Complementi Algebra I

Mirko Torresani

18 novembre 2021

Sommario

In queste pagine vengono dimostrati alcuni interessanti complementi di Algebra I. Per la comprensione è quindi necessario sapere il programma di quest'ultima, in particolare quello del corso tenuto dalla professoressa Ilaria del Corso.

Chiusura Normale

Data un'estensione $\mathbb{F}/\mathbb{K}$ non normale, uno si potrebbe chiedere se esiste la più piccola estensione normale di $\mathbb{K}$ che contiene $\mathbb{F}$. La risposta è affermativa, e per la dimostrazione iniziamo con questo teorema. Ricordiamo che con $\overline{\mathbb{K}}$ indichiamo una chiusura algebrica di $\mathbb{K}$.

Teorema. *Sia $\mathbb{F}/\mathbb{K}$ una estensione algebrica. Allora per ogni immersione $\varphi\colon \mathbb{K} \hookrightarrow \overline{\mathbb{K}}$ esiste una $\tilde{\varphi}\colon \mathbb{F} \hookrightarrow \overline{\mathbb{K}}$ tale che $\tilde{\varphi}|_{\mathbb{K}} = \varphi$.*

Dimostrazione. Dimostriamo il caso infinito, essendo il caso finito già stato trattato a lezione.

Sia quindi

$$X = \left\{ (\mathbb{E}, \psi) \;\middle|\; \mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{F}, \psi\colon \mathbb{E} \hookrightarrow \overline{\mathbb{K}}, \psi|_{\mathbb{K}} = \varphi \right\}$$

L'insieme X è non vuoto essendo che $(\mathbb{K}, \varphi) \in X$. Inoltre definiamo la relazione $\preccurlyeq$ come

$$(\mathbb{E}_1, \psi_1) \preccurlyeq (\mathbb{E}_2, \psi_2) \Leftrightarrow \mathbb{E}_1 \subseteq \mathbb{E}_2, \psi_2|_{\mathbb{E}_1} = \psi_1$$

L'obiettivo è dimostrare che $(X, \preccurlyeq)$ è un insieme induttivo.

Sia quindi $C = \{(\mathbb{E}_i, \psi_i)\}_{i \in I}$ un catena di X. Poniamo allora

$$\begin{aligned} \mathbb{E}_\infty &= \bigcup_{i \in I} \mathbb{E}_i \\ \psi\colon \mathbb{E}_\infty &\to \overline{\mathbb{K}} \\ x &\mapsto \psi_i(x) \text{ } t.c. \text{ } x \in \mathbb{E}_i \end{aligned}$$

Dimostriamo innanzitutto la buona definizione di ψ. Se $x \in \mathbb{E}_\infty$ è tale che $x \in \mathbb{E}_i \cap \mathbb{E}_j$, senza perdita di generalità possiamo porre $(\mathbb{E}_i, \psi_i) \preccurlyeq (\mathbb{E}_j, \psi_j)$. Quindi $\psi_j(x) = \psi_j|_{\mathbb{E}_i}(x) = \psi_i(x)$ e ψ è ben definita.

Affermiamo che $(\mathbb{E}_\infty, \psi)$ è maggiorante in X di C. Infatti

1. $\mathbb{E}_\infty$ è un campo perché unione di campi in catena.

2. Per ogni $i \in I$ vale che $\mathbb{K} \subseteq \mathbb{E}_i \subseteq \mathbb{F}$, quindi $\mathbb{K} \subseteq \mathbb{E}_\infty \subseteq \mathbb{F}$.

3. ψ è un omomorfismo, infatti per ogni $x, y \in \mathbb{E}_\infty$ poniamo $x \in E_x, y \in \mathbb{E}_y$. Senza perdita di generalità $\mathbb{E}_x \subseteq \mathbb{E}_y$, da cui $x, y \in \mathbb{E}_y$. Quindi

$$\psi(x+y) = \psi_y(x+y) = \psi(x) + \psi(y)$$
$$\psi(xy) = \psi_y(xy) = \psi(x)\psi(y)$$

4. Per ogni $i \in I$, allora $\psi|_{\mathbb{K}} = \psi_i|_{\mathbb{K}} = \varphi$.

5. Per ogni $i \in I$ otteniamo per definizione $\mathbb{E}_i \subseteq \mathbb{E}_\infty$ e $\psi|_{\mathbb{E}_i} = \psi_i$.

Quindi abbiamo ottenuto che ogni catena non vuota ammette un maggiorante in X, e quindi per il lemma di Zorn X ammette un elemento massimale (F, σ).

L'ultimo passo è dimostrare che $F = \mathbb{F}$. Certamente $F \subseteq \mathbb{F}$. D'altra parte se per assurdo $F \subsetneqq \mathbb{F}$, allora esiste un $\alpha \in \mathbb{F} \setminus F$ e $\mathbb{K} \subseteq F \subsetneqq F(\alpha) \subseteq \mathbb{F}$. Essendo $\mathbb{F}$ algebrico su $\mathbb{K}$ allora l'estensione $F(\alpha)/F$ è anche essa algebrica e, essendo semplice, finita.
Quindi esiste un $\tilde{\sigma} \colon F(\alpha) \hookrightarrow \overline{\mathbb{K}}$ tale che $\tilde{\sigma}|_F = \sigma$. Inoltre $\tilde{\sigma}|_{\mathbb{K}} = \sigma|_{\mathbb{K}} = \varphi$.

Abbiamo quindi ottenuto che $(F(\alpha), \tilde{\sigma}) \in X$. Ma allora $(F, \sigma) \preccurlyeq (F(\alpha), \tilde{\sigma})$, da cui $(F, \sigma) = (F(\alpha), \tilde{\sigma})$. Ciò implica che $F = F(\alpha)$, assurdo.

Quindi abbiamo concluso che $F = \mathbb{F}$, da cui $\sigma \colon \mathbb{F} \hookrightarrow \overline{\mathbb{K}}$ e $\sigma|_{\mathbb{K}} = \varphi$, cioè σ è l'immersione cercata. □

Dimostrato questo possiamo dimostrare il teorema.

Lemma. *Sia $\mathbb{F}/\mathbb{K}$ un'estensione algebrica e sia $\varphi \colon \mathbb{F} \hookrightarrow \overline{\mathbb{K}}$ un immersione tale che $\varphi|_{\mathbb{K}} = id$ e $\varphi(\mathbb{F}) \subseteq \mathbb{F}$. Allora $\varphi(\mathbb{F}) = \mathbb{F}$.*

Dimostrazione. Sia $\alpha \in \mathbb{F}$ e consideriamo il polinomio minimo μ_α. Allora φ agisce sull'orbita $\{\varphi^i(\alpha)\}$ come una permutazione (infatti φ è iniettiva e l'orbita è finita). Allora esiste un $\beta = \varphi^i(\alpha)$ tale che $\varphi(\beta) = \alpha$. □

Teorema. *Sia $\mathbb{F}/\mathbb{K}$ un'estensione algebrica e siano $\{\varphi_i \colon \mathbb{F} \hookrightarrow \overline{\mathbb{K}}\}_{i \in I}$ immersioni tale che $\varphi_i|_{\mathbb{K}} = id$. Allora si definisce chiusura normale di $\mathbb{F}/\mathbb{K}$ come il composto*

$$\tilde{\mathbb{F}} = \prod_{i \in I} \varphi_i(\mathbb{F})$$

Inoltre

1. *La chiusura normale è la più piccola estensione normale su $\mathbb{K}$ che contiene $\mathbb{F}$.*

2. *Se $\mathbb{F}/\mathbb{K}$ è finita allora anche $\tilde{\mathbb{F}}/\mathbb{K}$ è finita.*

Dimostrazione. Dividiamo la dimostrazione nei due punti

1. Dimostriamo innanzitutto che $\tilde{\mathbb{F}}/\mathbb{K}$ è normale. Sia $\sigma\colon \mathbb{F} \hookrightarrow \overline{\mathbb{K}}$ tale che $\sigma|_{\mathbb{K}} = id$. Allora $\sigma(\varphi_i(\mathbb{F})) = (\sigma \circ \varphi_i)(\mathbb{F}) = \varphi_j(\mathbb{F}) \subseteq \tilde{\mathbb{F}}$ per ogni $i \in I$. Quindi $\sigma(\tilde{\mathbb{F}}) \subseteq \tilde{\mathbb{F}}$, cioè $\mathbb{F}/\mathbb{K}$ è normale per i lemma precedente.

   Dimostriamo ora la minimalità. Sia quindi una sovraestensione $\mathbb{E}/\mathbb{K}$ di $\mathbb{F}$ algebrica normale. Allora essendo $\mathbb{E}/\mathbb{K}$ algebrica possiamo estendere un qualsiasi φ_i ad un $\tilde{\varphi}_i \in Aut(\mathbb{E})$. Allora $\varphi_i(\mathbb{F}) \subseteq \tilde{\varphi}_i(\mathbb{E}) = \mathbb{E}$ per ogni $i \in I$, da cui
   $$\tilde{\varphi} = \prod_{i \in I} \varphi_i(\mathbb{F}) \subseteq \mathbb{E}$$

2. Infine è da dimostrare la finitezza. Essendo $\mathbb{F}/\mathbb{K}$ è finito è possibile scrivere $\mathbb{F} = \mathbb{K}(x_1, \dots, x_n)$. Allora $\tilde{\mathbb{F}} = CsP(\mu_{x_1}, \dots, \mu_{x_n})$ che ha grado finito.

□

Teorema Fondamentale dell'Algebra

Andiamo a dimostrare il teorema fondamentale dell'Algebra iniziando innanzitutto con tre lemmi:

Lemma. *Il campo $\mathbb{R}$ non possiede estensioni di grado dispari non banali.*

Dimostrazione. Supponiamo per assurdo che esista un'estensione $\mathbb{F}/\mathbb{R}$ di grado n dispari. Il campo $\mathbb{R}$ ha caratteristica nulla. Quindi per il teorema dell'elemento primitivo esiste un $\alpha \in \mathbb{F}$ tale che $\mathbb{F} = \mathbb{R}(\alpha)$. Sia μ_α il polinomio minimo di α su $\mathbb{R}$. Esso è irriducibile, però è di grado dispari, quindi ammette una radice. Assurdo. □

Lemma. *Il campo $\mathbb{C}$ non ammette estensioni quadratiche.*

Dimostrazione. Sia $\mathbb{F}/\mathbb{C}$ per assurdo un'estensione quadratica. Allora sappiamo che $\mathbb{F} = \mathbb{C}(\sqrt{\gamma})$ con $\gamma \in \mathbb{C}$. Ma in $\mathbb{C}$ è possibile estrarre le radici quadrate, quindi $\sqrt{\gamma} \in \mathbb{C}$ e $\mathbb{F}/\mathbb{C}$ ha grado 1. Assurdo. □

Lemma. *Ogni estensione di grado due $\mathbb{E}/\mathbb{R}$ è della forma $\mathbb{E} = \mathbb{R}(\sqrt{-1}) \sim \mathbb{C}$. Inoltre fissata una chiusura algebrica $\overline{\mathbb{R}}$ di $\mathbb{R}$, esiste un'unica estensione di grado due di $\mathbb{R}$ in $\overline{\mathbb{R}}$.*

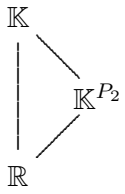
Dimostrazione. Essendo di grado due $\mathbb{E} = \mathbb{R}(\sqrt{\alpha})$. Allora se $\alpha \geq 0$ l'estensione è banale, assurdo. Se $\alpha < 0$ allora $\mathbb{R}(\sqrt{\alpha}) = \mathbb{R}(\sqrt{-1}) \sim \mathbb{C}$.

Fissando la chiusura algebrica si ottiene infine l'unicità. □

Teorema (Teorema Fondamentale dell'Algebra)**.** *Il campo $\mathbb{C}$ è algebricamente chiuso e rappresenta la chiusura algebrica di $\mathbb{R}$.*

Dimostrazione. Supponiamo per assurdo che $\mathbb{C}$ non sia algebricamente chiuso. Quindi esiste un'estensione finita non banale $\mathbb{F}/\mathbb{C}$. Sia inoltre $\mathbb{K}$ la chiusura normale di $\mathbb{F}/\mathbb{R}$. Allora possiamo considerare $G = Gal(\mathbb{K}/\mathbb{R})$ e $H = P_2 \leq G$ un suo 2-Sylow eventualmente banale.

Se si considera allora il seguente diagramma



Si ottiene che $[\mathbb{K}^{P_2} : \mathbb{R}] = |G|/|P_2|$ che è dispari. Quindi per il lemma precedente $\mathbb{K}^{P_2} = \mathbb{R}$ e G è un 2-gruppo.

Allora esistono due catene parallele di estensioni di grado 2.

$$\{e\} = H_0 \subseteq \cdots \subseteq H_{a-2} \subseteq H_{a-1} \subseteq H_a = P_2 = G$$
$$\mathbb{K} \supseteq \cdots \supseteq \mathbb{K}^{H_{a-2}} \supseteq \mathbb{K}^{H_{a-1}} \supseteq \mathbb{R}$$

Essendo $\mathbb{K}^{H_{a-1}}/\mathbb{R}$ di grado due, sappiamo per il lemma precedente che $\mathbb{K}^{H_{a-1}} = \mathbb{C}$. Ma $\mathbb{C}$ non ammette estensioni quadratiche. Quindi la catena si interrompe subito, $G \sim \mathbb{Z}_2$ e $\mathbb{K} = \mathbb{F} = \mathbb{C}$.

Infine $\mathbb{C}$ è la chiusura algebrica di $\mathbb{R}$. Infatti $\mathbb{C}$ è algebricamente chiuso per quello detto prima, $\mathbb{C}/\mathbb{R}$ è algebrica essendo finita. □

Teorema Fondamentale delle Funzioni Simmetriche

Andiamo a parlare delle cosiddette *funzioni simmetriche*, cioè funzioni razionali invarianti sotto permutazioni delle variabili. Notiamo innanzitutto che le permutazioni delle variabili costituiscono un sottogruppo di $Aut(\mathbb{K}(x_1, \ldots, x_n))$, e in particolare l'insieme delle funzioni simmetriche è

$$S(x_1, \ldots, x_n) = \mathbb{K}(x_1, \ldots, x_n)^{S_n}$$

Quindi l'insieme considerato è un sottocampo, essendo l'insieme fissato da un sottogruppo del gruppo degli automorfismi. Quindi possiamo studiare l'oggetto in questione tramite la teoria di Galois. In particolare iniziamo col seguente lemma di supporto:

Lemma. *Sia un'estensione separabile $\mathbb{F}/\mathbb{K}$, tale che ogni elemento di $\mathbb{F}$ ha grado al massimo n su $\mathbb{K}$. Allora $\mathbb{F}/\mathbb{K}$ è semplice e $[\mathbb{F} : \mathbb{K}] \leq n$*

Dimostrazione. Sia l'insieme

$$T = \{[\mathbb{K}(\alpha) : \mathbb{K}] \,|\, \alpha \in \mathbb{F}\} \subseteq \{1, \ldots, n\}$$

Esso ammette un elemento massimo e poniamo $\alpha \in \mathbb{F}$ che realizza tale massimo.

Vogliamo adesso dimostrare che $\mathbb{K}(\alpha) = \mathbb{F}$. Se per assurdo $\mathbb{K}(\alpha) \subsetneq \mathbb{F}$, allora esiste un $\beta \in \mathbb{F} \setminus \mathbb{K}(\alpha)$. Allora possiamo considerare la torre

$$\begin{array}{c} \mathbb{F} \\ | \\ | \\ | \\ \mathbb{K}(\alpha, \beta) \\ | \\ | \\ | \\ \mathbb{K}(\alpha) \\ | \\ | \\ | \\ \mathbb{K} \end{array}$$

Essendo $\mathbb{K}(\alpha)/\mathbb{K}$ e $\mathbb{K}(\beta)/\mathbb{K}$ finite, anche $\mathbb{K}(\alpha, \beta)/\mathbb{K}$ lo è. Quindi per il teorema dell'elemento primitivo $\mathbb{K}(\alpha, \beta) = \mathbb{K}(\gamma)$. Ma $[\mathbb{K}(\gamma) : \mathbb{K}] = [\mathbb{K}(\alpha, \beta) : \mathbb{K}] > n$. Assurdo.

Quindi $\mathbb{F} = \mathbb{K}(\alpha)$ e $[\mathbb{F} : \mathbb{K}] \leq n$. □

A questo punto andiamo a dimostrare un teorema che ci servirà, ma che ha anche importanza a sè.

Teorema (Teorema di Artin)**.** *Sia $\mathbb{F}$ un campo e G un sottogruppo finito di $Aut(\mathbb{F})$. Posto $\mathbb{K} = \mathbb{F}^G$, allora $\mathbb{F}/\mathbb{K}$ è un'estensione di Galois con gruppo di Galois proprio G.*

Dimostrazione. Dimostriamo la separabilità, finitezza e normalità separatamente.

(Separabilità) Sia $\alpha \in \mathbb{F}$, vogliamo dimostrare che μ_α non ha radici multiple in $\overline{\mathbb{K}}$, con μ_α il polinomio minimo di α su $\mathbb{K}$. Per farlo consideriamo il sottogruppo H_α di G dato da

$$H_\alpha = \{\, h \in G \mid h(\alpha) = \alpha \,\}$$

Innanzitutto notiamo che per ogni $g, g' \in G$, $g(\alpha) = g'(\alpha)$ se e solo se $gH_\alpha = g'H_\alpha$. Quindi siano $g_1, \ldots, g_n$ i rappresentanti delle classi laterali di H_α e sia il polinomio

$$F(x) = \prod_{i=1}^{n} (x - g_i(\alpha)) \in \mathbb{F}[x]$$

Allora si osserva subito che

1. $F(x)$ non ha radici multiple. Infatti se esistessero $\gamma \in \mathbb{F}$ e due indici i, j tale che $g_i(\alpha) = \gamma = g_j(\alpha)$, allora $g_i H_\alpha = g_j H_\alpha$. Assurdo per la scelta effettuata.

2. $F(x) \in \mathbb{K}[x]$. Infatti posto $g \in G$, allora $(g \circ g_i)H_\alpha = (g \circ g_j)H_\alpha$ se e solo se $g_i H_\alpha = g_j H_\alpha$. Quindi otteniamo di nuovo tutte e sole le classi laterali di H_α e $(gF)(x) = F(x)$. Valendo per tutti i $g \in G$ si ottiene $F(x) \in \mathbb{K}[x]$.

Quindi $F(x) \in \mathbb{K}[x]$ si annulla in α e non ha radici multiple. Da cui neanche μ_α può averle.

Valendo questo per ogni $\alpha \in \mathbb{F}$ otteniamo che $\mathbb{F}/\mathbb{K}$ è separabile.

(Finitezza) Sia $\alpha \in \mathbb{F}$ e consideriamo il polinomio

$$F_\alpha(x) = \prod_{\sigma \in G} (x - \sigma(\alpha))$$

Come al solito si osserva che $(\sigma F_\alpha)(x) = F_\alpha(x)\ \forall \sigma \in G$ e $F_\alpha(x)$ si annulla in α. Quindi $[\mathbb{K}(\alpha) : \mathbb{K}] \leq |G|$.

Valendo ciò per ogni $\alpha \in \mathbb{F}$, per il lemma precedente $[\mathbb{F} : \mathbb{K}] \leq |G|$.

(Normalità) Tramite il polinomio precedente possiamo anche dimostrare la normalità. Infatti essendo $\mathbb{F}/\mathbb{K}$ finita e separabile è semplice. Quindi esiste un $\alpha \in \mathbb{F}$ tale che $\mathbb{F} = \mathbb{K}(\alpha)$. Ma allora $\mu_\alpha \mid F_\alpha(x)$ e tutte le radici di μ_α appartengono a $\mathbb{F}$.

Quindi $\mathbb{F} = Csp(F_\alpha(x), \mathbb{K})$, cioè $\mathbb{F}/\mathbb{K}$ è normale.

(Gruppo di Galois) Abbiamo quindi dimostrato che $\mathbb{F}/\mathbb{K}$ è un'estensione di Galois. Per dimostrarne il gruppo di Galois notiamo che per costruzione $G \leq Gal(\mathbb{F}/\mathbb{K})$. Inoltre

$$|G| \leq |Gal(\mathbb{F}/\mathbb{K})| = [\mathbb{F} : \mathbb{K}] \leq |G|$$

Quindi $|G| = |Gal(\mathbb{F}/\mathbb{K})|$ e $G = Gal(\mathbb{F}/\mathbb{K})$. □

Quindi abbiamo dimostrato che $\mathbb{K}(x_1, \ldots, x_n)/\mathbb{K}(x_1, \ldots, x_n)^{S_n}$ è un'estensione di Galois con gruppo di Galois S_n. A questo punto possiamo enunciare il teorema delle funzioni simmetriche, andando innanzitutto a definire le cosiddette funzioni simmetriche elementari:

Definizione. *Date n variabili $x_1, \ldots, x_n$ definiamo funzioni simmetriche elementari come:*

$$\begin{aligned}
e_1 &= x_1 + \cdots + x_n \\
e_2 &= x_1x_2 + \ldots x_1x_n + \cdots + x_{n-1}x_n \\
&\cdots \\
e_k &= \sum_{1 \leq i_1 \leq \cdots \leq i_k \leq n} x_{i_1} \ldots x_{i_k}
\end{aligned}$$

Definite queste funzioni andiamo finalmente ad enunciare il nostro teorema:

Teorema (Teorema delle Funzioni Simmetriche)**.** *Per ogni $f \in \mathbb{K}(x_1, \dots, x_n)$ funzione simmetrica esiste $g \in \mathbb{K}(t_1, \dots, t_n)$ tale che $f = g(e_1, \dots, e_n)$*

Dimostrazione. Sia il seguente diagramma di campi

$$\begin{array}{c} \mathbb{K}(x_1, \dots, x_n) = \mathbb{F} \\ | \\ | \\ \mathbb{K}(x_1, \dots, x_n)^{S_n} \\ | \\ | \\ \mathbb{K}(e_1, \dots, e_n) = \mathbb{E} \end{array}$$

Per il teorema di Artin sappiamo che $[\mathbb{F} : \mathbb{K}(x_1, \dots, x_n)^{S_n}] = n!$.

D'altra parte sia $p(t) = (t - x_1) \dots (t - x_n) \in \mathbb{F}[t]$. Allora dalle formule di Viète sappiamo che

$$\begin{aligned} p(t) &= (t - x_1)(t - x_2) \dots (t - x_{n-1})(t - x_n) \\ &= t^n - (x_1 + \cdots + x_n)t^{n-1} + (x_1x_2 + \cdots + x_{n-1}x_n)t^{n-2} + \cdots + (-1)^n x_1 \dots x_n \\ &= t^n - e_1 t^{n-1} + e_2 t^{n-2} + \cdots + (-1)^n e_n \in \mathbb{E}[t] \end{aligned}$$

Quindi otteniamo che

$$\mathbb{F} = \mathbb{K}(x_1, \dots, x_n) = \mathbb{K}(e_1, \dots, e_n)(x_1, \dots, x_n) = CsP(p(t), \mathbb{E})$$

da cui

$$[\mathbb{F} : \mathbb{E}] \leq (\deg(p(t)))! = n!$$

Quindi confrontando il grado ottenuto precedentemente si ottiene che $\mathbb{K}(x_1, \dots, x_n)^{S_n} = \mathbb{K}(e_1, \dots, e_n)$ □

Problema Inverso di Galois

A questo punto ci dedichiamo al cosiddetto problema inverso di Galois, estremamente importante nella matematica odierna e non ancora risolto completamente. Innanzitutto partiamo con la seguente definizione

Definizione. *Dato un gruppo finito G e un campo $\mathbb{K}$, G si dice realizzabile su $\mathbb{K}$ se esiste un'estensione di Galois $\mathbb{F}/\mathbb{K}$ tale che $G \simeq Gal(\mathbb{F}/\mathbb{K})$.*

Il problema inverso di Galois consiste nel dimostrare quali gruppi G siano realizzabile su qualche campo. In questa generalità la risposta è affermativa, vale cioè il teorema

Teorema. *Dato un gruppo finito G esiste sempre un campo $\mathbb{K}$ tale che G è realizzabile su $\mathbb{K}$.*

Dimostrazione. Per il teorema di Cayley sappiamo che esiste un immersione $G \hookrightarrow S_n$ con $n = |G|$. Essendo che per il teorema di Artin $S_n = Gal(\mathbb{K}(x_1, \dots, x_n)/\mathbb{K}(e_1, \dots, e_n))$, allora per il Teorema di Corrispondenza di Galois otteniamo la seguente uguaglianza

$$G = Gal(\mathbb{K}(x_1, \dots, x_n)/\mathbb{K}(x_1, \dots, x_n)^G)$$

□

Essendo la risposta nella generalità sempre vera, di solito con il termine "*Problema Inverso di Galois*" si intende stabilire quali gruppi finiti sono realizzabili su $\mathbb{Q}$. Il problema non è stato ad oggi ancora risolto, ma si congettura che tutti i gruppi finiti siano realizzabili sui razionali. Qua dimostreremo l'affermazione nel caso in cui G sia abeliano. Per farlo ci serve il *teorema delle progressioni aritmetiche di Dirichlet*, che dimostreremo solo in un caso particolare, che è quello che a noi serve.

Iniziamo quindi con questo lemma

Lemma. *Dato un polinomio $f(x) \in \mathbb{Z}[x]$, esistono infiniti primi p per cui $f(x)$ ha una radice in $\mathbb{F}_p$.*

Dimostrazione. Dimostriamo innanzitutto il caso $f(0) = 1$, che implicherà quello generale.

Ovviamente essendo $\mathbb{Q}$ un campo infinito, esiste sicuramente un $K \in \mathbb{Z}$ per cui $f(K) \neq \pm 1$. Prendendo allora $p \mid f(K)$, si ottiene che f ha la radice K in $\mathbb{F}_p$.

Supponiamo per assurdo che esistano solo $p_1, \dots, p_r$ primi tale che $f(x)$ abbia una radice in $\mathbb{F}_{p_i}$.

Notiamo innanzitutto che per ogni $N \in \mathbb{Z}$

$$f(p_1 \dots p_r N) = 1 + (p_1 \dots p_r N)H \equiv 1 \pmod{p_1, \dots, p_r}$$

Essendo $\mathbb{Q}$ un campo infinito, esiste un $N \in \mathbb{Z}$ tale che $f(p_1 \dots p_r N) \neq \pm 1$. Allora posto $p' \mid f(p_1 \dots p_r N)$ primo, ottengo

1. $f(p_1 \dots p_r N) \equiv 0 \pmod{p'}$

2. Se per assurdo $p' = p_i$, allora $f(p_1 \dots p_r N) \equiv 1 \pmod{p_1, \dots, p_r} \Rightarrow f(p_1 \dots p_r N) \equiv 1 \pmod{p'}$. Assurdo.

Quindi $f(x)$ ha una radice in $\mathbb{F}_{p'}$ e $p' \notin \{p_1, \dots, p_r\}$. Assurdo perché avevamo supposto che erano gli unici.

Possiamo allora concludere che esistono infiniti primi p per cui $f(x)$ ha una radice in $\mathbb{F}_p$.

Dimostriamo adesso il caso generale.

Sia quindi $f(x) \in \mathbb{Z}[x]$. Se $f(0) = 0$, allora f ha una radice in ogni $\mathbb{F}_p$. Altrimenti consideriamo il polinomio

$$g(x) = \frac{f(xf(0))}{f(0)} \in \mathbb{Z}[x] \tag{1}$$

Il polinomio g ha termine noto unitario, quindi l'insieme

$$P = \{\, p \text{ primo} \mid g(x) \text{ ha una radice in } \mathbb{F}_p \,\}$$

è infinito. Sia allora l'insieme ovviamente finito

$$T = \{\, p \text{ primo} \mid p \mid f(0) \,\}$$

L'insieme $P \setminus T$ è infinito, e per ogni $p \in P \setminus T$ possiamo portare la divisione (1) in $\mathbb{F}_p$. Possiamo quindi affermare che per ogni $p \in P \setminus T$ esiste un $x_p \in \mathbb{F}_p$ tale che

$$f(x_p f(0))[f(0)]^{-1} \equiv 0 \pmod{p}$$

cioè

$$f(x_p f(0)) \equiv 0 \pmod{p}$$

Quindi per ogni $p \in P \setminus T$, $f(x)$ ha una radice in $\mathbb{F}_p$. □

A questo punto possiamo dimostrare il teorema di Dirichlet nel caso di interesse.

Teorema (Teorema delle Progressione Aritmetiche di Dirichlet)**.** *Dati $a, q \in \mathbb{Z}$ coprimi, allora l'insieme*

$$\{\, a + qn \mid n \in \mathbb{Z} \,\}$$

contiene infiniti numeri primi.

Dimostrazione. (a = 1)
Consideriamo il polinomio ciclotomico primitivo q-esimo $\Phi_q \in \mathbb{Z}[x]$ e il polinomio

$$g(x) = \prod_{\substack{k \mid q \\ k < q}} (x^k - 1)$$

Per costruzione $(g(x), \Phi_q) = 1$, cioè esistono $u(x), v(x) \in Q[x]$ tale che

$$u(x)\Phi_q(x) + v(x)g(x) = 1$$

Possiamo quindi moltiplicare per il comun denominatore D e ottenere $U(x), V(x) \in \mathbb{Z}[x]$ tale che

$$U(x)\Phi_q + V(x)g(x) = D$$

A questo punto per il lemma precedente esistono infiniti primi per cui Φ_q ha una radice, e a meno di sottrarre un insieme finito, possiamo supporre che questi primi non dividano D. Allora otteniamo che per ogni p considerato esiste un $n \in \mathbb{Z}$ tale che

$$V(n)g(n) \equiv D \not\equiv 0 \pmod{p} \;\Rightarrow\; g(n) \not\equiv 0 \pmod{p}$$

cioè esiste un $n \in \mathbb{Z}$ tale che

$$\begin{cases} n^q - 1 \equiv \prod_{d|q} \Phi_d(n) \equiv 0 \pmod{p} \\ \prod_{\substack{k|q \\ k<q}} (n^d - 1) \equiv g(n) \not\equiv 0 \pmod{p} \end{cases}$$

Da cui

$$\begin{cases} n^q \equiv 1 \pmod{p} \\ n^d \not\equiv 1 \pmod{p} \; \forall d < q, d \mid q \end{cases}$$

che implica $ord_p(n) = q \mid p-1$, da cui $p \equiv 1 \pmod{q}$.

Abbiamo quindi dimostrato che esistono infiniti primi per cui $p \equiv 1 \pmod{q}$, che era il nostro obiettivo. □

Con il teorema di Dirichlet possiamo finalmente risolvere il problema inverso di Galois abeliano.

Teorema. *Ogni gruppo abeliano finito G è realizzabile su $\mathbb{Q}$.*

Dimostrazione. Notiamo innanzitutto che ogni gruppo abeliano può essere scomposto in prodotto diretto di p-gruppi.

$$G \simeq G(p_1) \times \cdots \times G(p_r)$$

Quindi se troviamo $\mathbb{F}_1, \ldots, \mathbb{F}_r$ tale che $\mathbb{F}_i/\mathbb{Q}$ è di Galois e $G(p_i) \simeq Gal(\mathbb{F}_i/\mathbb{Q})$, allora $(\mathbb{F}_1 \ldots \mathbb{F}_r)/\mathbb{Q} = \mathbb{F}/\mathbb{Q}$ è di Galois e $G \simeq Gal(\mathbb{F}/\mathbb{Q})$. Infatti i p-gruppi sono a due a due coprimi, e quindi le estensioni relative hanno intersezioni due a due banali.

Quindi ci siamo ricondotti a studiare il caso in cui G è un p-gruppo.

In questa situazione G si può scomporre come

$$G \simeq \mathbb{Z}_{p^{r_1}} \times \cdots \times \mathbb{Z}_{p^{r_t}} \quad r_1 \geq \cdots \geq r_t$$

Innanzitutto dobbiamo realizzare i gruppi ciclici $\mathbb{Z}_{p^{r_1}}, \ldots, \mathbb{Z}_{p^{r_t}}$, e per farlo sfruttiamo il teorema delle progressioni aritmetiche di Dirichlet. Infatti grazie ad esso sappiamo che esistono $q_1, \ldots, q_t$ primi distinti tale che $q_i \equiv 1 \pmod{p^{r_i}}$. Inoltre sappiamo che l'estensione $\mathbb{Q}(\zeta_{q_i})/\mathbb{Q}$ è di Galois e $Gal(\mathbb{Q}(\zeta_{q_i})/\mathbb{Q}) \simeq \mathbb{Z}_{q_i}^* \simeq \mathbb{Z}_{q_i-1}$.

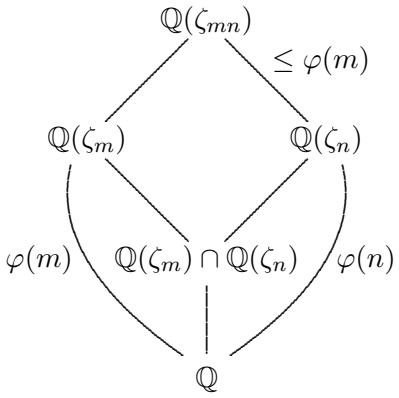
Nel gruppo $\mathbb{Z}_{q_i-1}$ è presente un sottogruppo H_i normale di ordine

$$|H_i| = \frac{q_i - 1}{p^{r_i}}$$

Quindi l'estensione $\mathbb{K}_i/\mathbb{Q} = \mathbb{Q}(\zeta_{q_i})^{H_i}/\mathbb{Q}$ è di Galois, con gruppo di Galois

$$Gal(\mathbb{K}_i/\mathbb{Q}) \simeq \frac{\mathbb{Z}_{q_i-1}}{H_i} \simeq \mathbb{Z}_{p^{r_i}}$$

Quindi abbiamo realizzato i gruppi ciclici, dobbiamo solamente realizzare il relativo prodotto diretto. Per farlo notiamo che se m, n sono interi coprimi, allora $\mathbb{Q}(\zeta_{mn}) = \mathbb{Q}(\zeta_m, \zeta_n)$. Da questo è immediato che se m, n sono interi coprimi, allora $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$. Infatti possiamo considerare il seguente diagramma



Essendo che $[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] = \varphi(mn) = \varphi(m)\varphi(n)$, è ovvio che $[\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}] = 1$.

Ma allora possiamo tornare a quanto detto precedentemente. Essendo che $q_1, \ldots, q_r$ sono primi distinti, allora $\mathbb{Q}(\zeta_{q_i}) \cap \mathbb{Q}(\zeta_{q_j}) = \mathbb{Q}$, da cui $\mathbb{K}_i \cap \mathbb{K}_j = \mathbb{Q}$. Quindi possiamo concludere che $(\mathbb{K}_1 \ldots \mathbb{K}_t)/\mathbb{Q}$ è di Galois e

$$Gal((\mathbb{K}_1 \ldots \mathbb{K}_t)/\mathbb{Q}) \simeq Gal(\mathbb{K}_1/\mathbb{Q}) \times \cdots \times Gal(\mathbb{K}_t/\mathbb{Q}) \simeq \mathbb{Z}_{p^{r_1}} \times \cdots \times \mathbb{Z}_{p^{r_t}} \simeq G$$

cioè G è realizzabile su $\mathbb{Q}$. □

Quindi abbiamo dimostrato che tutti i gruppi abeliani finiti sono realizzabili su $\mathbb{Q}$.

Per quanto riguarda la questione più in generale, il teorema di irriducibilità di Hilbert implica che per realizzare un gruppo su $\mathbb{Q}$ è sufficiente realizzarlo su $\mathbb{Q}(x_1, \ldots, x_n)$. Da questo si può dimostrare che tutti i gruppi simmetrici e alterni sono realizzabili su $\mathbb{Q}$.

Inoltre tutti i gruppi semplici, ad eccezione del gruppo di Mathieu M_{23}, sono stati realizzati su $\mathbb{Q}$.

Infine è stato dimostrato [Igor' Sfarevic, 1954] che tutti i gruppi risolubili sono realizzabili su un'estensione di $\mathbb{Q}$.