Άπειρη Θεωρία Galois

Δημήτριος Νούλας

Δεκέμβρης 2020

Outline

1. Κλασική Θεωρία Galois
2. Άπειρη Θεωρία Galois
3. Μια κατηγορική οπτική

Σώμα ριζών

Ορισμός

Έστω μια επέκταση σωμάτων K/F *και* $f(x) \in F[x]$*. Τότε το* K *λέγεται σώμα ριζών του* $f(x)$ *υπεράνω του* F *αν* $K = F(a_1, \ldots, a_n)$ *και* $f(x) = a(x - a_1) \cdots (x - a_n) \in K[x]$

Σώμα ριζών

Ορισμός

Έστω μια επέκταση σωμάτων K/F και $f(x) \in F[x]$. Τότε το K λέγεται σώμα ριζών του $f(x)$ υπεράνω του F αν $K = F(a_1, \ldots, a_n)$ και $f(x) = a(x - a_1) \cdots (x - a_n) \in K[x]$

Για ένα σύνολο πολυωνύμων

Αν $S \subseteq F[x]$ τότε επεκτείνουμε τον ορισμό και λέμε ότι το K είναι σώμα ριζών του S αν καθένα από τα πολυώνυμα του S διασπάται πλήρως στο K και $K = F(X)$, όπου X το σύνολο ριζών των πολυωνύμων. Αν $S = \{f_1, f_2, \ldots f_n\}$ τότε το K είναι σώμα ριζών του $S \iff K$ σώμα ριζών του $f_1 f_2 \cdots f_n$.
Ύπαρξη; Αν το S είναι άπειρο;

Αλγεβρική Κλειστότητα

Ορισμός

Έστω επέκταση K/F, τότε ονομάζουμε αλγεβρική κλειστότητα του F στο K το σώμα $\overline{F} = \{a \in K : a$ αλγεβρικό υπεράνω του $F\}$

Αλγεβρική Κλειστότητα

Ορισμός

Έστω επέκταση K/F, τότε ονομάζουμε αλγεβρική κλειστότητα του F στο K το σώμα $\overline{F} = \{a \in K : a \text{ αλγεβρικό υπεράνω του } F\}$

Αλγεβρικά Κλειστό Σώμα

Ισοδύναμα, έχουμε ότι ένα σώμα K είναι αλγεβρικά κλειστό αν κάθε πολυώνυμο στο $K[x]$ έχει ρίζα στο K.

Αλγεβρική Κλειστότητα

Ορισμός

Έστω επέκταση K/F, τότε ονομάζουμε αλγεβρική κλειστότητα του F στο K το σώμα $\overline{F} = \{a \in K : a \text{ αλγεβρικό υπεράνω του } F\}$

Αλγεβρικά Κλειστό Σώμα

Ισοδύναμα, έχουμε ότι ένα σώμα K είναι αλγεβρικά κλειστό αν κάθε πολυώνυμο στο $K[x]$ έχει ρίζα στο K.

Θεώρημα

Κάθε σώμα F έχει αλγεβρική κλειστότητα. Έπεται ως πόρισμα η ύπαρξη σώματος ριζών ενός τυχαίου συνόλου πολυωνύμων $\subseteq F[x]$.

Θεώρημα Επέκτασης Ισομορφισμών

Θεώρημα

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 $\tau(a) = a'$.

Κανονική Επέκταση

Ορισμός

Έστω επέκταση K/F. Λέμε την επέκταση του F κανονική αν το K είναι σώμα ριζών ενός συνόλου πολυωνύμων με συντελεστές από το F.

Κανονική Επέκταση

Ορισμός

Έστω επέκταση K/F. Λέμε την επέκταση του F κανονική αν το K είναι σώμα ριζών ενός συνόλου πολυωνύμων με συντελεστές από το F.

Ισοδύναμος ορισμός

Στη βιβλιογραφία πολλές φορές ορίζεται και ως: Κάθε ανάγωγο πολυώνυμο του $F[x]$ που έχει ρίζα στο K διασπάται πλήρως στο K. Ο όρος κανονική επέκταση δεν είναι τυχαίος καθώς όπως θα δούμε η κανονικότητα της επέκτασης έχει να κάνει με την κανονικότητα υποομάδας.

Κανονική Επέκταση

Ορισμός

Αν K/F επέκταση τότε ορίζουμε την ομάδα Galois να είναι το σύνολο των αυτομορφισμών του K που κρατάνε σταθερό το F και την συμβολίζουμε με $Gal(K/F)$

Ένα σημαντικό αποτέλεσμα

Αν $K/L/F$ διαδοχικές επεκτάσεις και K/F κανονική τότε η απεικόνιση:

$$Gal(K/F) \longrightarrow Gal(L/F)$$

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

είναι επί.

Διαχωρίσιμη Επέκταση

Χρειαζόμαστε ακόμα μια έννοια για την αντιστοιχία Galois!

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.

Διαχωρίσιμη Επέκταση

Χρειαζόμαστε ακόμα μια έννοια για την αντιστοιχία Galois!

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.

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.

Διαχωρίσιμη Επέκταση

Παράδειγμα

Τα πολυώνυμα $x^2 - 2$ *και* $(x-1)^5$ *είναι διαχωρίσιμα υπεράνω του* $\mathbb{Q}$. *Γενικότερα κάθε επέκταση σώματος χαρακτηριστικής* 0 *είναι διαχωρίσιμη. Αν* F *σώμα χαρακτηριστικής* $p > 0$ *και* $a \notin F^p$ *τότε το* $x^p - a \in F[x]$ *δεν είναι διαχωρίσιμο.*

Επέκταση Galois

Ορισμός (Επέκταση Galois)

Για μια αλγεβρική επέκταση:
Διαχωρίσιμη + Κανονική := Galois !

Επέκταση Galois

Ορισμός (Επέκταση Galois)

Για μια αλγεβρική επέκταση:
Διαχωρίσιμη + Κανονική := Galois !

Ισοδύναμος ορισμός

Στην βιβλιογραφία ορίζεται και ως: μια αλγεβρική επέκταση K/F είναι Galois αν $F = F^{Gal(K/F)}$, όπου $F^H = \{a \in K : \sigma(a) = a \quad \forall \sigma \in H\}$ το σταθερό σώμα της υποομάδας $H \leq Gal(K/F)$. Αυτός ο ορισμός δείχνει και ποια θέλουμε να είναι η αντιστοιχία μεταξύ ενδιάμεσων σωμάτων και υποομάδων της ομάδας Galois. Επιπλέον, αν η επέκταση K/F είναι Galois και πεπερασμένη τότε παίρνουμε την ισότητα από την γενική σχέση: $|Gal(K/F)| \leq [K : F]$

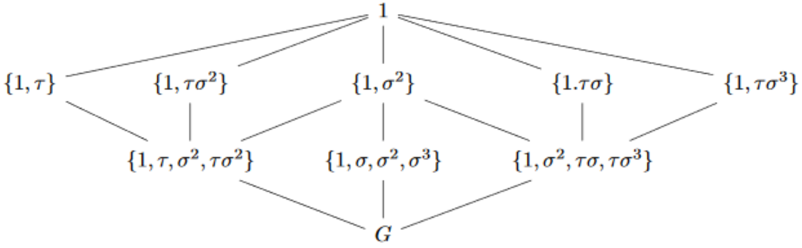
Θεμελιώδες Θεώρημα της Θεωρίας Galois

Θεώρημα

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 $Gal(L/F) \cong G/H$.

Θεμελιώδες Θεώρημα της Θεωρίας Galois

$$\begin{tikzcd}
K \arrow[d, dash] & & 1 \arrow[d, dash] \\
E \arrow[d, dash] \arrow[rr, "E \longmapsto Gal(K{,}E)"] & & Gal(K,E) \arrow[d, dash] \\
F & & G
\end{tikzcd}
\qquad
\begin{tikzcd}
1 \arrow[d, dash] & & K \arrow[d, dash] \\
H \arrow[d, dash] \arrow[rr, "F \longmapsto F^H"] & & F^H \arrow[d, dash] \\
G & & F
\end{tikzcd}$$


1
{1, τ}
{1, τσ²}
{1, σ²}
{1.τσ}
{1, τσ³}
{1, τ, σ², τσ²}
{1, σ, σ², σ³}
{1, σ², τσ, τσ³}
G

$$
\begin{tikzcd}
& & K \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\rho) \arrow[dr, dash] & \mathbb{Q}(i\rho) \arrow[d, dash] & \mathbb{Q}(\rho^2, i) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}((1-i)\rho) \arrow[d, dash] & \mathbb{Q}((1+i)\rho) \arrow[dl, dash] \\
& \mathbb{Q}(\rho^2) \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & \mathbb{Q}(i\rho^2) \arrow[dl, dash] & \\
& & F & &
\end{tikzcd}
$$

Outline

Ισχύει το ίδιο αν δεν υποθέσουμε ότι η Galois επέκταση K/F είναι πεπερασμένη;

Ισχύει το ίδιο αν δεν υποθέσουμε ότι η Galois επέκταση K/F είναι πεπερασμένη;

Η απάντηση είναι πως όχι! χρειαζόμαστε κάποιον περιορισμό...

Άπειρες επεκτάσεις Galois

Παράδειγμα

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

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

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

για τα αντιστρέψιμα $a \pmod{2^n}$. *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.

Συνέχεια παραδείγματος

Αν περιοριστούμε σε $H_n = (\sigma_5|_{K_n})$ και $H_n' = (\sigma_{13}|_{K_n})$ έχουμε ότι αυτές οι δύο ταυτίζονται ως υποομάδες της $Gal(K_n, \mathbb{Q})$. Εδώ η αντιστοιχία Galois για την πεπερασμένη επέκταση μας δίνει ότι $K_n^{H_n} = \mathbb{Q}(i) = K_n^{H_n'}$. Καθώς, ενώνουμε συνέχεια το σώμα $\mathbb{Q}(i)$ καταλήγουμε στο ότι $K^H = K^{H'}$, παρόλο που $H \neq H'$!

καταρρέει η αντιστοιχία...

Ένα δεύτερο παράδειγμα

Αν θεωρήσουμε την Galois επέκταση
$K = \mathbb{Q}(i, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \ldots)$ του $\mathbb{Q}$ τότε:

$$Gal(K/\mathbb{Q}) \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$$

Ένα δεύτερο παράδειγμα

Αν θεωρήσουμε την Galois επέκταση
$K = \mathbb{Q}(i, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \ldots)$ του $\mathbb{Q}$ τότε:

$$Gal(K/\mathbb{Q}) \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$$

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, ώστε να δουλεύει η αντιστοιχία όπως πριν.

Μερικοί Συμβολισμοί

Έστω K/F Galois επέκταση, συμβολίζουμε:

$$G = Gal(K/F)$$

$$\mathcal{I} = \{E : K/E/F, \quad [E:F] < \infty, \quad E/F \quad \text{Galois}\ \}$$

$$\mathcal{N} = \{N \subseteq G : N = Gal(K/E) \quad \text{για κάποιο } E \in \mathcal{I}\}$$

Λήμμα

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

Λήμμα

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

Λήμμα

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* $|G/N| = |Gal(E/F)| = [E : F] < \infty$.

Λήμμα

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

Λήμμα

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* $|G/N| = |Gal(E/F)| = [E : F] < \infty$.

Λήμμα

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

Λήμμα

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

Τοπολογία Krull

Ορισμός (Τοπολογία Krull)

Το $(G, \mathcal{T})$ 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 $N_i \in \mathcal{N}$.

Ιδιότητες της τοπολογίας Krull

Το σύνολο $\{\sigma N : \quad \sigma \in G, N \in \mathcal{N}\}$ είναι βάση της τοπολογίας.

Ιδιότητες της τοπολογίας Krull

Το σύνολο $\{\sigma N : \quad \sigma \in G, N \in \mathcal{N}\}$ είναι βάση της τοπολογίας.

Έστω $N \in \mathcal{N}$, τότε $[G : N] < \infty$ και το σN είναι κλειστό ώς πεπερασμένη ένωση συμπλόκων. Άρα η τοπολογία έχει βάση από ανοιχτά κλειστά.

Ιδιότητες της τοπολογίας Krull

Πρόταση

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

Ιδιότητες της τοπολογίας Krull

Πρόταση

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

Απόδειξη

Έστω $\sigma, \tau \in G, \sigma \neq \tau$.

$$\{\sigma\} = \bigcap_{N} \sigma N$$

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

Ιδιότητες της τοπολογίας Krull

Πρόταση

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

Ιδιότητες της τοπολογίας Krull

Πρόταση

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.

Ιδιότητες της τοπολογίας Krull

Πρόταση

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

Ιδιότητες της τοπολογίας Krull

Πρόταση

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

Ιδέα

Δείχνουμε ότι η ομάδα G είναι ισόμορφη και ταυτόχρονα, με την ίδια απεικόνιση, ομοιομορφική με το ευθύ γινόμενο:

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

Τις ομάδες G/N τις εμπλουτίζουμε με την διακριτή τοπολογία και το P παίρνει την τοπολογία γινόμενο. Επίσης το P είναι χώρος Hausdorff και επικαλούμενοι το θεώρημα Tychonoff είναι και συμπαγής.

Θεώρημα

Ο τοπολογικός χώρος $(G, \mathcal{T})$ *είναι συμπαγής, Hausdorff και totally disconnected.*

Θεώρημα

Ο τοπολογικός χώρος $(G, \mathcal{T})$ είναι συμπαγής, Hausdorff και totally disconnected.

το επόμενο θεώρημα θα 'διορθώσει' την αντιστοιχία:

Θεώρημα

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.

Ψάχνοντας πηγές ανακαλύπτει κανείς νέες αποδεικτικές μεθόδους:

Proposition 3.5. *Let* $G = \mathrm{Gal}(\Omega/F)$, *and let* $H \subset G$ *be a subgroup. Then* $\mathrm{Gal}(\Omega/\Omega^H)$ *is the closure of* H.

Proof. I don't understand this proof well enough to give a succinct proof appropriate for a seminar. □

Θεμελιώδες Θεώρημα της Άπειρης Θεωρίας Galois

Θεώρημα

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. 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.

$$\begin{tikzcd}
K \arrow[d, dash] & & 1 \arrow[d, dash] \\
L \arrow[d, dash] \arrow[rr, "L \longmapsto Gal(K,L)"] & & Gal(K,L) \arrow[d, dash] \\
F & & G
\end{tikzcd}
\qquad
\begin{tikzcd}
1 \arrow[d, dash] & & K \arrow[d, dash] \\
H \arrow[d, dash] \arrow[rr, "F \longmapsto F^H"] & & F^H \arrow[d, dash] \\
G & & F
\end{tikzcd}$$

Γενίκευση

Έστω K/F πεπερασμένη Galois επέκταση. Τότε η Krull τοπολογία στο $Gal(K/F)$ είναι η διακριτή. Έτσι κάθε υποομάδα της $Gal(K/F)$ είναι κλειστή.

Γενίκευση

Έστω K/F πεπερασμένη Galois επέκταση. Τότε η Krull τοπολογία στο $Gal(K/F)$ είναι η διακριτή. Έτσι κάθε υποομάδα της $Gal(K/F)$ είναι κλειστή.

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.

Ένα όμορφο αποτέλεσμα

Έστω $K/L/F$ όπου οι επεκτάσεις K/F και L/F είναι Galois, τότε παρακάτω έχουμε μια βραχεία ακριβή ακολουθία ομάδων:

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

Outline

Τοπολογικές Ομάδες

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 συνεχείς για να τους λέμε ομομορφισμούς τοπολογικών ομάδων.

Κατευθυνόμενο Σύνολο

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* $\lambda_1, \lambda_2 \leq \lambda_3$.

Αντίστροφο Σύστημα

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:*

$$f_i^i = id(G_i)$$

$$f_i^j \circ f_j^k = f_i^k$$

Αντίστροφο Όριο

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:

Καθολική ιδιότητα αντιστρόφων ορίων

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:

$$\begin{tikzcd}
H \arrow[r, "\tau_i"] \arrow[d, "\tau"'] & G_i \\
G \arrow[ur, "f_i"] &
\end{tikzcd}$$

Αντίστροφο Όριο

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.

Profinite Ομάδες

Ορισμός (Profinite)

Μια τοπολογική ομάδα λέγεται αν είναι ισόμορφη με το αντίστροφο όριο ενός αντιστρόφου συστήματος πεπερασμένων ομάδων.

Profinite Ομάδες

Ορισμός (Profinite)

Μια τοπολογική ομάδα λέγεται αν είναι ισόμορφη με το αντίστροφο όριο ενός αντιστρόφου συστήματος πεπερασμένων ομάδων.

Ισοδύναμος ορισμός

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

Profinite Ομάδες

Ορισμός (Profinite)

Μια τοπολογική ομάδα λέγεται αν είναι ισόμορφη με το αντίστροφο όριο ενός αντιστρόφου συστήματος πεπερασμένων ομάδων.

Ισοδύναμος ορισμός

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

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

Profinite Ομάδες

Το παράδειγμα που μας ενδιαφέρει είναι ότι για κάθε άπειρη επέκταση Galois, η ομάδα Galois που προκύπτει είναι profinite. Με τους προηγούμενους ορισμούς, αν 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:

$$G/Gal(K/E_i) \cong Gal(E_i/F) \longrightarrow Gal(E_j/F) \cong G/Gal(K/E_j)$$

$$\sigma \longmapsto \sigma\big|_{E_j}$$

Τότε τα παραπάνω αποτελούν αντίστροφο σύστημα και μάλιστα έχουμε τον ομοιομορφισμό τοπολογικών ομάδων:

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

δηλαδή, η τοπολογία που προκύπτει στο αντίστροφο όριο ως τοπολογία περιορισμός δεν είναι άλλη από την τοπολογία Krull.

...ή μάλλον βραχεία ακριβής ακολουθία profinite τοπολογικών ομάδων!

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

Κάπου εδώ ένας αγαπημένος καθηγητής μας θα ρώταγε:

Ισχύει το αντίστροφο;

Κάπου εδώ ένας αγαπημένος καθηγητής μας θα ρώταγε:

Ισχύει το αντίστροφο;

PROFINITE GROUPS ARE GALOIS GROUPS

WILLIAM C. WATERHOUSE

ABSTRACT. Artin's theorem on finite automorphism groups of fields extends to profinite groups, and hence every profinite group is a galois group.

Σε προηγούμενο παράδειγμα είδαμε ότι αν $K = \mathbb{Q}(i, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \dots)$ τότε:

$$Gal(K/\mathbb{Q}) \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$$

Τα ενδιάμεσα σώματα του K θα είναι της μορφής: $E = \mathbb{Q}(\sqrt{p_1}, \dots \sqrt{p_n})$ και έτσι αν πάρουμε $\leq \iff \subseteq$

$$E_1 = \mathbb{Q}(\sqrt{p_1}, \dots \sqrt{p_n}) \leq E_2 = \mathbb{Q}(\sqrt{p_1}, \dots \sqrt{p_n}, \sqrt{q_1}, \dots, \sqrt{p_n})$$

με τις απεικονίσεις $Gal(E_2/\mathbb{Q}) \to Gal(E_1/\mathbb{Q})$ με κανόνα τον περιορισμό $\sigma \mapsto \sigma|_{E_1}$ τότε οι παραπάνω ομάδες είναι ισόμορφες με το αντίστροφο όριο για το σύστημα που μόλις ορίσαμε.

$$\varprojlim_{p \text{ prime}} Gal(\mathbb{Q}(\sqrt{p})/\mathbb{Q})$$

P-adic Numbers

Ο ορισμός της προσθετικής ομάδας των p-adic ακεραίων είναι η profinite 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 $n \geq m$.

Η τοπολογία που προκύπτει στο αντίστροφο όριο ταυτίζεται με την τοπολογία που έχουν οι p-adic ακέραιοι μέσω του συνήθους ορισμού τους από την ανάλυση.

Βιβλιογραφία

- Patrick Morandi. *Fields and Galois Theory.* Springer-Verlag, New York, 1996.
- James S. Milne. *Fields and Galois Theory.* Available at www.jmilne.org/math/, 2020.
- Frederick Butler. *Infinite Galois Theory, Master Thesis, University of Pennsylvania, 2001*