) = N$. Από την υπενθύμιση της πρότασης 7 έχουμε ότι το θ είναι επιμορφισμός. Τα υπόλοιπα έπονται από το 1ο θεώρημα ισομορφισμών ομάδων και ότι η επέκταση E/F είναι Galois. □

Λήμμα 13. *$\bigcap_{N \in \mathcal{N}} N = \{1_G\} = \{id : K \mapsto K\}$. Επιπλέον, $\bigcap_{N \in \mathcal{N}} \sigma N = \{\sigma\}$ για κάθε $\sigma \in G$.*

Απόδειξη.

Έστω $\tau \in \bigcap_{N \in \mathcal{N}} N$ και $a \in K$. Από το λήμμα 11 υπάρχει $E \in \mathcal{I}$ με $a \in E$. Έχουμε $N := Gal(K/E) \in \mathcal{N}$ εφόσον $E \in \mathcal{I}$. Ο αυτομορφισμός τ κρατάει σταθερό το E καθώς $\tau \in N$, επομένως $\tau(a) = a$ για το τυχόν $a \in K$. Συνεπώς $\tau = id_K$ και άρα αυτό είναι το μοναδικό στοιχείο της τομής. Για το δεύτερο επιχείρημα, αν $\tau \in \sigma N$ για κάθε N τότε $\sigma^{-1}\tau \in N$ για κάθε N, επομένως $\sigma^{-1}\tau = id_K$ και άρα $\tau = \sigma$ για το τυχόν $\tau \in \bigcap_{N \in \mathcal{N}} \sigma N$. □

Λήμμα 14. *Αν $N_1, N_2 \in \mathcal{N}$ τότε $N_1 \cap N_2 \in \mathcal{N}$.*

Απόδειξη.

Έστω $N_i = Gal(K/E_i)$ με $E_i \in \mathcal{I}$. Κάθε E_i είναι πεπερασμένη επέκταση Galois του F,

επομένως το σώμα E_1E_2 είναι και αυτό πεπερασμένη επέκταση Galois του F, άρα $E_1E_2 \in \mathcal{I}$. Ωστόσο, έχουμε ότι $Gal(K/E_1E_2) = N_1 \cap N_2$. Πράγματι,

$$\sigma \in N_1 \cap N_2 \iff \sigma|_{E_1} = id \text{ και } \sigma|_{E_2} = id \iff E_1 \subseteq F^{(\sigma)} \text{ και } E_2 \subseteq F^{(\sigma)}$$

$$\iff E_1E_2 \subseteq F^{(\sigma)}$$

όπου η τελευταία σχέση είναι ισοδύναμη με την $\sigma \in Gal(K/E_1E_2)$. Επομένως $N_1 \cap N_2 = Gal(K/E_1E_2) \in \mathcal{N}$. □

Τώρα θα ορίσουμε την τοπολογία στην ομάδα Galois G.

Ορισμός (Τοπολογία Krull)**.** *$(G, \mathcal{T})$ είναι τοπολογικός χώρος όπου $\mathcal{T}$ είναι η τοπολογία Krull που ορίζεται ως εξής: Ένα υποσύνολο X του G είναι ανοιχτό αν $X = \varnothing$ ή $X = \cup_i \sigma_i N_i$ για κάποια $\sigma_i \in G$ και $N_i \in \mathcal{N}$.*

Βέβαια πρέπει να δείξουμε ότι πράγματι έχουμε μια τοπολογία. Από τον ορισμό το $\varnothing$ είναι ανοιχτό και οι ενώσεις ανοιχτών είναι ανοιχτό σύνολο. Έχουμε ότι $F \in \mathcal{I}$ και άρα $G \in \mathcal{N}$, δηλαδή το G μπορεί να γραφτεί ως ένωση εφόσον κάποιο $N_i = G$. Μένει να δείξουμε την κλειστότητα στις πεπερασμένες τομές.

Έχουμε ότι:

$$\left(\bigcup_i \sigma_i N_i\right) \cap \left(\bigcup_j \sigma_j N_j\right) = \bigcup_{i,j} (\sigma_i N_i \cap \sigma_j N_j)$$

και άρα αρκεί να δείξουμε ότι το $\tau_1 N_1 \cap \tau_2 N_2$ είναι ανοιχτό για κάθε $N_1, N_2 \in \mathcal{N}$. Πράγματι, έστω $\sigma \in \tau_1 N_1 \cap \tau_2 N_2$, τότε :

$$\tau_1 N_1 \cap \tau_2 N_2 = \sigma N_1 \cap \sigma N_2 = \sigma(N_1 \cap N_2)$$

και το $\sigma(N_1 \cap N_2)$ είναι ανοιχτό εφόσον $N_1 \cap N_2 \in \mathcal{N}$ από το λήμμα 14.

3.1 Ιδιότητες της τοπολογίας Krull

Εφόσον κάθε μη κενό ανοιχτό υποσύνολο του G έχει οριστεί ως ένωση τότε το σύνολο:

$$\{\sigma N : \sigma \in G, N \in \mathcal{N}\}$$

είναι βάση της τοπολογίας.

Αν τώρα $N \in \mathcal{N}$ τότε $|G : N| < \infty$ οπότε αν S είναι ένα σύνολο αντιπροσώπων των συμπλόκων του N τότε έχουμε:

$$G - \sigma N = \bigcup_{a \in S, a \notin \sigma N} aN$$

δηλαδή, το $G - \sigma N$ είναι πεπερασμένων ένωση συμπλόκων του N. Επομένως, το σN είναι και ανοιχτό και κλειστό (clopen). Καταλήξαμε στο ότι αυτή η τοπολογία έχει βάση από ανοιχτά κλειστά σύνολα.

Πρόταση 17. *Ο τοπολογικός χώρος $(G, \mathcal{T})$ είναι Hausdorff.*

Απόδειξη. Έστω $\sigma, \tau \in G, \sigma \neq \tau$. Από το λήμμα 13 έχουμε ότι

$$\{\sigma\} = \bigcap_N \sigma N$$

δηλαδή υπάρχει $N \in \mathcal{N}$ έτσι ώστε $\tau \notin N \implies \tau \in G - \sigma N$. Τα $\sigma N, G - \sigma N$ είναι ανοιχτά και διαχωρίζουν τα σ, τ. □

Πρόταση 18. *Ο τοπολογικός χώρος $(G, \mathcal{T})$ είναι totally disconnected.*

Απόδειξη. Έστω $X \subseteq G$ που περιέχει τουλάχιστον δύο στοιχεία σ, τ. Όμοια με την προηγούμενη απόδειξη, υπάρχει σN ανοιχτή περιοχή του σ που δεν περιέχει το τ. Συνεπώς:

$$X = (\sigma N \cap X) \bigcup ((G - \sigma N) \cap X)$$

δηλαδή το X γράφεται ως ένωση ξένων, μη κενών ανοιχτών (της $\mathcal{T}_X$). Άρα τα μοναδικά συνεκτικά υποσύνολα του G είναι μονοσύνολα. □

Στην συνέχεια ακολουθεί και η πιο σημαντική ιδιότητα της τοπολογίας Krull, η οποία είναι και αρκετά πιο δύσκολη να αποδειχθεί.

Πρόταση 19. *Ο τοπολογικός χώρος $(G, \mathcal{T})$ είναι συμπαγής.*

Απόδειξη.

Θα δείξουμε ότι το G μπορεί να κατασκευαστεί από πεπερασμένες Galois ομάδες. Θεωρούμε τις ομάδες πηλίκο G/N οι οποίες είναι πεπερασμένες (από το λήμμα 12) και θέτουμε

$$P = \prod_{N \in \mathcal{N}} G/N$$

το ευθύ γινόμενό των ομάδων.

Αν Θεωρήσουμε τους τοπολογικούς χώρους $(G/N, \mathcal{T}_\delta)$, όπου $\mathcal{T}_\delta$ η διακριτή τοπολογία, μπορούμε να κάνουμε το P τοπολογικό χώρο δίνοντάς του την τοπολογία γινόμενο. Στην συνέχεια, τα G/N είναι πεπερασμένα και άρα συμπαγή. Άρα, από το θεώρημα Tychonoff το P είναι συμπαγής τοπολογικός χώρος. Επιπλέον, κάθε G/N είναι Hausdorff ως πεπερασμένο με διακριτή τοπολογία και η ιδιότητα Hausdorff διατηρείται στο γινόμενο, άρα ο P είναι επίσης Hausdorff.

Υπάρχει τώρα ένας φυσικός ομομορφισμός ομάδων:

$$f : G \longrightarrow P$$

$$\sigma \longmapsto \{\sigma N\} = \prod_{N \in \mathcal{N}} \sigma N$$

Είναι πράγματι ομομορφισμός ομάδων εφόσον:

$$\sigma \circ \tau \longmapsto \prod_{N \in \mathcal{N}} (\sigma \circ \tau) N$$

και

$$f(\sigma) f(\tau) = \left(\prod_{N \in \mathcal{N}} \sigma N \right) \left(\prod_{N \in \mathcal{N}} \tau N \right) = \prod_{N \in \mathcal{N}} (\sigma N)(\tau N) = \prod_{N \in \mathcal{N}} (\sigma \circ \tau) N$$

όπου στην δεύτερη ισότητα ή πράξη γίνεται στο ευθύ γινόμενο ομάδων ΄κατά συντεταγμένη΄ και στην επόμενη ισότητα είναι η πράξη εξ΄ορισμού της ομάδας πηλίκο G/N.

Στην συνέχεια θα δείξουμε ότι η f είναι ομοιομορφισμός, αν θεωρήσουμε ως σύνολο άφιξης την εικόνα της, και ότι η εικόνα της είναι κλειστό υποσύνολο του P. Από εκεί θα έπεται ότι η εικόνα θα είναι συμπαγής. Συνεπώς, μέσω του ομοιομορφισμού f θα έχουμε δείξει το ζητούμενο.

Έστω $f : G \to imf$ όπως παραπάνω και $\sigma \in G$ τέτοιο ώστε $\{\sigma N\} = \{N\}$.

$$\sigma \in ker(f) \iff \{\sigma N\} = \{N\} \iff \sigma \in \bigcap_{N\in\mathcal{N}} N = \{id\}$$

όπου η τελευταία ισότητα ισχύει από το λήμμα 13. Συνεπώς, η f είναι 1-1 και εξ΄ορισμού επί.

Έστω $\pi_N : P \to G/N$ η προβολή στον N-παράγοντα. Τότε $\pi_N(f(\sigma)) = \sigma N$ για κάθε $\sigma \in G$. Στη διακριτή τοπολογία στα G/N η βάση αποτελείται από μονοσύνολα, δηλαδή στοιχεία της μορφής τN. Κάθε ανοιχτό υποσύνολο του P είναι ένωση βασικών και από τον ορισμό της τοπολογίας γινόμενο, κάθε βασικό στοιχείο είναι πεπερασμένη τομή συνόλων της μορφής $\pi_N^{-1}(\tau N)$ για διάφορα $\tau \in G$ και $N \in \mathcal{N}$.

Θα δείξουμε πρώτα ότι η f^{-1} είναι συνεχής, αρκεί η f να είναι ανοιχτή, δηλαδή να στέλνει ανοιχτά σε ανοιχτά. Έστω σH ενα βασικό ανοιχτό, έχουμε $\sigma \in G, H \in N$ και άρα υπάρχει $E \in \mathcal{I}$ τέτοιο ώστε $H = Gal(K/E)$. Τότε:

$$f(\sigma H) = \{(\sigma h N)_{N\in\mathcal{N}} | \quad h \in H, h|_E = 1_E\} = \{(\sigma h N)_{N\in\mathcal{N}} | \quad h \in H, \sigma h|_E = \sigma|_E\}$$

$$= \{(\tau N)_{N\in\mathcal{N}} | \quad \tau|_E = \sigma|_E\} = \pi_H^{-1}(\sigma H)$$

όπου η τελευταία ισότητα ισχύει εφόσον:

Αν $(\tau N)_{N\in\mathcal{N}}$ με $\tau|_E = \sigma|_E$ τότε έστω $x \in E$, έχουμε: $\sigma^{-1}\tau(x) = \sigma^{-1}\sigma(x) = x$ δηλαδή το $\sigma^{-1}\tau$ κρατάει σταθερό το E αν και μόνο αν $\sigma^{-1}\tau \in H \iff \sigma^{-1}\tau H = H \iff \sigma H = \tau H$. Άρα αν πάρουμε την προβολή $\pi_H\left((\tau N)_{N\in\mathcal{N}}\right) = \tau H = \sigma H$. Έχουμε συνεπώς την μια σχέση του περιέχεσθαι.

Αντίστροφα, αν $(\tau N)_{N\in\mathcal{N}}$ τέτοιο ώστε:

$$\tau H = \pi_H\left((\tau N)_{N\in\mathcal{N}}\right) = \sigma H$$

$$\tau H = \sigma H$$

και $x \in E$ τότε $\sigma h_1(x) = \tau h_2(x) \implies \sigma(x) = \tau(x)$ και άρα $\sigma|_E = \tau|_E$. Έχουμε από ορισμό της τοπολογίας γινόμενο ότι $\pi_H^{-1}(\sigma H)$ ανοιχτό (στο P) και $f(\sigma H) \subseteq imf$ άρα $f(\sigma H) = \pi_H^{-1}(\sigma H) \cap imf$ ανοιχτό στο imf.

Με βάση τα προηγούμενα, για να δείξουμε ότι η f αντιστρέφει ανοιχτά σε ανοιχτά αρκεί να ισχύει ότι το $f^{-1}(\pi_N^{-1}(\sigma H))$ είναι ανοιχτό στο G για κάθε σH. Πράγματι:

$$f^{-1}(\pi_H^{-1}(\sigma N)) = f^{-1}(\{(\tau N)_{N\in\mathcal{N}} | \quad \tau|_E = \sigma|_E\}) = \sigma H$$

το οποίο είναι ανοιχτό.

Μένει να δείξουμε ότι η εικόνα imf είναι κλειστή στο P. Εδώ αντί για G/N θα χρησιμοποιούμε το ισόμορφό του $Gal(E_N/F)$ με $E_N = F^N$ με βάση το λήμμα 12. Έτσι, θα αναγνωρίζουμε το σύμπλοκο τN ως $\tau|_{E_N}$. Με αυτή τη σύμβαση, αν $p \in P$ δηλαδή $p = (\tau_N N)_N$ τότε $\pi_N(p) = \tau_N N = \tau_N|_{E_N}$ είναι ένας αυτομορφισμός του E_N. Θέτουμε:

$$C = \{p \in P : \forall N, M \in \mathcal{N}, \quad \pi_N(p)|_{E_N\cap E_M} = \pi_M(p)|_{E_N\cap E_M}\}$$

Θα δείξουμε ότι $C = imf$. Για την κατεύθυνση $imf \subseteq C$ έχουμε ότι:

$$\pi_N(f(\tau))|_{E_N} = \pi_N[(\tau N)_{N\in\mathcal{N}}]|_{E_N} = (\tau N)|_{E_N} = (\tau|_{E_N})|_{E_N} = \tau|_{E_N}$$

για κάθε $\tau \in G$. Άρα:

$$\pi_N(f(\tau))|_{E_N\cap E_M} = (\tau|_{E_N})|_{E_N\cap E_M} = \tau|_{E_N\cap E_M} = (\tau|_{E_M})|_{E_N\cap E_M} = \pi_M(f(\tau))|_{E_N\cap E_M}$$

δηλαδή για κάθε $\tau \in G$ ισχύει ότι $f(\tau) \in C$.

Αντίστροφα, έστω $p \in C$. Ορίζουμε $\tau : K \to K$ τέτοια ώστε αν $a \in K$ διαλέγουμε ένα $E_N \in \mathcal{I}$ με $a \in E_N$, γνωρίζουμε ότι υπάρχει τέτοιο από το λήμμα 11, έτσι ώστε $a \mapsto \pi_N(p)(a)$. Για να είναι καλά ορισμένη απεικόνιση πρέπει να μην εξαρτάται από την επιλογή του E_N και αυτό ακριβώς μας παρέχει η συνθήκη του $p \in C$. Δηλαδή, διαλέγουμε E_N, E_M τέτοια ώστε $a \in E_N, E_M \implies a \in E_N \cap E_M$ και άρα εφόσον $p \in C$ ισχύει ότι:

$$\pi_N(p)(a) = \pi_M(p)(a)$$

Το τ είναι και ομομορφισμός δακτυλίων. Πράγματι, αν $a, b \in K$ και έστω $E_N \in I$ με $a, b \in E_N$ τότε το τ δρα κατάλληλα στα a, b μέσω του ομομορφισμού $\tau|_{E_N} = \pi_N(p)$.

Επιπλέον είναι 1-1 και επί εφόσον μπορούμε μέσω του $p^{-}1$ να κατασκευάσουμε το τ^{-1}, δηλαδή:

$$\pi_N(p^{-1})(a) = (\pi_N(p))^{-1}(a) = \tau^{-1}(a)$$

Στην συνέχεια, αν το x ανήκει στο στο αρχικό σώμα F που έχουμε θεωρήσει στην αρχή του κεφαλαίου, διαλέγουμε $E_N \in \mathcal{I}$ με $x \in E_N$ όμοια με πριν και άρα το $\pi_N(p)$ είναι εξ ορισμού στοιχείο του G. Δηλαδή είναι F-ισομορφισμός του K περιορισμένος στο E_N. Άρα έχουμε ότι $\pi_N(p) \in Gal(E_N/F)$ και συνεπώς $\tau \in G$.

Έτσι καθώς έχουμε $\tau|_{E_N} = \pi_N(p)$ ισχύει ότι:

$$f(\tau) = (\tau N)_{N \in \mathcal{N}} = (\tau|_{E_N})_{N \in \mathcal{N}} = (\pi_N(p))_{N \in \mathcal{N}} = p$$

δηλαδή $p \in imf \implies C = imf$.

Για την κλειστότητα, έστω $p \in P \setminus C$. Δηλαδή, υπάρχουν $N, M \in \mathcal{N}$ τέτοια ώστε:

$$\pi_N(p)|_{E_N \cap E_M} \neq \pi_M(p)|_{E_N \cap E_M}$$

Για το σύνολο:

$$X = \pi_N^{-1}(\pi_N(p)) \bigcap \pi_M^{-1}(\pi_M(p))$$

έχουμε ότι περιέχει το p και ότι είναι ανοιχτό υποσύνολο του P ως πεπερασμένη τομή ανοιχτών, από ορισμό προβολών στην τοπολογία γινόμενο. Αν $x \in X$, τότε παίρνουμε τις προβολές $\pi_N(x) = \pi_N(p)$ και $\pi_M(x) = \pi_M(p)$ τα οποία δεν είναι ίσα καθώς παραπάνω φαίνεται ότι δεν ταυτίζονται στον περιορισμό στο $E_N \cap E_M$. Δηλαδή το X περιέχεται εξόλοκλήρου στο P και συνεπώς είναι ανοιχτή περιοχή του τυχαίου $p \in P \setminus C$. Καταλήξαμε στο ότι $P \setminus C$ ανοιχτό, ισοδύναμα C κλειστό. □

Το επόμενο θεώρημα είναι το τελευταίο βήμα που χρειαζόμαστε για να επεκτείνουμε το θεμελιώδης θεώρημα σε άπειρες επεκτάσεις Galois. Εδώ θα φανεί πως χρησιμοποιείται η τοπολογία στο G και έρχεται σε αναλογία με την πρόταση ότι αν G είναι μια πεπερασμένη ομάδα αυτομορφισμών του K τότε $G = Gal(K/F^G)$.

Θεώρημα 10. *Έστω H υποομάδα της G και έστω $H' = Gal(K/F^H)$. Τότε $H' = \overline{H}$, η κλειστή θήκη του H στην τοπολογία του G.*

Απόδειξη.

Από τον ορισμό του σταθερού σώματος έχουμε ότι $H \subseteq H'$. Αρκεί να δείξουμε ότι το H' είναι κλειστό και ότι $H' \subseteq \overline{H}$.

Έστω $\sigma \in G - H'$. Τότε υπάρχει $a \in F^H$ τέτοιο ώστε $\sigma(a) \neq a$. Παίρνουμε $E \in \mathcal{I}$ με $a \in E$ και θεωρούμε την ομάδα $N = Gal(K/E) \in \mathcal{N}$. Για κάθε $\tau \in N$ έχουμε $\tau(a) = a$ εφόσον κρατάνε οι ισομορφισμοί σταθερό το E και έτσι $\sigma\tau(a) = \sigma(a) \neq a$. Δηλαδή, το σN είναι ανοιχτή περιοχή του σ και ξένη με το H'. Συνεπώς το $G - H'$ είναι ανοιχτό και άρα το H' κλειστό.

Για να δείξουμε ότι $H' \subseteq \overline{H}$, έστω $\sigma \in H'$ με $N \in \mathcal{N}$ και $E = F^N \in \mathcal{I}$. Ορίζουμε:

$$H_0 = \{p|_E : p \in H\} \leq Gal(E/F)$$

όπου είναι πράγματι υποομάδα της πεπερασμένης $Gal(E/F)$ εφόσον οι αυτομορφισμοί της είναι αυτομορφισμοί της $H \subseteq G$ που κρατάνε σταθερό το F και είναι περιορισμένοι στο E. Έχουμε:

$$F^{H_0} = \{a \in K : p|_E(a) = a \quad \forall p|_E \in H_0\} = E \cap \{a \in K : p(a) = a \quad \forall p \in H\} = E \cap F^H$$

Από αντιστοιχία Galois για την πεπερασμένη $Gal(E/F)$ έχουμε $H_0 = Gal(E/(E \cap F^H))$.

$$\begin{array}{ccccc} 1 & & E & & 1 \\ | & & | & & | \\ H_0 & \xrightarrow{H \longmapsto F^H} & F^{H_0} & \xrightarrow{L \longmapsto Gal(E/L)} & H_0 \\ | & & | & & | \\ Gal(E/F) & & F & & Gal(E/F) \end{array}$$

Αν $\sigma \in Gal(K/F^H)$, τότε $\sigma|_{F^H} = id$ δηλαδή το σ κρατάει σταθερό το $E \cap F^H \subseteq F^H$ και άρα αν το περιορίσουμε στο E έχουμε:

$$\sigma|_E \in Gal(E/(E \cap F^H)) = H_0$$

Από ορισμό H_0 υπάρχει $p \in H$ με $p|_E = \sigma|_E$. Δηλαδή $\sigma^{-1}p|_E = 1_E$. Άρα έχουμε:

$$\sigma^{-1}p \in Gal(K/E) = N \implies p \in \sigma N \cap H$$

Δηλαδή, αφού το N ήταν τυχόν, κάθε βασική ανοιχτή περιοχή σN του $\sigma \in H'$ τέμνει το H, το οποίο είναι ισοδύναμο από χαρακτηρισμό κλειστής θήκης ότι $\sigma \in \overline{H}$.

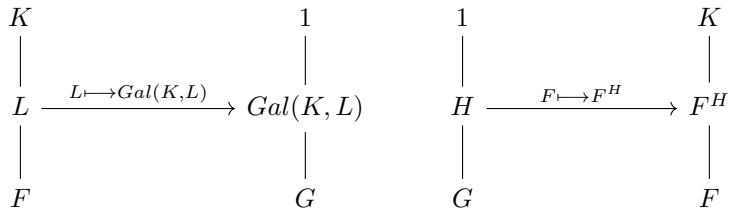
□

3.2 Θεμελιώδες Θεώρημα της Άπειρης Θεωρίας Galois

Θεώρημα 11 (Θεμελιώδες Θεώρημα της Άπειρης Θεωρίας Galois)**.** *Έστω K/F Galois επέκταση και $G = Gal(K/F)$. Με την Krull τοπολογία στο G οι απεικονίσεις $L \mapsto Gal(K/L)$ και $H \mapsto F^H$ είναι 1-1 και εμφυτεύουν τα σύνολα:*

$$\{L : K/L/F\} \longleftrightarrow \{H \leq G : H = \overline{H}\}$$

το ένα στο άλλο με την ανάποδη αντιστοιχία. Δηλαδή αν H κλειστό και $K/L/F$ έχουμε:



Επιπλέον, αν $L \longleftrightarrow H$ *τότε* $|G : H| < \infty \iff [L : F] < \infty$*, αν και μόνο αν το* H *είναι ανοιχτό στην τοπολογία. Όταν αυτό συμβαίνει, ισχύει* $|G : H| = [L : F]$*. Ακόμα,* $H \trianglelefteq G$ *αν και μόνο αν η επέκταση* L/F *είναι Galois. Όταν αυτό συμβαίνει έχουμε τον ισομορφισμό ομάδων* $Gal(L/F) \cong G/H$*. Αν εμπλουτίσουμε την ομάδα πηλίκο* G/H *με την τοπολογία πηλίκο, τότε αυτός ο ισομορφισμός είναι και ομοιομορφισμός.*

Απόδειξη.

Έστω L υπόσωμα του K που περιέχει το F, τότε εφόσον το K είναι κανονική και διαχωρίσιμη επέκταση του F θα ισχύουν και τα ίδια υπεράνω του L. Έτσι έχουμε ότι η επέκταση K/L είναι Galois και άρα $L = F^{Gal(K/L)}$. Αν $H \leq G$ τότε από το προηγούμενο θεώρημα έχουμε ότι $H = Gal(K/F^H)$ αν και μόνο αν το H είναι κλειστό. Άρα έχουμε την ζητούμενη αντιστοιχία.

Έστω L ενδιάμεσο σώμα της K/F και έστω $H = Gal(K/L)$, δηλαδή H κλειστό από το προηγούμενο θεώρημα. Αν υποθέσουμε ότι $|G : H| < \infty$ έχουμε την ξένη ένωση:

$$G = H \cup a_1 \cup \ldots \cup a_n H$$

Αυτό σημαίνει ότι το $G - H$ είναι πεπερασμένη ένωση συμπλόκων του H. Ωστόσο, επειδή το H είναι κλειστό θα είναι και κάθε σύμπλοκο του κλειστό, δηλαδή θα είναι το $G - H$ κλειστό και συνεπώς το H ανοιχτό. Πράγματι, έστω $x \in \overline{aH}$. Τότε:

$$\begin{aligned} & xN \cap aH \neq \varnothing \quad \forall N \in \mathcal{N} \\ \iff & a^{-1}xN \cap H \neq \varnothing \quad \forall N \in \mathcal{N} \\ \iff & a^{-1}x \in \overline{H} = H \implies x \in aH \end{aligned}$$

Αντίστροφα, αν το H είναι ανοιχτό τότε περιέχει μια βασική περιοχή του id. Δηλαδή υπάρχει $N \in \mathcal{N}$ τέτοιο ώστε:

$$idN = N \subseteq H \implies F^N \supseteq F^N$$

δηλαδή $L \subseteq E$, αν θεωρήσουμε $E = F^N$. Επειδή $N \in \mathcal{N}$, έχουμε ότι $E \in \mathcal{I}$ και άρα $[E : F] < \infty$. Από κανόνα πύργων παίρνουμε:

$$[E : F] = [E : L][L : F]$$

και άρα $[L : F] < \infty$.

Για την τελευταία κατεύθυνση, αν $[L : F] < \infty$ τότε $L = F(a_1, \ldots a_n)$ με $a_i \in K$ και για αυτά τα a_i το λήμμα 11 μας λέει ότι υπάρχει $E \in \mathcal{I}$ με $a_i \in E$ για κάθε i και συνεπώς $L \subseteq E$. Έστω τώρα $N = Gal(K/E)$ τότε:

$$L \subseteq H \implies Gal(K/L) \geq Gal(K/H)$$

δηλαδή $N \leq H$ και $|G : H| \leq |G : N| < \infty$.

Από το λήμμα 12 έχουμε ότι $G/N \cong Gal(E/F)$ μέσω της απεικόνισης $\sigma N \mapsto \sigma|_E$. Επομένως,

η ομάδα πηλίκο H/N απεικονίζεται στο $\{p|_E : p \in H\} = H_0$, το οποίο είναι υποομάδα της $Gal(E/F)$ και έχουμε δείξει προηγουμένως ότι αυτό έχει σταθερό σώμα $L \cap E = L$. Από το θεμελιώδες θεώρημα για πεπερασμένες επεκτάσεις έχουμε ότι $|H_0| = [E : L]$. Από αυτό έπεται ότι:

$$|G : H| = |G/N : H/N| = \frac{|G/N|}{|H/N|} = \frac{[E : F]}{[E : L]} = [L : F]$$

Υποθέτουμε τώρα ότι η $H = Gal(K/L)$ είναι κανονική υποομάδα της G. Έστω $a \in L$ και $f(x) = Irr(a, F)$. Αν $b \in K$ είναι ρίζα του $f(x)$ τότε από το θεώρημα επέκτασης ισομορφισμών υπάρχει $\sigma \in G$ με $\sigma(a) = b$. Θα δείξουμε ότι $b \in L$. Έστω $\tau \in H$, τότε:

$$\tau(b) = \sigma^{-1}(\sigma\tau\sigma^{-1}(a)) = \sigma^{-1}(a) = b$$

εφόσον $H \trianglelefteq G$ και άρα $\sigma\tau\sigma^{-1} \in H$. Συνεπώς το b ανήκει στο σταθερό σώμα της H, δηλαδή στο L. Δείξαμε ότι το $f(x)$ διασπάται πλήρως στο L. Αυτό αποδεικνύει την κανονικότητα της επέκτασης L/F και η διαχωρισιμότητα της επέκτασης έπεται από την διαχωρισιμότητα της K/F. Άρα η επέκταση L/F είναι Galois.

Αντίστροφα, αν L/F Galois επέκταση τότε από υπενθύμιση έχουμε ότι:

$$\theta : G \longrightarrow Gal(L/F)$$

$$\sigma \longmapsto \sigma|_L$$

Το θ είναι καλά ορισμένος ομομορφισμός ομάδων με πυρήνα το $H = Gal(K/L)$ αφού αν

$$\theta(\sigma) = 1_L \implies \sigma|_L = 1_L \implies \sigma \in Gal(K/L)$$

συνεπώς έχουμε $H \trianglelefteq G$ ως πυρήνα ομομορφισμού. Επιπλέον ο θ είναι επί αφού αν έχουμε ένα τυχόν $\tau \in Gal(L/F)$ τότε το επεκτείνουμε μέσω του θεωρήματος επέκτασης ισομορφισμών σε $\tau' \in G$ και έτσι $\tau'|_L = \tau$. Από το πρώτο θεώρημα ισομορφισμών ομάδων έχουμε ότι $G/H \cong Gal(L/F)$.

Το τελευταίο βήμα της απόδειξης είναι να δείξουμε ότι ο ισομορφισμός αυτός είναι και ομοιομορφισμός, ωστόσο, η συνέχεια και η κλειστότητα διατηρούνται στην τοπολογία πηλίκο. Άρα αρκεί να δείξουμε ότι η θ είναι συνεχής και κλειστή. Τότε η επαγόμενη απεικόνιση:

$$\nu : G/H \longrightarrow Gal(L/F)$$

θα είναι ομοιμορφισμός.

Όμοια με την Galois επέκταση K/F, στην Galois επέκταση L/F τα βασικά ανοιχτά υποσύνολα της $Gal(L/F)$ είναι της μορφής $\rho Gal(L/E)$ για πεπερασμένες Galois επεκτάσεις E/F όπου $E \subseteq L$. Έστω $N = Gal(K/E) \in \mathcal{N}$. Το σύνολο $\theta^{-1}(Gal(L/E))$ περιέχει όλους τους ισομορφισμούς $\sigma \in G$ που αφού τους περιορίσουμε στο L μέσω της θ κρατάνε σταθερό το E, δηλαδή:

$$\theta^{-1}(Gal(L/E)) = N$$

όμοια:

$$\theta^{-1}(\rho Gal(L/E)) = \tau N$$

για κάθε $\tau \in G$ τέτοιο ώστε $\theta(\tau) = \tau|_L = \rho$.

Τα τN είναι βασικά ανοιχτά υποσύνολα του G, συνεπώς δείξαμε ότι η θ είναι συνεχής. Επιπλέον, η εικόνα μέσω συνεχούς απεικόνισης ενός συμπαγούς συνόλου παραμένει συμπαγές

σύνολο. Η G είναι συμπαγής και άρα είναι και η $Gal(L/F)$. Αντίστοιχα με την απόδειξη για την G, η $Gal(L/F)$ είναι Hausdorff και κάθε συμπαγές υποσύνολο χώρου Hausdorff είναι κλειστό. Δηλαδή, αν θεωρήσουμε ένα κλειστό υποσύνολο της G αυτό θα είναι συμπαγές και μέσω της θ θα απεικονίζεται σε κλειστό υποσύνολο της $Gal(L/F)$. Έτσι, δείξαμε ότι και η θ^{-1} είναι συνεχής και άρα ο ισομορφισμός που επάγεται από την θ είναι αμφισυνεχής όταν δωθεί η τοπολογία πηλίκο στο G/H. Δηλαδή, είναι και ομοιμορφισμός. □

Παράδειγμα 4. *έστω K/F πεπερασμένη Galois επέκταση. Τότε η Krull τοπολογία στο $Gal(K/F)$ είναι η διακριτή. Πράγματι αν $\sigma \in G$, έχουμε $K \in \mathcal{I}$ αφού $[K:F] < \infty$ και άρα το $\sigma N = \sigma Gal(K/K) = \sigma\{1_K\} = \{\sigma\}$ είναι ανοιχτή περιοχή του σ. Ετσι, κάθε υποομάδα $H \leq G$ είναι κλειστή και βρισκόμαστε ξανά στο αρχικό θεμελιώδες θεώρημα της θεωρίας Galois.*

Πριν δώσουμε δύο ακόμα παραδείγματα, το θεμελιώδες θεώρημα της άπειρης θεωρίας Galois μαζί με την υπενθύμιση μας δίνουν ένα 'όμορφο' αποτέλεσμα. Έστω $K/L/F$, όπου οι επεκτάσεις K/F και L/F είναι Galois. Αν $f(\sigma) = \sigma$ και $g(\sigma) = \sigma|_L$ τότε παρακάτω έχουμε μια βραχεία ακριβή ακολουθία ομάδων: (ή profinite τοπολογικών ομάδων με βάση το επόμενο κεφάλαιο.)

$$1 \longrightarrow Gal(K/L) \xrightarrow{f} Gal(K/F) \xrightarrow{g} Gal(L/F) \longrightarrow 1$$

Παράδειγμα 5. *Έστω $K = \mathbb{Q}(\zeta_{2^\infty}) = \cup_n \mathbb{Q}(\zeta_{2^n})$ και $K_n = \mathbb{Q}(\zeta_{2^n})$. Έχουμε ότι:*

$$Gal(K_n, \mathbb{Q}) \cong (\mathbb{Z}/2^n\mathbb{Z})^*$$

$$\sigma_a(\zeta_{2^n}) = \zeta_{2^n}^a$$

για τα αντιστρέψιμα a $(mod 2^n)$.

Θεωρούμε τις κυκλικές υποομάδες $H = (\sigma_5)$ και $H' = (\sigma_{13})$ της $Gal(K/\mathbb{Q})$. Έχουμε ότι $H \neq H'$, διαφορετικά αν απεικονίζαμε έναν γεννήτορα της μιας ομάδας σε έναν γεννήτορα της άλλης θα είχαμε $\zeta_{2^n}^5 = \zeta_{2^n}^{13^k}$ το οποίο είναι ισοδύναμο με το άτοπο $5 = 13^k \quad (mod 2^n)$ για κάθε φυσικό n και σταθερό k. Ωστόσο, θα δείξουμε ότι ισχύει $K^H = K^{H'}$! Θεωρούμε επίσης H_n, H'_n τις κυκλικές υποομάδες $(\sigma_5|_{K_n})$ και $(\sigma_{13}|_{K_n})$ της $Gal(K_n/\mathbb{Q})$. Αυτές είναι ισόμορφες καθώς $< 5 \quad mod 2^n >=< 13 \quad mod 2^n >$ για κάθε $n \geq 2$. Καθώς $13, 5 = 1 \quad (mod 4)$ έχουμε ότι τα σ_5, σ_{13} κρατάνε σταθερό το i, δηλαδή $\mathbb{Q}(i) \subseteq K_n^{H_n}, K_n^{H'_n}$. Από πεπερασμένη αντιστοιχία Galois έχουμε ότι $K_n^{H_n} = \mathbb{Q}(i) = K_n^{H'_n}$. Αυτό είναι για τυχόν $n \in \mathbb{N}$. Συνεπώς, παρόλο που $H \neq H'$ ισχύει ότι:

$$K^H = \{a \in K : \quad \sigma(a) = a \quad \forall \sigma \in H\} = \cup_n \{a \in K : \sigma|_{K_n}(a) = a \quad \forall \sigma \in H_n\} =$$

$$\cup_n K_n^{H_n} = \cup_n \mathbb{Q}(i) = \cup_n K_n^{H'_n} = K^{H'}$$

Παράδειγμα 6. *Αν θεωρήσουμε την Galois επέκταση $\mathbb{Q}(i, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \ldots)$ του $\mathbb{Q}$ τότε επειδή οι αυτομορφισμοί του θα απεικονίζουν κάθε $\sqrt{p}$ (ή το i) στα $\pm\sqrt{p}$ (ή $\pm i$) έχουμε ότι:*

$$G \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$$

Αυτή η ομάδα έχει υπεραριθμήσιμες υποομάδες με δείκτη 2, ενώ οι επεκτάσεις διάστασης 2 του $\mathbb{Q}$ είναι αριθμήσιμες.

Πράγματι, κάθε επέκταση διάστασης 2 του $\mathbb{Q}$ θα είναι μια επισύναψη του $\sqrt{q}$ για κάθε $q \in \mathbb{Q}$

(με την σύμβαση ότι για $a > 0, \sqrt{-a} = i\sqrt{a}$) όπου το $|q|$ δεν είναι τέλειο τετράγωνο. Δηλαδή, έχουμε αριθμήσιμες επιλογές για τις επεκτάσεις διάστασης 2.

Για το άλλο επιχείρημα, μπορούμε να δούμε την ομάδα G ως έναν διανυσματικό χώρο υπεράνω του $\mathbb{Z}/2\mathbb{Z}$ άπειρης αριθμήσιμης διάστασης και να θεωρήσουμε τον δυϊκό χώρο:

$$G^* = \{\phi : G \to \mathbb{Z}/2\mathbb{Z} | \quad \phi \text{ γραμμική απεικόνιση } \}$$

Ένα γνωστό θεώρημα της συναρτησιακής ανάλυσης μας λέει ότι κάθε διανυσματικός χώρος έχει Hamel βάση. Αν θεωρήσουμε μια Hamel βάση $\{e_n\}_{n\in\mathbb{N}}$ του διανυσματικού χώρου του G υπεράνω του $\mathbb{Z}/2\mathbb{Z}$, τότε ένα τυχόν στοιχείο του χώρου γράφεται ως:

$$x = \sum_{n=1}^{\infty} \lambda_n e_n$$

με $\lambda_n \in \mathbb{Z}/2\mathbb{Z}$. Αν θεωρήσουμε και μια απεικόνιση $\phi \in G^*$ τότε:

$$\phi(x) = \sum_{n=0}^{\infty} \lambda_n \phi(e_n)$$

δηλαδή η ϕ καθορίζεται πλήρως σαν απεικόνιση από τις επιλογές $\phi(e_n) \in \mathbb{Z}/2\mathbb{Z}$. Με άλλα λόγια ο χώρος G^* έχει την ίδια πληθικότητα με το σύνολο $\{0,1\}^{\mathbb{N}}$, δηλαδή άπειρη υπεραριθμήσιμη.

Από αυτό έπεται ότι και ο υπόχωρος $\{ker\phi : \phi \in G^*\}$ θα είναι υπεραριθμήσιμος. Πράγματι, για κάθε $x \in G, \phi \in G^*$ έχουμε $\phi(x) = 0$ ή 1 και άρα ο πυρήνας $ker\phi$ μας ορίζει μονοσήμαντα την ϕ για κάθε $x \in G$. Δηλαδή, αν ξέρουμε ποια x πάει η ϕ στο 0, ξέρουμε ακριβώς ότι τα $x \in G - ker\phi$ τα πάει στο 1. Με άλλα λόγια, μια επιλογή ενός συνόλου $ker\phi$ είναι μια επιλογή μιας ϕ και αντίστροφα. Έτσι καταλήγουμε στην υπεραριθμησιμότητα του υπόχωρου.

Η κάθε ϕ ως γραμμική είναι και ομομορφισμός ομάδων και έτσι χρησιμοποιώντας το 1ο θεώρημα ισομορφισμών ομάδων για τις ϕ, έχουμε υπεραριθμήσιμους πυρήνες, δηλαδή υπεραριθμήσιμες υποομάδες H τέτοιες ώστε:

$$|G : H| = |G : ker\phi| = |\mathbb{Z}/2\mathbb{Z}| = 2$$

Ουσιαστικά, οι υποομάδες της ομάδας Galois μιας άπειρης επέκτασης είναι `πάρα πολλές` σε σχέση με τις ενδιάμεσες πεπερασμένες επεκτάσεις. Για αυτό και αποτυγχάνει η αντιστοιχία Galois χωρίς τον περιορισμό της κλειστότητας των υποομάδων.

4 Περαιτέρω Μελέτη

Στην προσπάθεια να γενικεύσει κανείς τα προηγούμενα επιχειρήματα μπορεί να φτάσει στους ακόλουθους ορισμούς:

Ορισμός. *Τοπολογική ομάδα G είναι ένας τοπολογικός χώρος $(G, \mathcal{T})$ όπου η G είναι ομάδα με τις ιδιότητες ότι η απεικόνιση πολλαπλασιασμού $(a, b) \mapsto ab$ και η αντιστροφή $a \mapsto a^{-1}$ είναι συνεχείς. Αντίστοιχα ζητάμε οι ομομορφισμοί μεταξύ των ομάδων να είναι και συνεχείς για να τους λέμε ομομορφισμούς τοπολογικών ομάδων.*

Όπως κάναμε και πριν δηλαδή που απαιτούσαμε ο ισομορφισμός ομάδων που προέκυπτε να είναι και ομοιομορφισμός.

Ορισμός. *Αν $\Lambda \neq \varnothing$ ένα σύνολο και $\leq$ είναι μια διμελής σχέση στο $\Lambda \times \Lambda$ τότε το $(\Lambda, \leq)$ λέγεται κατευθυνόμενο σύνολο αν ικανοποιούνται οι δύο σχέσεις της προδιάταξης:*
1) *Αυτοπαθής $\lambda \leq \lambda \quad \forall \lambda \in \Lambda$*
2) *Μεταβατική $\lambda_1 \leq \lambda_2$ και $\lambda_2 \leq \lambda_3 \implies \lambda_1$*
μαζί με την :
3) *Για κάθε $\lambda_1, \lambda_2 \in \Lambda$ υπάρχει $\lambda_3 \in \Lambda$ τέτοιο ώστε $\lambda_1, \lambda_2 \leq \lambda_3$.*

Για παράδειγμα, αν σκεφτόμαστε υποσύνολα A, B ενός μη κενού συνόλου X τότε η σχέση $A \leq B \iff A \supseteq B$ καθιστά το X κατευθυνόμενο εφόσον $A, B \leq A \cap B$.

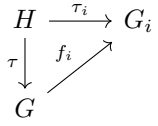
Στην συνέχεια, τα επόμενα είναι συνήθως ορισμένα στην θεωρία των κατηγοριών αλλά εδώ θα τα ορίσουμε περιορισμένοι στις ομάδες.

Ορισμός (Inverse System)**.** *Ένα αντίστροφο σύστημα αποτελείται από ένα κατευθυνόμενο σύνολο $(J, \leq)$ και μια συλλογή πεπερασμένων ομάδων $\mathcal{G} = \{G_i : i \in J\}$ οι οποίες είναι τοπολογικές ομάδες εφοδιασμένες με την διακριτή τοπολογία. Επιπλέον απαιτούμε και μια συλλογή ομομορφισμών $\{f_i^j : G_j \to G_i | i, j \in J \quad \forall i \leq j\}$ οι οποίοι ικανοποιούν τις εξής σχέσεις:*

$$f_i^i = id(G_i)$$
$$f_i^j \circ f_j^k = f_i^k$$

Ορισμός (Inverse Limit)**.** *Αντίστροφο όριο ενός συστήματος όπως παραπάνω θα λέμε μια ομάδα G μαζί με τους ομομορφισμούς $f_i : G \to G_i$ που ικανοποιούν $f_i^j \circ f_j = f_i$ για κάθε ζεύγος $i \leq j$, εφόσον η ομάδα G ικανοποιεί την παρακάτω καθολική ιδιότητα:*

Αν H είναι μια ομάδα μαζί με ομομορφισμούς $\tau_i : H \to G_i$ που ικανοποιούν $f_i^j \circ \tau_j = \tau_i$ για κάθε ζεύγος $i \leq j$ τότε υπάρχει μοναδικός ομομορφισμός $\tau : H \to G$ με $\tau_i = f_i \circ \tau$ για κάθε i. Δηλαδή το παρακάτω διάγραμμα μετατίθεται:



Έτσι μπορεί να δειχθεί ότι το αντίστροφο όριο ενός συστήματος υπάρχει, είναι μοναδικό ως προς ισομορφισμό και είναι το

$$\varprojlim G_i = \{(g_i)_{i \in J} \in \prod_{i \in J} G_i : \quad f_i^j(g_j) = g_i \quad \forall i \leq j\}$$

Σαν ομάδα, το αντίστροφο όριο είναι υποομάδα της $\prod G_i$ και είναι τοπολογική ομάδα που παίρνει την επαγόμενη τοπολογία περιορισμό, εφόσον στην $\prod G_i$ δίνεται η τοπολογία γινόμενο.

Στην συνέχεια θα δώσουμε έναν τελευταίο ορισμό που θα δέσει με το προηγούμενο κεφάλαιο:

Ορισμός (Profinite)**.** *Μια τοπολογική ομάδα λέγεται profinite (projective + finite) αν είναι ισόμορφη με το αντίστροφο όριο ενός αντιστρόφου συστήματος πεπερασμένων ομάδων.*

Τα αποτελέσματα του προηγούμενο κεφαλαίου θα μπορούσαν να παραπέμψουν κάποιον ότι ένας ισοδύναμος ορισμός είναι ακριβώς η τοπολογική ομάδα να έχει τις ιδιότητες: συμπάγεια, Hausdorff και totally disconnected.

Έτσι, ένα παράδειγμα χωρίς ιδιαίτερο ενδιαφέρον είναι ότι κάθε πεπερασμένη ομάδα μαζί με την διακριτή τοπολογία είναι profinite.

Το παράδειγμα που μας ενδιαφέρει είναι ότι για κάθε άπειρη επέκταση Galois, η ομάδα Galois που προκύπτει είναι profinite. Αν ακολουθήσουμε τους ορισμούς του προηγούμενο κεφαλαίου και θεωρήσουμε την συλλογή πεπερασμένων ομάδων με την διακριτή τοπολογία:

$$\{G/N : \quad N \in \mathcal{N}\}$$

και ως ομομορφισμούς:

$$f_i^j : G/N_i \longrightarrow G/N_j$$

τις κανονικές προβολές, όπου $N_i \geq N_j \iff N_i \subseteq N_j$ δηλαδή τις απεικονίσεις:

$$G/Gal(K/E_i) \cong Gal(E_i/F) \longrightarrow Gal(E_j/F) \cong G/Gal(K/E_j)$$
$$\sigma \longmapsto \sigma|_{E_j}$$

τότε τα παραπάνω αποτελούν αντίστροφο σύστημα και μάλιστα έχουμε τον ομοιομορφισμό:

$$G \cong \varprojlim G/N$$

δηλαδή, η τοπολογία που προκύπτει στο αντίστροφο όριο ως τοπολογία περιορισμός δεν είναι άλλη από την τοπολογία Krull.
Αξίζει να αναφερθούμε και σε ένα αποτέλεσμα που βλέπει τα πράγματα από αντίθετη σκοπιά, το οποίο είναι ότι κάθε profinite ομάδα είναι ομάδα Galois για κάποια επέκταση σωμάτων. (βλέπε Profinite groups are Galois groups, William C. Waterhouse, 1974)

Ένα άλλο παράδειγμα άξιο μελέτης είναι ο ορισμός της προσθετικής ομάδας των p-adic ακεραίων. Είναι η προφινιτε ομάδα $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ όπου το n διατρέχει τους φυσικούς μαζί με τις φυσικές απεικονίσεις $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ για όλα τα $n \geq m$. Αναμενόμενο είναι και η τοπολογία που προκύπτει στο αντίστροφο όριονα ταυτίζεται με την τοπολογία που έχουν οι p-adic ακέραιοι μέσω του συνήθους ορισμού τους από την ανάλυση.

Αναφορές

[1] Patrick Morandi. *Fields and Galois Theory.* Springer-Verlag, New York, 1996.

[2] James S. Milne. *Fields and Galois Theory.* Available at www.jmilne.org/math/, 2020.

[3] Frederick Butler. *Infinite Galois Theory, Master Thesis, University of Pennsylvania, 2001.*