Corrispondenza di Galois per estensioni di grado infinito

Candidato
Giovanni Tognolini

Relatore
Prof. Andrea Caranti

Università di Trento

16 Luglio 2018

Indice

Definizione

Sia E/F un'estensione di campi. Denotiamo con

$$\mathrm{Gal}(E/F) := \{f : E \to E \text{ automorfismi} \mid f_{|F} = id_F\}.$$

L'estensione E/F è detta di Galois se

$$E^{\mathrm{Gal}(E/F)} := \{\alpha \in E \mid f(\alpha) = \alpha \text{ per ogni } f \in \mathrm{Gal}(E/F)\} = F.$$

Teoria di Galois: separabilità e normalità

Definizione

Sia E/F un'estensione di campi. Denotiamo con

$$\mathrm{Gal}(E/F) := \{f : E \to E \text{ automorfismi} \mid f_{|F} = id_F\}.$$

L'estensione E/F è detta di Galois se

$$E^{\mathrm{Gal}(E/F)} := \{\alpha \in E \mid f(\alpha) = \alpha \text{ per ogni } f \in \mathrm{Gal}(E/F)\} = F.$$

Proposizione

Sia E/F un'estensione *finita* di campi. Sono equivalenti

1. E/F è di Galois;
2. E/F è un'estensione normale e separabile;
3. E è il campo di spezzamento di un polinomio separabile a coefficienti in F.

Teoria di Galois: separabilità e normalità

Definizione

Sia E/F un'estensione di campi. Denotiamo con

$$\mathrm{Gal}(E/F) := \{f : E \to E \text{ automorfismi} \mid f_{|F} = id_F\}.$$

L'estensione E/F è detta di Galois se

$$E^{\mathrm{Gal}(E/F)} := \{\alpha \in E \mid f(\alpha) = \alpha \text{ per ogni } f \in \mathrm{Gal}(E/F)\} = F.$$

Proposizione

Sia E/F un'estensione di campi. Sono equivalenti

1. E/F è di Galois;
2. E/F è un'estensione normale e separabile;
3. E è il campo di spezzamento di una famiglia di polinomi separabili a coefficienti in F.

Teoria di Galois: Teorema Fondamentale

Teorema (Corrispondenza di Galois per estensioni di grado finito)

Sia E/F un'estensione di Galois finita e sia $G := \mathrm{Gal}(E/F)$. Allora le mappe

$$L \mapsto H := \mathrm{Gal}(E/L) \qquad e \qquad H \mapsto L := E^H$$

inducono una biiezione fra i sottocampi intermedi di E/F e i sottogruppi di G che rovescia le inclusioni. L'estensione L/F è di Galois se e solo se H è normale in G e in tal caso si ha $\mathrm{Gal}(L/F) \cong G/H$.

Teoria di Galois: Teorema Fondamentale

Teorema (Corrispondenza di Galois per estensioni di grado finito)

Sia E/F un'estensione di Galois finita e sia $G := \mathrm{Gal}(E/F)$. Allora le mappe

$$L \mapsto H := \mathrm{Gal}(E/L) \qquad e \qquad H \mapsto L := E^H$$

inducono una biiezione fra i sottocampi intermedi di E/F e i sottogruppi di G che rovescia le inclusioni. L'estensione L/F è di Galois se e solo se H è normale in G e in tal caso si ha $\mathrm{Gal}(L/F) \cong G/H$.

Gruppi topologici: risultati elementari

Definizione

Un gruppo topologico è una terna $(G, \cdot, \tau)$, dove $(G, \cdot)$ è un gruppo e τ è una topologia su G tale che renda continue le mappe

$$\begin{aligned} \varphi \colon (G, \tau) &\longrightarrow (G, \tau) \\ g &\longmapsto g^{-1} \end{aligned} \qquad \begin{aligned} \psi \colon (G \times G, \xi) &\longrightarrow (G, \tau) \\ (g_1, g_2) &\longmapsto g_1 g_2 \end{aligned} \tag{1}$$

dove abbiamo indicato con ξ la topologia prodotto su $G \times G$.

Proposizione

Sia $\{G_i, \cdot_i, \tau_i\}_{i \in I}$ una famiglia di gruppi topologici, allora lo spazio topologico $(\prod_i G_i, \cdot, \xi)$, dove $\cdot$ è l'operazione definita componente per componente, e ξ è la topologia prodotto, è un gruppo topologico.

Osservazione

Se H è un sottogruppo di G e H è munito della topologia indotta, allora H è un gruppo topologico.

Gruppi topologici: risultati elementari

Definizione

Un gruppo topologico è una terna $(G, \cdot, \tau)$, dove $(G, \cdot)$ è un gruppo e τ è una topologia su G tale che renda continue le mappe

$$\begin{aligned} \varphi\colon (G,\tau) &\longrightarrow (G,\tau) \\ g &\longmapsto g^{-1} \end{aligned} \qquad \begin{aligned} \psi\colon (G\times G,\xi) &\longrightarrow (G,\tau) \\ (g_1,g_2) &\longmapsto g_1 g_2 \end{aligned} \tag{1}$$

dove abbiamo indicato con ξ la topologia prodotto su $G \times G$.

Proposizione

Sia $\{G_i, \cdot_i, \tau_i\}_{i\in I}$ una famiglia di gruppi topologici, allora lo spazio topologico $(\prod_i G_i, \cdot, \xi)$, dove $\cdot$ è l'operazione definita componente per componente, e ξ è la topologia prodotto, è un gruppo topologico.

Osservazione

Se H è un sottogruppo di G e H è munito della topologia indotta, allora H è un gruppo topologico.

Gruppi topologici: risultati elementari

Definizione

Un gruppo topologico è una terna $(G, \cdot, \tau)$, dove $(G, \cdot)$ è un gruppo e τ è una topologia su G tale che renda continue le mappe

$$\begin{aligned} \varphi \colon (G,\tau) &\longrightarrow (G,\tau) \\ g &\longmapsto g^{-1} \end{aligned} \qquad \begin{aligned} \psi \colon (G\times G,\xi) &\longrightarrow (G,\tau) \\ (g_1,g_2) &\longmapsto g_1 g_2 \end{aligned} \tag{1}$$

dove abbiamo indicato con ξ la topologia prodotto su $G \times G$.

Proposizione

Sia $\{G_i, \cdot_i, \tau_i\}_{i\in I}$ una famiglia di gruppi topologici, allora lo spazio topologico $(\prod_i G_i, \cdot, \xi)$, dove $\cdot$ è l'operazione definita componente per componente, e ξ è la topologia prodotto, è un gruppo topologico.

Osservazione

Se H è un sottogruppo di G e H è munito della topologia indotta, allora H è un gruppo topologico.

Sistemi e limiti inversi

Definizione

Sia $(\Lambda, \leq)$ un insieme parzialmente ordinato; diremo che $(\Lambda, \leq)$ è diretto se per ogni $a, b \in \Lambda$ esiste $c \in \Lambda$ tale che $a \leq c$ e $b \leq c$.

Definizione (Sistema inverso)

Sia $(\Lambda, \leq)$ un insieme parzialmente ordinato diretto. Un sistema inverso di gruppi su Λ è una famiglia $\{G_a, \varphi_{ab}\}_{a \leq b}$, dove G_a è un gruppo per ogni a, e $\forall a \leq b$, $\varphi_{ab} : G_b \to G_a$ è un morfismo di gruppi tale che $\varphi_{aa} = id$ e il diagramma

$$\begin{array}{ccc} G_b & \xrightarrow{\varphi_{ab}} & G_a \\ {\scriptstyle \varphi_{bc}}\uparrow & \nearrow_{\varphi_{ac}} & \\ G_c & & \end{array}$$

commuta per ogni $a \leq b \leq c$.

Esempio

- Insieme parzialmento ordinato diretto: $(\mathbb{N}, R)$, dove $(m, n) \in R \Leftrightarrow m|n$;
- Insieme di gruppi indicizzati su $\mathbb{N}$: $\{\mathbb{Z}/n\mathbb{Z}\}_{n \in \mathbb{N}}$;
- Famiglia di morfismi: $\varphi_{mn} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ mappe di proiezione naturale;

Sistemi e limiti inversi

Definizione

Sia $(\Lambda, \leq)$ un insieme parzialmente ordinato; diremo che $(\Lambda, \leq)$ è diretto se per ogni $a, b \in \Lambda$ esiste $c \in \Lambda$ tale che $a \leq c$ e $b \leq c$.

Definizione (Sistema inverso)

Sia $(\Lambda, \leq)$ un insieme parzialmente ordinato diretto. Un sistema inverso di gruppi su Λ è una famiglia $\{G_a, \varphi_{ab}\}_{a \leq b}$, dove G_a è un gruppo per ogni a, e $\forall a \leq b$, $\varphi_{ab} : G_b \to G_a$ è un morfismo di gruppi tale che $\varphi_{aa} = id$ e il diagramma

$$\begin{array}{ccc} G_b & \xrightarrow{\varphi_{ab}} & G_a \\ {\scriptstyle \varphi_{bc}}\uparrow & \nearrow_{\varphi_{ac}} & \\ G_c & & \end{array}$$

commuta per ogni $a \leq b \leq c$.

Esempio

- Insieme parzialmento ordinato diretto: $(\mathbb{N}, R)$, dove $(m, n) \in R \Leftrightarrow m|n$;
- Insieme di gruppi indicizzati su $\mathbb{N}$: $\{\mathbb{Z}/n\mathbb{Z}\}_{n \in \mathbb{N}}$;
- Famiglia di morfismi: $\varphi_{mn} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ mappe di proiezione naturale;

Sistemi e limiti inversi

Definizione

Sia $(\Lambda, \leq)$ un insieme parzialmente ordinato; diremo che $(\Lambda, \leq)$ è diretto se per ogni $a, b \in \Lambda$ esiste $c \in \Lambda$ tale che $a \leq c$ e $b \leq c$.

Definizione (Sistema inverso)

Sia $(\Lambda, \leq)$ un insieme parzialmente ordinato diretto. Un sistema inverso di gruppi su Λ è una famiglia $\{G_a, \varphi_{ab}\}_{a \leq b}$, dove G_a è un gruppo per ogni a, e $\forall a \leq b$, $\varphi_{ab} : G_b \to G_a$ è un morfismo di gruppi tale che $\varphi_{aa} = id$ e il diagramma

$$\begin{array}{ccc} G_b & \xrightarrow{\varphi_{ab}} & G_a \\ {\scriptstyle \varphi_{bc}}\uparrow & \nearrow_{\varphi_{ac}} & \\ G_c & & \end{array}$$

commuta per ogni $a \leq b \leq c$.

Esempio

- Insieme parzialmento ordinato diretto: $(\mathbb{N}, R)$, dove $(m, n) \in R \Leftrightarrow m|n$;
- Insieme di gruppi indicizzati su $\mathbb{N}$: $\{\mathbb{Z}/n\mathbb{Z}\}_{n \in \mathbb{N}}$;
- Famiglia di morfismi: $\varphi_{mn} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ mappe di proiezione naturale;

Sistemi e limiti inversi

Definizione

Sia $(\Lambda, \leq)$ un insieme parzialmente ordinato; diremo che $(\Lambda, \leq)$ è diretto se per ogni $a, b \in \Lambda$ esiste $c \in \Lambda$ tale che $a \leq c$ e $b \leq c$.

Definizione (Sistema inverso)

Sia $(\Lambda, \leq)$ un insieme parzialmente ordinato diretto. Un sistema inverso di gruppi su Λ è una famiglia $\{G_a, \varphi_{ab}\}_{a \leq b}$, dove G_a è un gruppo per ogni a, e $\forall a \leq b$, $\varphi_{ab} : G_b \to G_a$ è un morfismo di gruppi tale che $\varphi_{aa} = id$ e il diagramma

$$\begin{array}{ccc} G_b & \xrightarrow{\varphi_{ab}} & G_a \\ {\scriptstyle \varphi_{bc}}\uparrow & \nearrow_{\varphi_{ac}} & \\ G_c & & \end{array}$$

commuta per ogni $a \leq b \leq c$.

Esempio

- Insieme parzialmento ordinato diretto: $(\mathbb{N}, R)$, dove $(m, n) \in R \Leftrightarrow m|n$;
- Insieme di gruppi indicizzati su $\mathbb{N}$: $\{\mathbb{Z}/n\mathbb{Z}\}_{n \in \mathbb{N}}$;
- Famiglia di morfismi: $\varphi_{mn} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ mappe di proiezione naturale;

Sistemi e limiti inversi

Definizione

Sia $(\Lambda, \leq)$ un insieme parzialmente ordinato; diremo che $(\Lambda, \leq)$ è diretto se per ogni $a, b \in \Lambda$ esiste $c \in \Lambda$ tale che $a \leq c$ e $b \leq c$.

Definizione (Sistema inverso)

Sia $(\Lambda, \leq)$ un insieme parzialmente ordinato diretto. Un sistema inverso di gruppi su Λ è una famiglia $\{G_a, \varphi_{ab}\}_{a \leq b}$, dove G_a è un gruppo per ogni a, e $\forall a \leq b$, $\varphi_{ab} : G_b \to G_a$ è un morfismo di gruppi tale che $\varphi_{aa} = id$ e il diagramma

$$\begin{array}{ccc} G_b & \xrightarrow{\varphi_{ab}} & G_a \\ {\scriptstyle \varphi_{bc}}\uparrow & \nearrow_{\varphi_{ac}} & \\ G_c & & \end{array}$$

commuta per ogni $a \leq b \leq c$.

Esempio

- Insieme parzialmento ordinato diretto: $(\mathbb{N}, R)$, dove $(m, n) \in R \Leftrightarrow m|n$;
- Insieme di gruppi indicizzati su $\mathbb{N}$: $\{\mathbb{Z}/n\mathbb{Z}\}_{n \in \mathbb{N}}$;
- Famiglia di morfismi: $\varphi_{mn} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ mappe di proiezione naturale;

Sistemi e limiti inversi

Definizione

Sia $(\Lambda, \leq)$ un insieme parzialmente ordinato; diremo che $(\Lambda, \leq)$ è diretto se per ogni $a, b \in \Lambda$ esiste $c \in \Lambda$ tale che $a \leq c$ e $b \leq c$.

Definizione (Sistema inverso)

Sia $(\Lambda, \leq)$ un insieme parzialmente ordinato diretto. Un sistema inverso di gruppi su Λ è una famiglia $\{G_a, \varphi_{ab}\}_{a \leq b}$, dove G_a è un gruppo per ogni a, e $\forall a \leq b$, $\varphi_{ab} : G_b \to G_a$ è un morfismo di gruppi tale che $\varphi_{aa} = id$ e il diagramma

$$\begin{array}{ccc} G_b & \xrightarrow{\varphi_{ab}} & G_a \\ {\scriptstyle \varphi_{bc}}\uparrow & \nearrow_{\varphi_{ac}} & \\ G_c & & \end{array}$$

commuta per ogni $a \leq b \leq c$.

Esempio

- Insieme parzialmento ordinato diretto: $(\mathbb{N}, R)$, dove $(m, n) \in R \Leftrightarrow m|n$;
- Insieme di gruppi indicizzati su $\mathbb{N}$: $\{\mathbb{Z}/n\mathbb{Z}\}_{n \in \mathbb{N}}$;
- Famiglia di morfismi: $\varphi_{mn} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ mappe di proiezione naturale;

Sistemi e limiti inversi

Definizione (Limite inverso)

Un limite inverso del sistema inverso $\{G_a, \varphi_{ab}\}_{a \leq b}$ è definito come

$$\varprojlim_{a \in \Lambda} G_a := \left\{ (g_a)_{a \in \Lambda} \in \prod_{a \in \Lambda} G_a : g_a = \varphi_{ab}(g_b) \text{ per ogni } a \leq b \right\}.$$

Esempio

- Insieme parzialmento ordinato diretto: $(\mathbb{N}, \leq)$;
- Insieme di gruppi indicizzati su $\mathbb{N}$: $\{\mathbb{Z}/p^n\mathbb{Z}\}_{n \in \mathbb{N}}$;
- Famiglia di morfismi: $\varphi_{mn} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ mappe di proiezione naturale;

Tale struttura definisce un sistema inverso. Denotiamo il limite inverso associato con

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \left\{ (a_n) \in \prod \mathbb{Z}/p^n\mathbb{Z} \text{ coerenti} \right\}.$$

Un generico elemento di Z_p è della forma

$$\begin{array}{ccccccc} \mathbb{Z}/p\mathbb{Z} & \times & \mathbb{Z}/p^2\mathbb{Z} & \times & \mathbb{Z}/p^3\mathbb{Z} & \times & \cdots \\ a_0 & & a_0 + pa_1 & & a_0 + pa_1 + p^2 a_2 & & \cdots \end{array}$$

Sistemi e limiti inversi

Definizione (Limite inverso)

Un limite inverso del sistema inverso $\{G_a, \varphi_{ab}\}_{a \leq b}$ è definito come

$$\varprojlim_{a \in \Lambda} G_a := \left\{ (g_a)_{a \in \Lambda} \in \prod_{a \in \Lambda} G_a : g_a = \varphi_{ab}(g_b) \text{ per ogni } a \leq b \right\}.$$

Esempio

- Insieme parzialmento ordinato diretto: $(\mathbb{N}, \leq)$;
- Insieme di gruppi indicizzati su $\mathbb{N}$: $\{\mathbb{Z}/p^n\mathbb{Z}\}_{n \in \mathbb{N}}$;
- Famiglia di morfismi: $\varphi_{mn} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ mappe di proiezione naturale;

Tale struttura definisce un sistema inverso. Denotiamo il limite inverso associato con

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \left\{ (a_n) \in \prod \mathbb{Z}/p^n\mathbb{Z} \text{ coerenti} \right\}.$$

Un generico elemento di Z_p è della forma

$$\begin{array}{ccccccc} \mathbb{Z}/p\mathbb{Z} & \times & \mathbb{Z}/p^2\mathbb{Z} & \times & \mathbb{Z}/p^3\mathbb{Z} & \times & \cdots \\ a_0 & & a_0 + pa_1 & & a_0 + pa_1 + p^2 a_2 & & \cdots \end{array}$$

Sistemi e limiti inversi

Definizione (Limite inverso)

Un limite inverso del sistema inverso $\{G_a, \varphi_{ab}\}_{a \leq b}$ è definito come

$$\varprojlim_{a \in \Lambda} G_a := \left\{ (g_a)_{a \in \Lambda} \in \prod_{a \in \Lambda} G_a : g_a = \varphi_{ab}(g_b) \text{ per ogni } a \leq b \right\}.$$

Esempio

- Insieme parzialmento ordinato diretto: $(\mathbb{N}, \leq)$;
- Insieme di gruppi indicizzati su $\mathbb{N}$: $\{\mathbb{Z}/p^n\mathbb{Z}\}_{n \in \mathbb{N}}$;
- Famiglia di morfismi: $\varphi_{mn} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ mappe di proiezione naturale;

Tale struttura definisce un sistema inverso. Denotiamo il limite inverso associato con

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \left\{ (a_n) \in \prod \mathbb{Z}/p^n\mathbb{Z} \text{ coerenti} \right\}.$$

Un generico elemento di Z_p è della forma

$$\begin{array}{ccccccc} \mathbb{Z}/p\mathbb{Z} & \times & \mathbb{Z}/p^2\mathbb{Z} & \times & \mathbb{Z}/p^3\mathbb{Z} & \times & \cdots \\ a_0 & & a_0 + pa_1 & & a_0 + pa_1 + p^2 a_2 & & \cdots \end{array}$$

Sistemi e limiti inversi

Definizione (Limite inverso)

Un limite inverso del sistema inverso $\{G_a, \varphi_{ab}\}_{a \leq b}$ è definito come

$$\varprojlim_{a \in \Lambda} G_a := \left\{ (g_a)_{a \in \Lambda} \in \prod_{a \in \Lambda} G_a : g_a = \varphi_{ab}(g_b) \text{ per ogni } a \leq b \right\}.$$

Esempio

- Insieme parzialmento ordinato diretto: $(\mathbb{N}, \leq)$;
- Insieme di gruppi indicizzati su $\mathbb{N}$: $\{\mathbb{Z}/p^n\mathbb{Z}\}_{n \in \mathbb{N}}$;
- Famiglia di morfismi: $\varphi_{mn} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ mappe di proiezione naturale;

Tale struttura definisce un sistema inverso. Denotiamo il limite inverso associato con

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \left\{ (a_n) \in \prod \mathbb{Z}/p^n\mathbb{Z} \text{ coerenti} \right\}.$$

Un generico elemento di Z_p è della forma

$$\begin{array}{ccccccc} \mathbb{Z}/p\mathbb{Z} & \times & \mathbb{Z}/p^2\mathbb{Z} & \times & \mathbb{Z}/p^3\mathbb{Z} & \times & \cdots \\ a_0 & & a_0 + pa_1 & & a_0 + pa_1 + p^2 a_2 & & \cdots \end{array}$$

Sistemi e limiti inversi

Definizione (Limite inverso)

Un limite inverso del sistema inverso $\{G_a, \varphi_{ab}\}_{a \leq b}$ è definito come

$$\varprojlim_{a \in \Lambda} G_a := \left\{ (g_a)_{a \in \Lambda} \in \prod_{a \in \Lambda} G_a : g_a = \varphi_{ab}(g_b) \text{ per ogni } a \leq b \right\}.$$

Esempio

- Insieme parzialmento ordinato diretto: $(\mathbb{N}, \leq)$;
- Insieme di gruppi indicizzati su $\mathbb{N}$: $\{\mathbb{Z}/p^n\mathbb{Z}\}_{n \in \mathbb{N}}$;
- Famiglia di morfismi: $\varphi_{mn} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ mappe di proiezione naturale;

Tale struttura definisce un sistema inverso. Denotiamo il limite inverso associato con

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \left\{ (a_n) \in \prod \mathbb{Z}/p^n\mathbb{Z} \text{ coerenti} \right\}.$$

Un generico elemento di Z_p è della forma

$$\begin{array}{ccccccc} \mathbb{Z}/p\mathbb{Z} & \times & \mathbb{Z}/p^2\mathbb{Z} & \times & \mathbb{Z}/p^3\mathbb{Z} & \times & \cdots \\ a_0 & & a_0 + pa_1 & & a_0 + pa_1 + p^2 a_2 & & \cdots \end{array}$$

Sistemi e limiti inversi

Definizione (Limite inverso)

Un limite inverso del sistema inverso $\{G_a, \varphi_{ab}\}_{a \leq b}$ è definito come

$$\varprojlim_{a \in \Lambda} G_a := \left\{ (g_a)_{a \in \Lambda} \in \prod_{a \in \Lambda} G_a : g_a = \varphi_{ab}(g_b) \text{ per ogni } a \leq b \right\}.$$

Esempio

- Insieme parzialmento ordinato diretto: $(\mathbb{N}, \leq)$;
- Insieme di gruppi indicizzati su $\mathbb{N}$: $\{\mathbb{Z}/p^n\mathbb{Z}\}_{n \in \mathbb{N}}$;
- Famiglia di morfismi: $\varphi_{mn} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ mappe di proiezione naturale;

Tale struttura definisce un sistema inverso. Denotiamo il limite inverso associato con

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \left\{ (a_n) \in \prod \mathbb{Z}/p^n\mathbb{Z} \text{ coerenti} \right\}.$$

Un generico elemento di Z_p è della forma

$$\begin{array}{ccccccc} \mathbb{Z}/p\mathbb{Z} & \times & \mathbb{Z}/p^2\mathbb{Z} & \times & \mathbb{Z}/p^3\mathbb{Z} & \times & \cdots \\ a_0 & & a_0 + pa_1 & & a_0 + pa_1 + p^2 a_2 & & \cdots \end{array}$$

Gruppi profiniti

Definizione

Un gruppo G si dice essere un gruppo profinito se $G = \varprojlim G_a$ per un certo sistema inverso $\{G_a, \varphi_{ab}\}$, dove ogni G_a è un gruppo finito.

Vorremmo dotare un gruppo prifinito di una buona topologia, che lo renda un gruppo topologico. Procediamo in questo modo:

- Consideriamo un sistema inverso $(G_a, \varphi_{ab})_\Lambda$ di gruppi finiti;
- Dotiamo ogni G_a della topologia discreta;
- Dotiamo $\prod G_a$, della topologia prodotto ξ;
- Dotiamo il gruppo profinito $\varprojlim G_a$ della topologia indotta da ξ;

Proposizione

Sia G un gruppo profinito, dotato della topologia sopra descritta, allora G è un gruppo topologico.

Gruppi profiniti

Definizione

Un gruppo G si dice essere un gruppo profinito se $G = \varprojlim G_a$ per un certo sistema inverso $\{G_a, \varphi_{ab}\}$, dove ogni G_a è un gruppo finito.

Vorremmo dotare un gruppo prifinito di una buona topologia, che lo renda un gruppo topologico. Procediamo in questo modo:

- Consideriamo un sistema inverso $(G_a, \varphi_{ab})_\Lambda$ di gruppi finiti;
- Dotiamo ogni G_a della topologia discreta;
- Dotiamo $\prod G_a$, della topologia prodotto ξ;
- Dotiamo il gruppo profinito $\varprojlim G_a$ della topologia indotta da ξ;

Proposizione

Sia G un gruppo profinito, dotato della topologia sopra descritta, allora G è un gruppo topologico.

Gruppi profiniti

Definizione

Un gruppo G si dice essere un gruppo profinito se $G = \varprojlim G_a$ per un certo sistema inverso $\{G_a, \varphi_{ab}\}$, dove ogni G_a è un gruppo finito.

Vorremmo dotare un gruppo prifinito di una buona topologia, che lo renda un gruppo topologico. Procediamo in questo modo:

- Consideriamo un sistema inverso $(G_a, \varphi_{ab})_\Lambda$ di gruppi finiti;
- Dotiamo ogni G_a della topologia discreta;
- Dotiamo $\prod G_a$, della topologia prodotto ξ;
- Dotiamo il gruppo profinito $\varprojlim G_a$ della topologia indotta da ξ;

Proposizione

Sia G un gruppo profinito, dotato della topologia sopra descritta, allora G è un gruppo topologico.

Gruppi profiniti

Definizione

Un gruppo G si dice essere un gruppo profinito se $G = \varprojlim G_a$ per un certo sistema inverso $\{G_a, \varphi_{ab}\}$, dove ogni G_a è un gruppo finito.

Vorremmo dotare un gruppo prifinito di una buona topologia, che lo renda un gruppo topologico. Procediamo in questo modo:

- Consideriamo un sistema inverso $(G_a, \varphi_{ab})_\Lambda$ di gruppi finiti;
- Dotiamo ogni G_a della topologia discreta;
- Dotiamo $\prod G_a$, della topologia prodotto ξ;
- Dotiamo il gruppo profinito $\varprojlim G_a$ della topologia indotta da ξ;

Proposizione

Sia G un gruppo profinito, dotato della topologia sopra descritta, allora G è un gruppo topologico.

Gruppi profiniti

Definizione

Un gruppo G si dice essere un gruppo profinito se $G = \varprojlim G_a$ per un certo sistema inverso $\{G_a, \varphi_{ab}\}$, dove ogni G_a è un gruppo finito.

Vorremmo dotare un gruppo prifinito di una buona topologia, che lo renda un gruppo topologico. Procediamo in questo modo:

- Consideriamo un sistema inverso $(G_a, \varphi_{ab})_\Lambda$ di gruppi finiti;
- Dotiamo ogni G_a della topologia discreta;
- Dotiamo $\prod G_a$, della topologia prodotto ξ;
- Dotiamo il gruppo profinito $\varprojlim G_a$ della topologia indotta da ξ;

Proposizione

Sia G un gruppo profinito, dotato della topologia sopra descritta, allora G è un gruppo topologico.

Gruppi profiniti

Definizione

Un gruppo G si dice essere un gruppo profinito se $G = \varprojlim G_a$ per un certo sistema inverso $\{G_a, \varphi_{ab}\}$, dove ogni G_a è un gruppo finito.

Vorremmo dotare un gruppo prifinito di una buona topologia, che lo renda un gruppo topologico. Procediamo in questo modo:

- Consideriamo un sistema inverso $(G_a, \varphi_{ab})_\Lambda$ di gruppi finiti;
- Dotiamo ogni G_a della topologia discreta;
- Dotiamo $\prod G_a$, della topologia prodotto ξ;
- Dotiamo il gruppo profinito $\varprojlim G_a$ della topologia indotta da ξ;

Proposizione

Sia G un gruppo profinito, dotato della topologia sopra descritta, allora G è un gruppo topologico.

Gruppi profiniti

Definizione

Un gruppo G si dice essere un gruppo profinito se $G = \varprojlim G_a$ per un certo sistema inverso $\{G_a, \varphi_{ab}\}$, dove ogni G_a è un gruppo finito.

Vorremmo dotare un gruppo prifinito di una buona topologia, che lo renda un gruppo topologico. Procediamo in questo modo:

- Consideriamo un sistema inverso $(G_a, \varphi_{ab})_\Lambda$ di gruppi finiti;
- Dotiamo ogni G_a della topologia discreta;
- Dotiamo $\prod G_a$, della topologia prodotto ξ;
- Dotiamo il gruppo profinito $\varprojlim G_a$ della topologia indotta da ξ;

Proposizione

Sia G un gruppo profinito, dotato della topologia sopra descritta, allora G è un gruppo topologico.

Il gruppo di Galois come gruppo profinito

Vorremmo poter vedere il gruppo di Galois come un gruppo profinito in modo da poter aver tutti i vantaggi legati alla teoria già nota di tali strutture. Avremo innanzitutto bisogno di un particolare sistema inverso, e prima ancora di un insieme parzialmente ordinato diretto.

Proposizione

Sia E/F un'estensione di Galois e siano $M/F, L/F$ due sottoestensioni finite e di Galois su F. Allora LM/F, la più piccola sottoestensione di E contenente sia M che L, è finita e di Galois su F.

- Insieme parzialmente ordinato diretto: $(\Lambda, \subseteq)$ insieme delle sottoestensioni di E finite e di Galois su F;
- Insieme di gruppi indicizzati su Λ: $\{\mathrm{Gal}(M/F)\}_{M\in\Lambda}$;
- Famiglia di morfismi: $\varphi_{MN} : \mathrm{Gal}(N/F) \to \mathrm{Gal}(M/F)$ le restrizioni naturali;

Proposizione

Sia E/F un'estensione di Galois. Allora

$$\mathrm{Gal}(E/F) \cong \varprojlim_{M\in\Lambda} \mathrm{Gal}(M/F).$$

Il gruppo di Galois come gruppo profinito

Vorremmo poter vedere il gruppo di Galois come un gruppo profinito in modo da poter aver tutti i vantaggi legati alla teoria già nota di tali strutture. Avremo innanzitutto bisogno di un particolare sistema inverso, e prima ancora di un insieme parzialmente ordinato diretto.

Proposizione

Sia E/F un'estensione di Galois e siano $M/F, L/F$ due sottoestensioni finite e di Galois su F. Allora LM/F, la più piccola sottoestensione di E contenente sia M che L, è finita e di Galois su F.

- Insieme parzialmente ordinato diretto: $(\Lambda, \subseteq)$ insieme delle sottoestensioni di E finite e di Galois su F;
- Insieme di gruppi indicizzati su Λ: $\{\mathrm{Gal}(M/F)\}_{M\in\Lambda}$;
- Famiglia di morfismi: $\varphi_{MN} : \mathrm{Gal}(N/F) \to \mathrm{Gal}(M/F)$ le restrizioni naturali;

Proposizione

Sia E/F un'estensione di Galois. Allora

$$\mathrm{Gal}(E/F) \cong \varprojlim_{M\in\Lambda} \mathrm{Gal}(M/F).$$

Il gruppo di Galois come gruppo profinito

Vorremmo poter vedere il gruppo di Galois come un gruppo profinito in modo da poter aver tutti i vantaggi legati alla teoria già nota di tali strutture. Avremo innanzitutto bisogno di un particolare sistema inverso, e prima ancora di un insieme parzialmente ordinato diretto.

Proposizione

Sia E/F un'estensione di Galois e siano $M/F, L/F$ due sottoestensioni finite e di Galois su F. Allora LM/F, la più piccola sottoestensione di E contenente sia M che L, è finita e di Galois su F.

- Insieme parzialmente ordinato diretto: $(\Lambda, \subseteq)$ insieme delle sottoestensioni di E finite e di Galois su F;
- Insieme di gruppi indicizzati su Λ: $\{\mathrm{Gal}(M/F)\}_{M\in\Lambda}$;
- Famiglia di morfismi: $\varphi_{MN} : \mathrm{Gal}(N/F) \to \mathrm{Gal}(M/F)$ le restrizioni naturali;

Proposizione

Sia E/F un'estensione di Galois. Allora

$$\mathrm{Gal}(E/F) \cong \varprojlim_{M\in\Lambda} \mathrm{Gal}(M/F).$$

Il gruppo di Galois come gruppo profinito

Vorremmo poter vedere il gruppo di Galois come un gruppo profinito in modo da poter aver tutti i vantaggi legati alla teoria già nota di tali strutture. Avremo innanzitutto bisogno di un particolare sistema inverso, e prima ancora di un insieme parzialmente ordinato diretto.

Proposizione

Sia E/F un'estensione di Galois e siano $M/F, L/F$ due sottoestensioni finite e di Galois su F. Allora LM/F, la più piccola sottoestensione di E contenente sia M che L, è finita e di Galois su F.

- Insieme parzialmente ordinato diretto: $(\Lambda, \subseteq)$ insieme delle sottoestensioni di E finite e di Galois su F;
- Insieme di gruppi indicizzati su Λ: $\{\mathrm{Gal}(M/F)\}_{M\in\Lambda}$;
- Famiglia di morfismi: $\varphi_{MN} : \mathrm{Gal}(N/F) \to \mathrm{Gal}(M/F)$ le restrizioni naturali;

Proposizione

Sia E/F un'estensione di Galois. Allora

$$\mathrm{Gal}(E/F) \cong \varprojlim_{M\in\Lambda} \mathrm{Gal}(M/F).$$

Il gruppo di Galois come gruppo profinito

Vorremmo poter vedere il gruppo di Galois come un gruppo profinito in modo da poter aver tutti i vantaggi legati alla teoria già nota di tali strutture. Avremo innanzitutto bisogno di un particolare sistema inverso, e prima ancora di un insieme parzialmente ordinato diretto.

Proposizione

Sia E/F un'estensione di Galois e siano $M/F, L/F$ due sottoestensioni finite e di Galois su F. Allora LM/F, la più piccola sottoestensione di E contenente sia M che L, è finita e di Galois su F.

- Insieme parzialmente ordinato diretto: $(\Lambda, \subseteq)$ insieme delle sottoestensioni di E finite e di Galois su F;
- Insieme di gruppi indicizzati su Λ: $\{\mathrm{Gal}(M/F)\}_{M\in\Lambda}$;
- Famiglia di morfismi: $\varphi_{MN} : \mathrm{Gal}(N/F) \to \mathrm{Gal}(M/F)$ le restrizioni naturali;

Proposizione

Sia E/F un'estensione di Galois. Allora

$$\mathrm{Gal}(E/F) \cong \varprojlim_{M\in\Lambda} \mathrm{Gal}(M/F).$$

Il gruppo di Galois come gruppo profinito

Vorremmo poter vedere il gruppo di Galois come un gruppo profinito in modo da poter aver tutti i vantaggi legati alla teoria già nota di tali strutture. Avremo innanzitutto bisogno di un particolare sistema inverso, e prima ancora di un insieme parzialmente ordinato diretto.

Proposizione

Sia E/F un'estensione di Galois e siano $M/F, L/F$ due sottoestensioni finite e di Galois su F. Allora LM/F, la più piccola sottoestensione di E contenente sia M che L, è finita e di Galois su F.

- Insieme parzialmente ordinato diretto: $(\Lambda, \subseteq)$ insieme delle sottoestensioni di E finite e di Galois su F;
- Insieme di gruppi indicizzati su Λ: $\{\mathrm{Gal}(M/F)\}_{M\in\Lambda}$;
- Famiglia di morfismi: $\varphi_{MN} : \mathrm{Gal}(N/F) \to \mathrm{Gal}(M/F)$ le restrizioni naturali;

Proposizione

Sia E/F un'estensione di Galois. Allora

$$\mathrm{Gal}(E/F) \cong \varprojlim_{M\in\Lambda} \mathrm{Gal}(M/F).$$

Il gruppo di Galois come gruppo profinito

Esempio

Ricordiamo che se $K_n = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$, con $p_1, ..., p_n$ primi distinti, allora $K_n/\mathbb{Q}$ è di Galois e vale:

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

Sia ora $K = \mathbb{Q}(\{\sqrt{p} \,|\, p \text{ primo}\})$. Si ha che $K/\mathbb{Q}$ è un'estensione di Galois di grado infinito, e pertanto:

- $\mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(F_i/\mathbb{Q})$, dove $F_i/\mathbb{Q}$ sono le sottoestensioni finite e di Galois di $K/\mathbb{Q}$;
- Ma i K_n sono una sottofamiglia filtrante delle $F_i \to \mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(K_n/\mathbb{Q})$;

Osservato che la famiglia $\{K_n\}$ è totalmente ordinata, segue:

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

Il gruppo di Galois come gruppo profinito

Esempio

Ricordiamo che se $K_n = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$, con $p_1, ..., p_n$ primi distinti, allora $K_n/\mathbb{Q}$ è di Galois e vale:

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

Sia ora $K = \mathbb{Q}(\{\sqrt{p} \,|\, p \text{ primo}\})$. Si ha che $K/\mathbb{Q}$ è un'estensione di Galois di grado infinito, e pertanto:

- $\mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(F_i/\mathbb{Q})$, dove $F_i/\mathbb{Q}$ sono le sottoestensioni finite e di Galois di $K/\mathbb{Q}$;
- Ma i K_n sono una sottofamiglia filtrante delle $F_i \to \mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(K_n/\mathbb{Q})$;

Osservato che la famiglia $\{K_n\}$ è totalmente ordinata, segue:

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

Il gruppo di Galois come gruppo profinito

Esempio

Ricordiamo che se $K_n = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$, con $p_1, ..., p_n$ primi distinti, allora $K_n/\mathbb{Q}$ è di Galois e vale:

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

Sia ora $K = \mathbb{Q}(\{\sqrt{p} \mid p \text{ primo}\})$. Si ha che $K/\mathbb{Q}$ è un'estensione di Galois di grado infinito, e pertanto:

- $\mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(F_i/\mathbb{Q})$, dove $F_i/\mathbb{Q}$ sono le sottoestensioni finite e di Galois di $K/\mathbb{Q}$;
- Ma i K_n sono una sottofamiglia filtrante delle $F_i \to \mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(K_n/\mathbb{Q})$;

Osservato che la famiglia $\{K_n\}$ è totalmente ordinata, segue:

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

Il gruppo di Galois come gruppo profinito

Esempio

Ricordiamo che se $K_n = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$, con $p_1, ..., p_n$ primi distinti, allora $K_n/\mathbb{Q}$ è di Galois e vale:

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

Sia ora $K = \mathbb{Q}(\{\sqrt{p} \mid p \text{ primo}\})$. Si ha che $K/\mathbb{Q}$ è un'estensione di Galois di grado infinito, e pertanto:

- $\mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(F_i/\mathbb{Q})$, dove $F_i/\mathbb{Q}$ sono le sottoestensioni finite e di Galois di $K/\mathbb{Q}$;
- Ma i K_n sono una sottofamiglia filtrante delle $F_i \to \mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(K_n/\mathbb{Q})$;

Osservato che la famiglia $\{K_n\}$ è totalmente ordinata, segue:

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

Il gruppo di Galois come gruppo profinito

Esempio

Ricordiamo che se $K_n = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$, con $p_1, ..., p_n$ primi distinti, allora $K_n/\mathbb{Q}$ è di Galois e vale:

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

Sia ora $K = \mathbb{Q}(\{\sqrt{p} \mid p \text{ primo}\})$. Si ha che $K/\mathbb{Q}$ è un'estensione di Galois di grado infinito, e pertanto:

- $\mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(F_i/\mathbb{Q})$, dove $F_i/\mathbb{Q}$ sono le sottoestensioni finite e di Galois di $K/\mathbb{Q}$;
- Ma i K_n sono una sottofamiglia filtrante delle $F_i \to \mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(K_n/\mathbb{Q})$;

Osservato che la famiglia $\{K_n\}$ è totalmente ordinata, segue:

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

Il gruppo di Galois come gruppo profinito

Esempio

Ricordiamo che se $K_n = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$, con $p_1, ..., p_n$ primi distinti, allora $K_n/\mathbb{Q}$ è di Galois e vale:

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

Sia ora $K = \mathbb{Q}(\{\sqrt{p} \mid p \text{ primo}\})$. Si ha che $K/\mathbb{Q}$ è un'estensione di Galois di grado infinito, e pertanto:

- $\mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(F_i/\mathbb{Q})$, dove $F_i/\mathbb{Q}$ sono le sottoestensioni finite e di Galois di $K/\mathbb{Q}$;
- Ma i K_n sono una sottofamiglia filtrante delle $F_i \to \mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(K_n/\mathbb{Q})$;

Osservato che la famiglia $\{K_n\}$ è totalmente ordinata, segue:

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

Il gruppo di Galois come gruppo profinito

Esempio

Ricordiamo che se $K_n = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$, con $p_1, ..., p_n$ primi distinti, allora $K_n/\mathbb{Q}$ è di Galois e vale:

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

Sia ora $K = \mathbb{Q}(\{\sqrt{p} \mid p \text{ primo}\})$. Si ha che $K/\mathbb{Q}$ è un'estensione di Galois di grado infinito, e pertanto:

- $\mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(F_i/\mathbb{Q})$, dove $F_i/\mathbb{Q}$ sono le sottoestensioni finite e di Galois di $K/\mathbb{Q}$;
- Ma i K_n sono una sottofamiglia filtrante delle $F_i \to \mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(K_n/\mathbb{Q})$;

Osservato che la famiglia $\{K_n\}$ è totalmente ordinata, segue:

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

Il gruppo di Galois come gruppo profinito

Esempio

Ricordiamo che se $K_n = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$, con $p_1, ..., p_n$ primi distinti, allora $K_n/\mathbb{Q}$ è di Galois e vale:

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

Sia ora $K = \mathbb{Q}(\{\sqrt{p} \mid p \text{ primo}\})$. Si ha che $K/\mathbb{Q}$ è un'estensione di Galois di grado infinito, e pertanto:

- $\mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(F_i/\mathbb{Q})$, dove $F_i/\mathbb{Q}$ sono le sottoestensioni finite e di Galois di $K/\mathbb{Q}$;
- Ma i K_n sono una sottofamiglia filtrante delle $F_i \to \mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(K_n/\mathbb{Q})$;

Osservato che la famiglia $\{K_n\}$ è totalmente ordinata, segue:

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

Il gruppo di Galois come gruppo profinito

Esempio

Ricordiamo che se $K_n = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$, con $p_1, ..., p_n$ primi distinti, allora $K_n/\mathbb{Q}$ è di Galois e vale:

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

Sia ora $K = \mathbb{Q}(\{\sqrt{p} \mid p \text{ primo}\})$. Si ha che $K/\mathbb{Q}$ è un'estensione di Galois di grado infinito, e pertanto:

- $\mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(F_i/\mathbb{Q})$, dove $F_i/\mathbb{Q}$ sono le sottoestensioni finite e di Galois di $K/\mathbb{Q}$;
- Ma i K_n sono una sottofamiglia filtrante delle $F_i \to \mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(K_n/\mathbb{Q})$;

Osservato che la famiglia $\{K_n\}$ è totalmente ordinata, segue:

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

Il gruppo di Galois come gruppo profinito

La caratterizzazione di $\mathrm{Gal}(E/F)$ come gruppo profinito non è sufficiente per avere una corrisopondenza come nel Teorema fondamentale nel caso finito.

Esempio

Consideriamo l'insieme $S := \{\sqrt{p} \mid p \in \mathbb{N} \text{ primo}\}$, e sia $K := \mathbb{Q}(S)$.

- $\mathrm{Gal}(K/\mathbb{Q}) \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$;
- Possiamo quindi immaginare $\mathrm{Gal}(K/\mathbb{Q})$ come uno spazio vettoriale V di dimensione infinita sul campo $F := \mathbb{Z}/2\mathbb{Z}$;
- Pertanto lo spazio vettoriale duale $V^* := \{\phi : V \to F : \phi \text{ è una mappa lineare}\}$ è più che numerabile;
- $\{\ker(\phi) : \phi \in V^*\}$ non è numerabile;
- Per ogni ϕ si ha che $\ker(\phi)$ è un sottogruppo di G di indice 2, e ci sono quindi una quantità non numerabile di sottogruppi di questo tipo.

Tuttavia, seguendo la logica del Teorema Fondamentale, i campi intermedi associati dovrebbero avere grado 2 su $\mathbb{Q}$, ovvero coinciderebbero con gli insiemi del tipo $\{\mathbb{Q}(\sqrt{p}) \mid p \in \mathbb{Q} \text{ non un quadrato perfetto}\}$, che è certamente una famiglia numerabile.

Il gruppo di Galois come gruppo profinito

La caratterizzazione di $\mathrm{Gal}(E/F)$ come gruppo profinito non è sufficiente per avere una corrisopondenza come nel Teorema fondamentale nel caso finito.

Esempio

Consideriamo l'insieme $S := \{\sqrt{p} \mid p \in \mathbb{N} \text{ primo}\}$, e sia $K := \mathbb{Q}(S)$.

- $\mathrm{Gal}(K/\mathbb{Q}) \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$;
- Possiamo quindi immaginare $\mathrm{Gal}(K/\mathbb{Q})$ come uno spazio vettoriale V di dimensione infinita sul campo $F := \mathbb{Z}/2\mathbb{Z}$;
- Pertanto lo spazio vettoriale duale $V^* := \{\phi : V \to F : \phi \text{ è una mappa lineare}\}$ è più che numerabile;
- $\{\ker(\phi) : \phi \in V^*\}$ non è numerabile;
- Per ogni ϕ si ha che $\ker(\phi)$ è un sottogruppo di G di indice 2, e ci sono quindi una quantità non numerabile di sottogruppi di questo tipo.

Tuttavia, seguendo la logica del Teorema Fondamentale, i campi intermedi associati dovrebbero avere grado 2 su $\mathbb{Q}$, ovvero coinciderebbero con gli insiemi del tipo $\{\mathbb{Q}(\sqrt{p}) \mid p \in \mathbb{Q} \text{ non un quadrato perfetto}\}$, che è certamente una famiglia numerabile.

Il gruppo di Galois come gruppo profinito

La caratterizzazione di $\mathrm{Gal}(E/F)$ come gruppo profinito non è sufficiente per avere una corrisopondenza come nel Teorema fondamentale nel caso finito.

Esempio

Consideriamo l'insieme $S := \{\sqrt{p} \mid p \in \mathbb{N} \text{ primo}\}$, e sia $K := \mathbb{Q}(S)$.

- $\mathrm{Gal}(K/\mathbb{Q}) \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$;
- Possiamo quindi immaginare $\mathrm{Gal}(K/\mathbb{Q})$ come uno spazio vettoriale V di dimensione infinita sul campo $F := \mathbb{Z}/2\mathbb{Z}$;
- Pertanto lo spazio vettoriale duale $V^* := \{\phi : V \to F : \phi \text{ è una mappa lineare}\}$ è più che numerabile;
- $\{\ker(\phi) : \phi \in V^*\}$ non è numerabile;
- Per ogni ϕ si ha che $\ker(\phi)$ è un sottogruppo di G di indice 2, e ci sono quindi una quantità non numerabile di sottogruppi di questo tipo.

Tuttavia, seguendo la logica del Teorema Fondamentale, i campi intermedi associati dovrebbero avere grado 2 su $\mathbb{Q}$, ovvero coinciderebbero con gli insiemi del tipo $\{\mathbb{Q}(\sqrt{p}) \mid p \in \mathbb{Q} \text{ non un quadrato perfetto}\}$, che è certamente una famiglia numerabile.

Il gruppo di Galois come gruppo profinito

La caratterizzazione di $\mathrm{Gal}(E/F)$ come gruppo profinito non è sufficiente per avere una corrisopondenza come nel Teorema fondamentale nel caso finito.

Esempio

Consideriamo l'insieme $S := \{\sqrt{p} \mid p \in \mathbb{N} \text{ primo}\}$, e sia $K := \mathbb{Q}(S)$.

- $\mathrm{Gal}(K/\mathbb{Q}) \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$;
- Possiamo quindi immaginare $\mathrm{Gal}(K/\mathbb{Q})$ come uno spazio vettoriale V di dimensione infinita sul campo $F := \mathbb{Z}/2\mathbb{Z}$;
- Pertanto lo spazio vettoriale duale $V^* := \{\phi : V \to F : \phi \text{ è una mappa lineare}\}$ è più che numerabile;
- $\{\ker(\phi) : \phi \in V^*\}$ non è numerabile;
- Per ogni ϕ si ha che $\ker(\phi)$ è un sottogruppo di G di indice 2, e ci sono quindi una quantità non numerabile di sottogruppi di questo tipo.

Tuttavia, seguendo la logica del Teorema Fondamentale, i campi intermedi associati dovrebbero avere grado 2 su $\mathbb{Q}$, ovvero coinciderebbero con gli insiemi del tipo $\{\mathbb{Q}(\sqrt{p}) \mid p \in \mathbb{Q} \text{ non un quadrato perfetto}\}$, che è certamente una famiglia numerabile.

Il gruppo di Galois come gruppo profinito

La caratterizzazione di $\mathrm{Gal}(E/F)$ come gruppo profinito non è sufficiente per avere una corrisopondenza come nel Teorema fondamentale nel caso finito.

Esempio

Consideriamo l'insieme $S := \{\sqrt{p} \mid p \in \mathbb{N} \text{ primo}\}$, e sia $K := \mathbb{Q}(S)$.

- $\mathrm{Gal}(K/\mathbb{Q}) \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$;
- Possiamo quindi immaginare $\mathrm{Gal}(K/\mathbb{Q})$ come uno spazio vettoriale V di dimensione infinita sul campo $F := \mathbb{Z}/2\mathbb{Z}$;
- Pertanto lo spazio vettoriale duale $V^* := \{\phi : V \to F : \phi \text{ è una mappa lineare}\}$ è più che numerabile;
- $\{\ker(\phi) : \phi \in V^*\}$ non è numerabile;
- Per ogni ϕ si ha che $\ker(\phi)$ è un sottogruppo di G di indice 2, e ci sono quindi una quantità non numerabile di sottogruppi di questo tipo.

Tuttavia, seguendo la logica del Teorema Fondamentale, i campi intermedi associati dovrebbero avere grado 2 su $\mathbb{Q}$, ovvero coinciderebbero con gli insiemi del tipo $\{\mathbb{Q}(\sqrt{p}) \mid p \in \mathbb{Q} \text{ non un quadrato perfetto}\}$, che è certamente una famiglia numerabile.

Il gruppo di Galois come gruppo profinito

La caratterizzazione di $\mathrm{Gal}(E/F)$ come gruppo profinito non è sufficiente per avere una corrisopondenza come nel Teorema fondamentale nel caso finito.

Esempio

Consideriamo l'insieme $S := \{\sqrt{p} \mid p \in \mathbb{N} \text{ primo}\}$, e sia $K := \mathbb{Q}(S)$.

- $\mathrm{Gal}(K/\mathbb{Q}) \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$;
- Possiamo quindi immaginare $\mathrm{Gal}(K/\mathbb{Q})$ come uno spazio vettoriale V di dimensione infinita sul campo $F := \mathbb{Z}/2\mathbb{Z}$;
- Pertanto lo spazio vettoriale duale $V^* := \{\phi : V \to F : \phi \text{ è una mappa lineare}\}$ è più che numerabile;
- $\{\ker(\phi) : \phi \in V^*\}$ non è numerabile;
- Per ogni ϕ si ha che $\ker(\phi)$ è un sottogruppo di G di indice 2, e ci sono quindi una quantità non numerabile di sottogruppi di questo tipo.

Tuttavia, seguendo la logica del Teorema Fondamentale, i campi intermedi associati dovrebbero avere grado 2 su $\mathbb{Q}$, ovvero coinciderebbero con gli insiemi del tipo $\{\mathbb{Q}(\sqrt{p}) \mid p \in \mathbb{Q} \text{ non un quadrato perfetto}\}$, che è certamente una famiglia numerabile.

Il gruppo di Galois come gruppo profinito

La caratterizzazione di $\mathrm{Gal}(E/F)$ come gruppo profinito non è sufficiente per avere una corrisopondenza come nel Teorema fondamentale nel caso finito.

Esempio

Consideriamo l'insieme $S := \{\sqrt{p} \mid p \in \mathbb{N} \text{ primo}\}$, e sia $K := \mathbb{Q}(S)$.

- $\mathrm{Gal}(K/\mathbb{Q}) \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$;
- Possiamo quindi immaginare $\mathrm{Gal}(K/\mathbb{Q})$ come uno spazio vettoriale V di dimensione infinita sul campo $F := \mathbb{Z}/2\mathbb{Z}$;
- Pertanto lo spazio vettoriale duale $V^* := \{\phi : V \to F : \phi \text{ è una mappa lineare}\}$ è più che numerabile;
- $\{\ker(\phi) : \phi \in V^*\}$ non è numerabile;
- Per ogni ϕ si ha che $\ker(\phi)$ è un sottogruppo di G di indice 2, e ci sono quindi una quantità non numerabile di sottogruppi di questo tipo.

Tuttavia, seguendo la logica del Teorema Fondamentale, i campi intermedi associati dovrebbero avere grado 2 su $\mathbb{Q}$, ovvero coinciderebbero con gli insiemi del tipo $\{\mathbb{Q}(\sqrt{p}) \mid p \in \mathbb{Q} \text{ non un quadrato perfetto}\}$, che è certamente una famiglia numerabile.

Il gruppo di Galois come gruppo profinito

La caratterizzazione di $\mathrm{Gal}(E/F)$ come gruppo profinito non è sufficiente per avere una corrisopondenza come nel Teorema fondamentale nel caso finito.

Esempio

Consideriamo l'insieme $S := \{\sqrt{p} \mid p \in \mathbb{N} \text{ primo}\}$, e sia $K := \mathbb{Q}(S)$.

- $\mathrm{Gal}(K/\mathbb{Q}) \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$;
- Possiamo quindi immaginare $\mathrm{Gal}(K/\mathbb{Q})$ come uno spazio vettoriale V di dimensione infinita sul campo $F := \mathbb{Z}/2\mathbb{Z}$;
- Pertanto lo spazio vettoriale duale $V^* := \{\phi : V \to F : \phi \text{ è una mappa lineare}\}$ è più che numerabile;
- $\{\ker(\phi) : \phi \in V^*\}$ non è numerabile;
- Per ogni ϕ si ha che $\ker(\phi)$ è un sottogruppo di G di indice 2, e ci sono quindi una quantità non numerabile di sottogruppi di questo tipo.

Tuttavia, seguendo la logica del Teorema Fondamentale, i campi intermedi associati dovrebbero avere grado 2 su $\mathbb{Q}$, ovvero coinciderebbero con gli insiemi del tipo $\{\mathbb{Q}(\sqrt{p}) \mid p \in \mathbb{Q} \text{ non un quadrato perfetto}\}$, che è certamente una famiglia numerabile.

Topologia di Krull

Risolveremo questo problema considerando solamente i sottogruppi chiusi di $\mathrm{Gal}(E/F)$ in un'opportuna topologia, che andremo ora a descrivere.

Definizione (topologia di Krull)

Dotiamo ogni $\mathrm{Gal}(M/F)$ della topologia discreta e consideriamo $(\prod \mathrm{Gal}(M/F), \xi)$, dove abbiamo indicato con ξ la topologia prodotto. Chiameremo topologia di Krull la topologia indotta da $(\prod \mathrm{Gal}(M/F), \xi)$ sul sottogruppo $\varprojlim \mathrm{Gal}(M/F)$.

$\Rightarrow$ È la stessa topologia che abbiamo definito prima!

Topologia di Krull

Risolveremo questo problema considerando solamente i sottogruppi chiusi di $\mathrm{Gal}(E/F)$ in un'opportuna topologia, che andremo ora a descrivere.

Definizione (topologia di Krull)

Dotiamo ogni $\mathrm{Gal}(M/F)$ della topologia discreta e consideriamo $(\prod \mathrm{Gal}(M/F), \xi)$, dove abbiamo indicato con ξ la topologia prodotto. Chiameremo topologia di Krull la topologia indotta da $(\prod \mathrm{Gal}(M/F), \xi)$ sul sottogruppo $\varprojlim \mathrm{Gal}(M/F)$.

$\Rightarrow$ È la stessa topologia che abbiamo definito prima!

Topologia di Krull

Risolveremo questo problema considerando solamente i sottogruppi chiusi di $\mathrm{Gal}(E/F)$ in un'opportuna topologia, che andremo ora a descrivere.

Definizione (topologia di Krull)

Dotiamo ogni $\mathrm{Gal}(M/F)$ della topologia discreta e consideriamo $(\prod \mathrm{Gal}(M/F), \xi)$, dove abbiamo indicato con ξ la topologia prodotto. Chiameremo topologia di Krull la topologia indotta da $(\prod \mathrm{Gal}(M/F), \xi)$ sul sottogruppo $\varprojlim \mathrm{Gal}(M/F)$.

$\Rightarrow$ È la stessa topologia che abbiamo definito prima!

Corrispondenza di Galois per estensioni di grado infinito

Teorema

Sia E/F un'estensione di Galois infinita e sia $G := \mathrm{Gal}(E/F)$. Allora le mappe

$$L \mapsto H := \mathrm{Gal}(E/L) \qquad e \qquad H \mapsto L := E^H$$

inducono una biiezione fra i sottocampi intermedi di E/F e i sottogruppi chiusi di G che rovescia le inclusioni. L'estensione L/F è di Galois se e solo se H è normale in G e in tal caso si ha $\mathrm{Gal}(L/F) \cong G/H$. L'estensione L/F è finita se e solo se H è un sottogruppo aperto di G.

Considerazioni conclusive

Ora che abbiamo enunciato il teorema fondamentale per estensioni di grado arbitrario una domanda che viene naturale porsi è:

Si tratta di un risultato effettivamente utile?

Definizione (Campo ordinato)

Un campo F è ordinato se esiste un insieme $P \subseteq F$, che chiameremo l'insieme degli elementi positivi, tale che P è chiuso sotto addizione e moltiplicazione, e F è l'unione disgiunta degli insiemi P, $\{0\}$ e $-P := \{-p : p \in P\}$.

Definizione (Campo reale chiuso)

Un campo F è reale chiuso se F è ordinato (con gli elementi positivi in P), ogni $x \in P$ ammette una radice quadrata in F, e ogni polinomio $f(Y) \in F[Y]$ di grado dispari ha una radice in F.

Teorema

Un campo F è reale chiuso se e solo se $\sqrt{-1} \notin F$ (ovvero il polinomio $Y^2 - 1$ non ha radici in F) e $K := F(\sqrt{-1})$ è algebricamente chiuso.

Considerazioni conclusive

Ora che abbiamo enunciato il teorema fondamentale per estensioni di grado arbitrario una domanda che viene naturale porsi è:
Si tratta di un risultato effettivamente utile?

Definizione (Campo ordinato)

Un campo F è ordinato se esiste un insieme $P \subseteq F$, che chiameremo l'insieme degli elementi positivi, tale che P è chiuso sotto addizione e moltiplicazione, e F è l'unione disgiunta degli insiemi P, $\{0\}$ e $-P := \{-p : p \in P\}$.

Definizione (Campo reale chiuso)

Un campo F è reale chiuso se F è ordinato (con gli elementi positivi in P), ogni $x \in P$ ammette una radice quadrata in F, e ogni polinomio $f(Y) \in F[Y]$ di grado dispari ha una radice in F.

Teorema

Un campo F è reale chiuso se e solo se $\sqrt{-1} \notin F$ (ovvero il polinomio $Y^2 - 1$ non ha radici in F) e $K := F(\sqrt{-1})$ è algebricamente chiuso.

Considerazioni conclusive

Ora che abbiamo enunciato il teorema fondamentale per estensioni di grado arbitrario una domanda che viene naturale porsi è:
Si tratta di un risultato effettivamente utile?

Definizione (Campo ordinato)

Un campo F è ordinato se esiste un insieme $P \subseteq F$, che chiameremo l'insieme degli elementi positivi, tale che P è chiuso sotto addizione e moltiplicazione, e F è l'unione disgiunta degli insiemi P, $\{0\}$ e $-P := \{-p : p \in P\}$.

Definizione (Campo reale chiuso)

Un campo F è reale chiuso se F è ordinato (con gli elementi positivi in P), ogni $x \in P$ ammette una radice quadrata in F, e ogni polinomio $f(Y) \in F[Y]$ di grado dispari ha una radice in F.

Teorema

Un campo F è reale chiuso se e solo se $\sqrt{-1} \notin F$ (ovvero il polinomio $Y^2 - 1$ non ha radici in F) e $K := F(\sqrt{-1})$ è algebricamente chiuso.

Considerazioni conclusive

Ora che abbiamo enunciato il teorema fondamentale per estensioni di grado arbitrario una domanda che viene naturale porsi è:
Si tratta di un risultato effettivamente utile?

Definizione (Campo ordinato)

Un campo F è ordinato se esiste un insieme $P \subseteq F$, che chiameremo l'insieme degli elementi positivi, tale che P è chiuso sotto addizione e moltiplicazione, e F è l'unione disgiunta degli insiemi P, $\{0\}$ e $-P := \{-p : p \in P\}$.

Definizione (Campo reale chiuso)

Un campo F è reale chiuso se F è ordinato (con gli elementi positivi in P), ogni $x \in P$ ammette una radice quadrata in F, e ogni polinomio $f(Y) \in F[Y]$ di grado dispari ha una radice in F.

Teorema

Un campo F è reale chiuso se e solo se $\sqrt{-1} \notin F$ (ovvero il polinomio $Y^2 - 1$ non ha radici in F) e $K := F(\sqrt{-1})$ è algebricamente chiuso.

Considerazioni conclusive

Ora che abbiamo enunciato il teorema fondamentale per estensioni di grado arbitrario una domanda che viene naturale porsi è:
Si tratta di un risultato effettivamente utile?

Definizione (Campo ordinato)

Un campo F è ordinato se esiste un insieme $P \subseteq F$, che chiameremo l'insieme degli elementi positivi, tale che P è chiuso sotto addizione e moltiplicazione, e F è l'unione disgiunta degli insiemi P, $\{0\}$ e $-P := \{-p : p \in P\}$.

Definizione (Campo reale chiuso)

Un campo F è reale chiuso se F è ordinato (con gli elementi positivi in P), ogni $x \in P$ ammette una radice quadrata in F, e ogni polinomio $f(Y) \in F[Y]$ di grado dispari ha una radice in F.

Teorema

Un campo F è reale chiuso se e solo se $\sqrt{-1} \notin F$ (ovvero il polinomio $Y^2 - 1$ non ha radici in F) e $K := F(\sqrt{-1})$ è algebricamente chiuso.

Considerazioni conclusive

Teorema (Artin-Schreirer)

Sia K un campo algebricamente chiuso, $F \subsetneq K$ un sottocampo proprio tale che $[K : F] < \infty$. Allora F è reale chiuso, e $K = F(\sqrt{-1})$.

- se $[\overline{F} : F] = n < \infty$ allora F è reale chiuso, $\overline{F} = F(\sqrt{-1})$, e quindi $n = 2$;
- se F non è reale chiuso, allora necessariamente $[\overline{F} : F] = \infty$;
- Ogni estensione algebrica di un campo finito oppure di caratteristica zero è separabile $\Longrightarrow \overline{F}/F$ è di Galois.

Conclusione:
la teoria che abbiamo sviluppato finora circa le estensioni di Galois di grado infinito è particolarmente utile, poichè la maggior parte dei campi che incontriamo non sono reali chiusi e sono o finiti o di caratteristica zero.

Considerazioni conclusive

Teorema (Artin-Schreirer)

Sia K un campo algebricamente chiuso, $F \subsetneq K$ un sottocampo proprio tale che $[K : F] < \infty$. Allora F è reale chiuso, e $K = F(\sqrt{-1})$.

- se $[\overline{F} : F] = n < \infty$ allora F è reale chiuso, $\overline{F} = F(\sqrt{-1})$, e quindi $n = 2$;
- se F non è reale chiuso, allora necessariamente $[\overline{F} : F] = \infty$;
- Ogni estensione algebrica di un campo finito oppure di caratteristica zero è separabile $\Longrightarrow \overline{F}/F$ è di Galois.

Conclusione:
la teoria che abbiamo sviluppato finora circa le estensioni di Galois di grado infinito è particolarmente utile, poichè la maggior parte dei campi che incontriamo non sono reali chiusi e sono o finiti o di caratteristica zero.

Considerazioni conclusive

Teorema (Artin-Schreirer)

Sia K un campo algebricamente chiuso, $F \subsetneq K$ un sottocampo proprio tale che $[K : F] < \infty$. Allora F è reale chiuso, e $K = F(\sqrt{-1})$.

- se $[\overline{F} : F] = n < \infty$ allora F è reale chiuso, $\overline{F} = F(\sqrt{-1})$, e quindi $n = 2$;
- se F non è reale chiuso, allora necessariamente $[\overline{F} : F] = \infty$;
- Ogni estensione algebrica di un campo finito oppure di caratteristica zero è separabile $\Longrightarrow \overline{F}/F$ è di Galois.

Conclusione:
la teoria che abbiamo sviluppato finora circa le estensioni di Galois di grado infinito è particolarmente utile, poichè la maggior parte dei campi che incontriamo non sono reali chiusi e sono o finiti o di caratteristica zero.

Considerazioni conclusive

Teorema (Artin-Schreirer)

Sia K un campo algebricamente chiuso, $F \subsetneq K$ un sottocampo proprio tale che $[K : F] < \infty$. Allora F è reale chiuso, e $K = F(\sqrt{-1})$.

- se $[\overline{F} : F] = n < \infty$ allora F è reale chiuso, $\overline{F} = F(\sqrt{-1})$, e quindi $n = 2$;
- se F non è reale chiuso, allora necessariamente $[\overline{F} : F] = \infty$;
- Ogni estensione algebrica di un campo finito oppure di caratteristica zero è separabile $\Longrightarrow \overline{F}/F$ è di Galois.

Conclusione:
la teoria che abbiamo sviluppato finora circa le estensioni di Galois di grado infinito è particolarmente utile, poichè la maggior parte dei campi che incontriamo non sono reali chiusi e sono o finiti o di caratteristica zero.

Considerazioni conclusive

Teorema (Artin-Schreirer)

Sia K un campo algebricamente chiuso, $F \subsetneq K$ un sottocampo proprio tale che $[K : F] < \infty$. Allora F è reale chiuso, e $K = F(\sqrt{-1})$.

- se $[\overline{F} : F] = n < \infty$ allora F è reale chiuso, $\overline{F} = F(\sqrt{-1})$, e quindi $n = 2$;
- se F non è reale chiuso, allora necessariamente $[\overline{F} : F] = \infty$;
- Ogni estensione algebrica di un campo finito oppure di caratteristica zero è separabile $\Longrightarrow \overline{F}/F$ è di Galois.

Conclusione:
la teoria che abbiamo sviluppato finora circa le estensioni di Galois di grado infinito è particolarmente utile, poichè la maggior parte dei campi che incontriamo non sono reali chiusi e sono o finiti o di caratteristica zero.

Considerazioni conclusive

Teorema (Artin-Schreirer)

Sia K un campo algebricamente chiuso, $F \subsetneq K$ un sottocampo proprio tale che $[K : F] < \infty$. Allora F è reale chiuso, e $K = F(\sqrt{-1})$.

- se $[\overline{F} : F] = n < \infty$ allora F è reale chiuso, $\overline{F} = F(\sqrt{-1})$, e quindi $n = 2$;
- se F non è reale chiuso, allora necessariamente $[\overline{F} : F] = \infty$;
- Ogni estensione algebrica di un campo finito oppure di caratteristica zero è separabile $\Longrightarrow \overline{F}/F$ è di Galois.

Conclusione:
la teoria che abbiamo sviluppato finora circa le estensioni di Galois di grado infinito è particolarmente utile, poichè la maggior parte dei campi che incontriamo non sono reali chiusi e sono o finiti o di caratteristica zero.