Θέματα Άλγεβρας και Γεωμετρίας Ι

Άπειρη Θεωρία Galois.

Ονομ/νο: Νούλας Δημήτριος
ΑΜ:
email:

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. □

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. □

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. □

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. □

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

Απόδειξη. □

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

Απόδειξη. □

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. □

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* $Irr(a, F) = Irr(\tau(a), F)$.

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

Απόδειξη. □

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. □

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. □

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

Απόδειξη. □

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

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. □

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. □

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

Απόδειξη. □

Ορισμός. *Έστω K/F και $f(x) \in F[x]$. Λέμε ότι το f διασπάται πλήρως στο K αν υπάρχουν $a_1, \dots a_n \in K$ 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 $K = F(a_1, \dots, a_n)$ όπου $a_1, \dots, a_n$ 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 $X = \{f_1, \dots f_n\}$ ουσιαστικά μιλάμε για το σώμα ριζών του πολυωνύμου $f = f_1 \cdots f_n$.

Θεώρημα 3 (Ύπαρξη ρίζας σε επέκταση)**.**

Απόδειξη. □

Θεώρημα 4 (Ύπαρξη σώματος ριζών για πεπερασμένα πολυώνυμα)**.**

Απόδειξη. □

Λήμμα 5. *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.*

Απόδειξη. □

Ορισμός. *Αν κάποιο K ικανοποιεί κάποια από τις συνθήκες του λήμματος 5 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 6. *Αν K/F αλγεβρική επέκταση, τότε $|K| \leq max\{|F|, |\mathbb{N}|\}$.*

Απόδειξη. □

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

Απόδειξη. □

Πόρισμα 6 (Υπαρξη σώματος ριζών)**.**

Λήμμα 7. *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. □

Λήμμα 8. *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. □

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. □

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. □

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. □

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. □

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. 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. □

1.3 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 9. *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. □

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. □

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. □

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. □

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.*

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 9, 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 $G = Gal(K/E)$. 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 $Gal(L/F) \cong G/H$.*

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:

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

□

2 Γενική Τοπολογία

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 10. *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. Εφόσον κάθε a_i είναι διαχωρίσιμο (!!!) υπεράνω του F τότε 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 11. *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 12. $\bigcap_{N \in \mathcal{N}} N = \{1_G\} = \{id : K \mapsto K\}$. *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 10 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 13. *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,

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

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

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 13.

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

Απόδειξη. Έστω $\sigma, \tau \in G, \sigma \neq \tau$. Από το λήμμα 12 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 12. *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 13. *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 11) 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 12. 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, $\sigma \in G, H \in N$ 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 $\sigma^{-1}\tau$ 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 11. 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 (17.1) , 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 $x \in F$ στο αρχικό υπόσωμα που έχουμε θεωρήσει στην αρχή του κεφαλάιου, 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 K -ισομορφισμός που κρατάει σταθερό το F και σε αυτή την περίπτωση 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 $p \in P \backslash C$ 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 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 Γαλοις για την πεπερασμένη $Gal(E/F)$ έχουμε $H_0 = Gal(E/(E \cap F^H))$. (αντιστοιχία σχήμα 1-H_0 - $Gal(E/F)$ μέσω της $Gal(E, \_)$ στον πύργο E - $F^{H_0} - F$)

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 Γαλοις επέκταση και $G = Gal(K/F)$. Με την Κρυλλ 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 $K/L/F$ (αντιστοχία σχήμα, προσοχή, να δώ μαλιάκα σημ για να μην μπερδευτώ) (γραφή όπως στο μεμορια)

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 Γαλοις. Όταν αυτό συμβαίνει έχουμε τον ισομορφισμό ομάδων $Gal(L/F) \cong G/N$. Αν εμπλουτίσουμε την ομάδα πηλίκο $Γ/N$ με την τοπολογία πηλίκο, τότε αυτός ο ισομορφισμός είναι και ομοιομορφισμός.

Απόδειξη. (να κάνω ενυμερατιον)

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 Γαλοις 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 έχουμε:

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

και άρα $[L : F] < \infty$.

Για την τελευταία κατεύθυνση, αν $[L : F] < \infty$ τότε $L = F(a_1, \dots a_n)$ με $a_i \in K$ και για αυτά τα a_i το λήμμα (17.1) 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 (17.2) 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 θεμελιώδης 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 (απόδειξη;). Άρα L/F Γαλοις επέκταση.

Αντίστροφα, αν L/F Γαλοις επέκταση τότε από υπενθύμιση (!!) έχουμε ότι

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

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

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 και τότε η επαγόμενη απεικόνιση:

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

θα είναι ομοιμορφισμός.

Όμοια με την Γαλοις επέκταση K/F , στην Γαλοις επέκταση L/F τα βασικά ανοιχτά υποσύνολα της $Gal(L/F)$ είναι της μορφής $\rho Gal(L/E)$ για πεπερασμένες Γαλοις 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 Ηαυσδορφφ και κάθε συμπαγές υποσύνολο χώρου Ηαυσδορφφ 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 και αμφισυνεχής όταν δωθεί η τοπολογία πηλίκο στο G/H, δηλαδή είναι και ομοιμορφισμός. □

Παράδειγμα 3. *έστω K/F πεπερασμένη Γαλοις επέκταση. Τότε η Κρυλλ 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 Γαλοις.*

Παράδειγμα 4. *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 $5 = 13^k \pmod{2^n}$ 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 $< 5 \mod 2^n >=< 13 \mod 2^n >$ για κάθε $n \geq 2$. Καθώς $13, 5 = 1 \pmod 4$ 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 5. *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. 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:*
ι) Αυτοπαθής $\lambda \leq \lambda \quad \forall \lambda \in \Lambda$ ιι) Μεταβατική $\lambda_1 \leq \lambda_2$ και $\lambda_2 \leq \lambda_3 \implies \lambda_1$
μαζί με την :
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: (διαγραμμα τικζσδ, τι ιμπορτ κανω;)

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 τοταλλψ δισχοννεχτεδ.

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 Γαλοις, η ομάδα γαλοις που προκύπτει είναι προφινιτε. 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 Κρυλλ.

Ένα άλλο παράδειγμα άξιο μελέτης είναι ο ορισμός της προσθετικής ομάδας των π-αδις 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 π-αδις 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.