

COLLOQUIO

Andrea Gallese - 15 aprile 2019

INTRODUZIONE

Di che cosa parleremo? Vogliamo introdurre un comodo strumento per parlare di problemi che sono in qualche modo naturalmente collegati ad estensioni di campi. In particolare ci concentreremo su alcuni risultati nella direzione del problema di Galois inverso nel caso abeliano.

Esempio 0. Per avere un'idea di quello che abbiamo in mente, iniziamo con un esempio banalissimo. Una domanda che ha qualche interesse porsi è: chi sono i quadrati in un dato campo K (finito)? Ovvero, cosa sappiamo dire sulla mappa

$$K^\times \xrightarrow{\cdot 2} K^\times?$$

Questo problema è banale quando K è algebricamente chiuso:

$$0 \longrightarrow \mu_2 \longrightarrow K^\times \xrightarrow{\cdot 2} K^\times \longrightarrow 0.$$

Siamo allora tentati di sollevare il problema alla chiusura algebrica, risolverlo, e dopodiché capire quali proprietà si conservano nel discendere alle sotto-estensioni. A questo punto è naturale prendere in considerazione il funtore $A \mapsto A^{\text{Gal}(\bar{K}/K)}$.

Lo strumento. Il nostro funtore è esatto a sinistra; l'algebra omologia fornisce un modo naturale di far proseguire la successione esatta: il funtore derivato a destra: $H^i(G, \bullet)$. Ci sono due modi per costruirlo: magia nera ($H^i(G, \bullet) := R^i F(\bullet)$) oppure sudore e sangue

$$K^i(A) = \{f: G^i \rightarrow A\}, \quad \delta^i(f)(g_1, \dots, g_{i+1}) = \sum_{j=0}^{i+1} (-1)^j (\bullet_0 f(\bullet_1, \dots, \bullet_i)) (\partial_j(1, g_0, \dots, g_i, 1))$$

Il secondo ci torna utile nel caso di azione banale: qui $H^1(G, A) = \text{Hom}(G, A)$.

PERCHÉ CI PIACE?

L'obiettivo diventa ora convincere il pubblico che, fatta la scelta naturale, abbiamo pure ottenuto un buon linguaggio: alcuni vecchi teoremi trovano piacevoli riformulazioni, ne è un esempio l'Hilbert 90 che guadagna un ruolo centrale nella teoria.

■ **Teorema 1** (Hilbert 90). *Data un'estensione L/K di Galois di gruppo G , si ha che: $H^1(G, L^\times)$.*

Dimostrazione. Mostriamo che tutti i cocicli sono cobordi: prendiamo un cociclo $a: G \rightarrow L^\times$, gli elementi di G sono linearmente indipendenti su L , quindi troviamo $x \in L^\times$ per cui

$$y = \sum_{g \in G} a_g g(x) \neq 0.$$

Ma $hy = a_h^{-1}y$ per ogni $h \in G$, da cui la tesi. □

Inoltre, alcuni risultati stranoti si ripresentano in forme sorprendentemente semplici, per dire:

► **Lemma 2.** *Parametrizzazione della circonferenza unitaria usando $H^1(G, \mathbb{Q}(i)^\times) = 0$.*

Dimostrazione. Essendo G è ciclico, abbiamo

$$\frac{\ker N}{I_G \mathbb{Q}(i)^\times} = \hat{H}^{-1}(G, \mathbb{Q}(i)^\times) = H^1(G, \mathbb{Q}(i)^\times) = 0.$$

□

Ma il problema di Galois inverso? Ah, sì! Fissato un gruppo abeliano A , le estensioni di Galois di gruppo A (abeliano!) sono classificate da

$$\mathrm{Hom}(G, A) = H^1(G, A).$$

Una conseguenza del poco detto fino ad ora è, per esempio:

■ **Teorema 3** (Kummer). *Le estensioni di Galois di gruppo $\mathbb{Z}/p\mathbb{Z}$ su un campo K che contiene le radici p -esime dell'unità μ_p sono classificate da $K^\times/K^{\times p}$.*

Dimostrazione. Partiamo dalla solita

$$0 \longrightarrow \mu_p \longrightarrow \bar{K}^\times \xrightarrow{\cdot p} \bar{K}^\times \longrightarrow 0,$$

che diventa, per Hilbert 90,

$$0 \longrightarrow \mu_p \longrightarrow K^\times \xrightarrow{\cdot p} K^\times \longrightarrow H^1(G, \mu_p) \longrightarrow 0,$$

che, per quanto detto sopra, è la tesi. □

ALTRI ORIZZONTI

Dualità di Pontryagin. Il duale di un gruppo G è definito come

$$G^\vee = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}),$$

il suo biduale sarà $(G^\vee)^\vee = G^{\mathrm{ab}}$. Questo assomiglia in qualche modo alla definizione di duale per spazi vettoriali: vale la pena di osservare che la dualità è equivalente ad avere un accoppiamento perfetto

$$A \times B \rightarrow \mathbb{Q}/\mathbb{Z}.$$

Dualità di Tate. Abbiamo un accoppiamento perfetto

$$H^1(G, M) \times H^1(G, M') \rightarrow H^2(G, \bar{K}^\times),$$

dove $M' = \mathrm{Hom}(M, \mu_\infty)$.

Una volta scoperto che $H^2(G, \bar{K}^\times) = \mathbb{Q}/\mathbb{Z}$, ci basterà porre $M = \mathbb{Q}/\mathbb{Z}$ per scoprire che le due dualità sono la stessa e concludere quindi che

$$G^{\mathrm{ab}} = H^1(G, M)^\vee = H^1(G, \mu_\infty) = \varprojlim H^1(G, \mu_n) = \varprojlim K^\times / K^{\times n}.$$