Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Mario Girardi, Giorgio Israel

Una caratterizzazione degli ampliamenti galoisiani

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **58** (1975), n.4, p. 494–498.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1975_8_58_4_494_0>

Algebra. — *Una caratterizzazione degli ampliamenti galoisiani.* Nota di MARIO GIRARDI e GIORGIO ISRAEL (*), presentata (**) dal Socio B. SEGRE.

SUMMARY. — This paper deals with a characterization of arbitrary Galois extensions generalizing a well known characterization of algebraic Galois extensions.

1. È noto che, se k e K sono due campi e K è un ampliamento algebrico di k, allora K è un ampliamento galoisiano di k se, e soltanto se, K è quasi galoisiano e separabile su k (v. [1], Cap. V, § 10, Prop. 1. e [2], Teor. III.5). In questo lavoro risolveremo il problema della generalizzazione di questo teorema al caso di un ampliamento qualsiasi.

Si noti che, mentre le definizioni di ampliamento galoisiano e di ampliamento separabile sono ben note nel caso di un ampliamento qualsiasi, la nozione di ampliamento quasi galoisiano viene usualmente introdotta soltanto nel caso algebrico; occorrerà pertanto estendere in modo opportuno quest'ultima nozione al caso di un ampliamento qualsiasi. Dimostreremo che, se K è un ampliamento galoisiano di k, allora K è separabile su k ed ogni polinomio irriducibile di $k[X]$ avente una radice in K si spezza in fattori lineari su K (Teor. 1); tale risultato non è tuttavia invertibile, come mostreremo con un esempio. Viceversa, generalizzata in modo spontaneo la definizione di ampliamento quasi galoisiano quale viene data nel caso algebrico, richiedendo che un ampliamento K di un campo k contenga tutti i coniugati su k di ogni suo elemento in un campo algebricamente chiuso Ω contenente K (v. [1], Cap. V, § 6, n. 2), proveremo che, se K soddisfa questa condizione (ampliamento stabile) ed è separabile su k, allora è galoisiano su k (Teor. 2). Anche questo risultato non è invertibile, come mostreremo con un esempio. La caratterizzazione cercata si otterrà, infine, imponendo una condizione più debole della stabilità, ma che coincide con essa nel caso algebrico (Teor. 3 e 4).

Dimostreremo inoltre che, se il grado di trascendenza di K su k è finito ($\mathrm{tr}\ K/k < \infty$), K è stabile su k se, e soltanto se, ogni k–monomorfismo di K in Ω è un k–automorfismo; proveremo anche che questa caratterizzazione non è valida se si omette la condizione $\mathrm{tr}\ K/k < \infty$. Infine, otterremo un'altra dimostrazione del Teor. 2 nel caso in cui K sia finitamente generato su k (campo di funzioni algebriche), estendendo la tecnica dimostrativa relativa al caso algebrico.

(*) Lavoro eseguito nell'ambito del Gruppo Nazionale per le Strutture Algebriche e Geometriche e loro Applicazioni del C.N.R.

(**) Nella seduta del 12 aprile 1975.

2. Premettiamo alcune notazioni e definizioni. Se K è un ampliamento di un campo k, denoteremo col simbolo $G(K/k)$ il gruppo di Galois di K su k; se G è un gruppo di automorfismi di K, denoteremo con K^G il sottocampo formato dagli elementi di K che rimangono fissi in ogni automorfismo di G.

D'ora in poi, con il simbolo Ω indicheremo un ampliamento algebricamente chiuso del campo k. Sia K un ampliamento di k contenuto in Ω. Ricordiamo che K dicesi *ampliamento galoisiano* di k se $k = K^{G(K/k)}$. Inoltre, K dicesi *ampliamento separabile* di k se k è di caratteristica zero oppure, essendo k di caratteristica $p \neq 0$, K risulta linearmente disgiunto da $k^{p^{-\infty}} = \Omega^{G(\Omega/k)}$ su k [v. [1], Cap. V, § 8, n. 1 e 2).

Diremo che K è un *ampliamento stabile* di k se, per ogni $x \in K$, tutti i suoi coniugati su k in Ω, appartengono a K. Infine, diremo che K è un *ampliamento quasi galoisiano* di k se $K^{G(K/k)} \subset \Omega^{G(\Omega/k)}$.

LEMMA. *K è stabile su k se, e soltanto se, la restrizione a* K *di ogni k-automorfismo di* $G(\Omega/k)$ *appartiene a* $G(K/k)$.

Dimostrazione. Se K è stabile e $\varphi \in G(\Omega/k)$, essendo la restrizione $\varphi|_K$ un k-monomorfismo di K in Ω, essa risulta un k-endomorfismo di K. Inoltre, $\varphi|_K$ è surgettivo; infatti, se esistesse un $x \in K - \varphi(K)$, x avrebbe un coniugato non appartenente a K. Il viceversa è ovvio.

3. TEOREMA 1. *Se* K *è un ampliamento galoisiano di k, allora* K *è separabile su k ed ogni polinomio irriducibile di k* [X] *avente una radice in* K *si spezza in fattori lineari su* K.

Dimostrazione. Per dimostrare che K è separabile su k, occorre dimostrare che K e $k^{p^{-1}}$ sono linearmente disgiunti su k; cioè che, se gli elementi $x_1, \cdots, x_n \in k^{p^{-1}}$ sono linearmente indipendenti su k, essi lo sono anche su K. Supponiamo, per assurdo, che $x_1, \cdots, x_n$ siano linearmente indipendenti su k e linearmente dipendenti su K, con n minimo. Consideriamo $K^{p^{-1}}$, il quale contiene $k^{p^{-1}} . K^{p^{-1}}$ è algebrico su K, per cui ogni $\varphi \in G(K/k)$ può essere prolungato ad un elemento di $G(K^{p^{-1}}/k)$. Inoltre, se $\Psi \in G(K^{p^{-1}}/k)$, allora $\Psi(k^{p^{-1}}) = k^{p^{-1}}$; difatti, se $x \in k^{p^{-1}}$, $\Psi(x^p) = (\Psi(x))^p$, da cui $\Psi(x) \in k^{p^{-1}}$. Sia $a_1 x_1 + \cdots + a_n x_n = 0$ una relazione di dipendenza lineare su K ($a_i \in K$) e supponiamo – come non è restrittivo – che $a_1 \neq 0$. Moltiplicando per a_1^{-1} si ottiene la relazione $x_1 + b_2 x_2 + \cdots + b_n x_n = 0$ ($b_i \in K$), ove almeno uno dei b_i non appartiene a k. Si consideri un $\varphi \in G(K/k)$ tale che il suo prolungamento a $K^{p^{-1}}$ non fissi gli elementi $b_i \notin k$. Continuando a chiamare tale prolungamento φ, si ottiene:

$$\varphi(x_1 + b_2 x_2 + \cdots + b_n x_n) = x_1 + \varphi(b_2) x_2 + \cdots + \varphi(b_n) x_n = 0.$$

Sottraendo la relazione così ottenuta dalla relazione di dipendenza lineare degli x_i, si ottiene:

$$(b_2 - \varphi(b_2)) x_2 + \cdots + (b_n - \varphi(b_n)) x_n = 0 \ ,$$

ove almeno uno dei coefficienti è non nullo: il che è assurdo perché n è minimo.

Dimostriamo la seconda parte del teorema. Se $x \in K$ è algebrico su k e e $x_1, \cdots, x_r$ ($x_1 = x$) sono tutte le immagini distinte di x in tutti i k–automorfismi di $G(K/k)$, allora $x_1, \cdots, x_r$ sono coniugati di x su k, in quanto ogni k–automorfismo di K può essere prolungato ad un k–automorfismo di Ω (v. [1] Cap. V, § 6, n. 1, Cor. 1). Ogni x_i è quindi radice del polinomio minimo, $f(X)$, di x su k e $r \leq \partial f(X)$. I coefficienti del polinomio $g(X) = (X - x_1) \cdots \cdots (X - x_r)$ appartengono a K; ma ogni $\varphi \in G(K/k)$ permuta tra loro gli x_i, per cui i coefficienti di $g(X)$ appartengono a K^G, cioè a k. Poichè $f(X)$ e $g(X)$ hanno in comune la radice x, $f(X)$ divide $g(X)$; ma $\partial g(X) \leq \partial f(X)$ e perciò $f(X) = g(X)$. Pertanto $f(X)$ si spezza in fattori lineari su K.

Il Teor. 1 non è invertibile, come mostra il seguente esempio. Sia k un campo finito avente q elementi e sia $K = k(X)$ il campo delle funzioni razionali in una indeterminata. K è separabile su k ed inoltre gli unici polinomi irriducibili di $k[X]$ aventi una radice in K sono i polinomi lineari. Tuttavia K non è galoisiano su k, perché

$$K^{G(K/k)} = k(Y) \quad , \quad \text{ove} \quad Y = \frac{(X^{q^2} - X)^{q+1}}{(X^q - X)^{q^2+1}}$$

(v. [4], p. 230, esempio 2).

TEOREMA 2. *Se* K *è un ampliamento stabile e separabile di* k, *allora* K *è galoisiano su* k.

Dimostrazione. Per la separabilità di K, $Kk^{p^{-\infty}} \cong K \otimes_k k^{p^{-\infty}}$, da cui segue che $K \cap k^{p^{-\infty}} = k$. È sufficiente mostrare che $K^{G(K/k)} \subset k^{p^{-\infty}}$: ne seguirà che $K^{G(K/k)} \subset k$, onde la tesi. Sia $x \in K^{G(K/k)}$ e $\varphi \in G(\Omega/k)$. Essendo K stabile, risulta $\varphi(K) = K$ (v. Lemma) e $\varphi|_K \in G(K/k)$. Pertanto, siccome $\varphi|_K(x) = x$, si ha che $\varphi(x) = x$. Perciò x è fisso in ogni $\varphi \in G(\Omega/k)$ e quindi $x \in k^{p^{-\infty}}$. Il teorema è immediato, se k è di caratteristica zero.

Anche il Teor. 2 non è invertibile, come mostra il seguente esempio. Se **C** è il campo complesso, il campo delle funzioni razionali $\mathbf{C}(X)$ è galoisiano su **C**. $\mathbf{C}(X)$ è separabile su **C**, ma non è stabile. Difatti, posto $\Omega = \overline{\mathbf{C}(X)}$ (chiusura algebrica di $\mathbf{C}(X)$), le radici del polinomio $Y^2 - X$ sono coniugate di X su **C**, perché trascendenti su **C**, ma non appartengono a $\mathbf{C}(X)$.

Dimostriamo ora la preannunciata caratterizzazione degli ampliamenti galoisiani.

TEOREMA 3. *Il campo* K *è un ampliamento galoisiano di* k *se, e soltanto se, esso è quasi galoisiano e separabile su* k.

Dimostrazione. Se il campo K è galoisiano su k, esso è separabile (Teor. 1). Inoltre, $K^{G(K/k)} = k \subset \Omega^{G(\Omega/k)}$.

Viceversa, se K è separabile e $K^{G(K/k)} \subset \Omega^{G(\Omega/k)}$, K è galoisiano su k, come risulta dalla dimostrazione del Teor. 2.

La dimostrazione del Teor. 2 mostra che un ampliamento stabile è quasi galoisiano. Il viceversa non è vero in generale, ma lo è nel caso di un amplia-

mento algebrico, a norma del teorema successivo. Ne segue che la nostra definizione di ampliamento quasi galoisiano si riduce a quella consueta, nel caso algebrico (v. [1], Cap. V, § 6, n. 3), e che il Teor. 3 è un'effettiva generalizzazione del teorema noto nel caso algebrico.

TEOREMA 4. *Un ampliamento algebrico* K *di* k *è stabile se, e soltanto se,* $K^{G(K/k)} \subset \Omega^{G(\Omega/k)}$.

Dimostrazione. Basta dimostrare la sufficienza. Sia $x \in K$ e siano $x_1, \cdots, x_r$ ($x_1 = x$) le immagini distinte di x nei vari k-automorfismi di $G(K/k)$. Consideriamo il polinomio $g(X) = (X - x_1) \cdots (X - x_r)$; siccome ogni $\varphi \in G(K/k)$ permuta fra loro gli x_i, i coefficienti di $g(X)$ appartengono a $K^{G(K/k)}$. Ne segue che $g(X)$ è invariante per ogni k-automorfismo di $G(\Omega/k)$, per cui $x_1, \cdots, x_r$ sono tutti i coniugati di x su k in Ω.

4. Si può dare la seguente caratterizzazione degli ampliamenti stabili di grado di trascendenza finito.

TEOREMA 5. *Se* K *è un ampliamento di* k *tale che* $\operatorname{tr} K/k < \infty$, *allora* K *è stabile su* k *se, e soltanto se, ogni* k*-monomorfismo di* K *in* Ω *è un* k*-automorfismo di* K.

Dimostrazione. Sia K stabile su k. Se φ è un k-monomorfismo di K in Ω, φ può essere prolungato ad un k-automorfismo di Ω (v. [1], Cap. V, § 6, n. 1, Cor. 2). Siccome $\varphi(K) = K$, si ha che $\varphi \in G(K/k)$.

Viceversa, se $x \in K$ e $y \in \Omega$ è un suo coniugato su k, esiste un $\varphi \in G(\Omega/k)$ tale che $\varphi(x) = y$. La restrizione $\varphi|_K$ è un k-monomorfismo di K in Ω ed essendo essa, per ipotesi, un k-automorfismo di K, si ha che $y \in K$.

Si noti che la necessità dell'asserto può essere provata soltanto nel caso in cui $\operatorname{tr} K/k < \infty$, e ciò dipende dal fatto che, nel caso generale, un k-monomorfismo di K in Ω non può essere sempre prolungato ad un k-automorfismo di Ω. Difatti, il seguente esempio mostra l'impossibilità di generalizzare il Teor. 5 al caso di un ampliamento qualsiasi. **C** è un ampliamento stabile di **Q**; ma esiste un'infinità di **Q**-monomorfismi di **C** in sé, su sottocampi distinti da **C** (v. [1], Cap. V, § 6, n. 3, esempio 1).

5. Concludiamo con una diversa dimostrazione del Teor. 2, nel caso in cui K sia un ampliamento finitamente generato di k.

È sufficiente dimostrare che $K^{G(K/k)} \subset k$. Se $x \in K^{G(K/k)}$, x non può essere trascendente su k. Difatti, se $y \in \Omega$ è trascendente su k e $y \neq x$, esiste un $\varphi \in G(\Omega/k)$ tale che $\varphi(x) = y$ e φ può essere ristretto ad un k-monomorfismo di K in Ω che subordina un isomorfismo fra $k(x)$ e $k(y)$ e che è un k-automorfismo di K; quindi x non è fisso in questo k-automorfismo. Sia $x \in K^{G(K/k)}$ e B denoti una base di trascendenza separante di K su k. Si ha che $k(B)(x) \supset \supset k(B)$ ed è un ampliamento algebrico. Se Ψ è un $k(B)$-monomorfismo di

$k(B)(x)$ in Ω, Ψ' può essere prolungato ad un k–monomorfismo di K in Ω. Essendo K stabile, $\Psi' \in G(K/k)$. Siccome $\Psi'(x) = x$, $[k(B)(x) : k(B)] = [k(B)(x) : k(B)]_s = 1$, cioè $x \in k(B)$ e quindi $x \in k$.

BIBLIOGRAFIA

[1] N. BOURBAKI (1959) – *Algèbre*, Cap. IV e V, Paris, Hermann.
[2] M. GIRARDI e G. ISRAEL – *Teoria dei campi*, Feltrinelli (in corso di stampa).
[3] N. JACOBSON (1964) – *Lectures in abstract algebra*, vol. III. Princeton, Van Nostrand.
[4] S. LANG (1965) – *Algebra* (Addison–Wesley Publ. Company).