Corso:Algebra IV I1/Risoluzione di radicali/Inverso del teorema di risoluubilità per radicali

1 Riepilogo

Sia $M \supseteq K$ un'estensione di grado finito, e indichiamo con $g_1, \ldots, g_n$ gli elementi di $\mathcal{G}(M/K)$. Allora, dato $\alpha \in M$, definiamo rispettivamente la traccia e la norma di α in questo modo:

$$t(\alpha) := \alpha^{g_1} + \alpha^{g_2} + \cdots + \alpha^{g_n}$$
$$n(\alpha) = \alpha^{g_1} * \alpha^{g_2} * \cdots * \alpha^{g_n}.$$

Osserviamo che $t(\alpha), n(\alpha) \in K$, $t(\alpha+\beta) = t(\alpha) + t(\beta)$, $n(\alpha\beta) = n(\alpha) * n(\beta)$, e per $a \in K$, $t(a) = na$ e $n(a) = a^n$, infine la traccia è suriettiva nel caso di campi di caratteristica 0. Abbiamo dimostrato anche che se $a \in K, \alpha \in M$, allora

$$t(a\alpha) = a * t(\alpha).$$

2 Automorfismi linearmente indipendenti

Definizione 3.9

Sia K un campo, e siano $\sigma_1, \ldots, \sigma_n$ automorfismi di K . Diciamo che $\sigma_1, \ldots, \sigma_n$ sono *linearmente indipendenti* se la scrittura

$$a_1 x^{\sigma_1} + a_2 x^{\sigma_2} + \cdots + a_n x^{\sigma_n} = 0,\ \forall x \in K,\ a_1, \ldots, a_n \in K$$

implica $a_1 = a_2 = \cdots = a_n = 0$.

Lemma 3.5

Sia K un campo, ogni insieme finito di automorfismi distinti di K è linearmente indipendente.

Dimostrazione

Supponiamo di avere n automorfismi di K , $\sigma_1, \sigma_2, \ldots, \sigma_n$, con $\sigma_i \neq \sigma_j$ se $i \neq j$, e supponiamo per assurdo che siano linearmente dipendenti. Tra tutte le relazioni

di dipendenza lineare di $\sigma_1, \ldots, \sigma_n$, ne scegliamo una con il massimo numero di coefficienti a_i uguali a 0.

A meno di riordinare, posso supporre che valga

$$a_1 x^{\sigma_1} + a_2 x^{\sigma_2} + \cdots + a_r x^{\sigma_r} = 0, \forall x \in K,\ a_i \neq 0\ \forall i = 1, \ldots, r \text{ formula 1.}$$

Se fosse $r = 1$, si avrebbe $a_1 x^{\sigma_1} = 0,\ \forall x$, ma questo non può avvenire (ad esempio, la relazione non vale per $x = 1$, perché $a_1 \neq 0$ e $x^{\sigma_1} = 1 \neq 0$). Allora $r \geq 2$.

Per ipotesi, $\sigma_1 \neq \sigma_2$, allora esiste $b \in K$ tale che $b^{\sigma_1} \neq b^{\sigma_2}$. La formula 1 rimane valida se sostituisco x con bx ($b \neq 0$ e quando x varia in K , bx descrive tutto K). Allora ottengo:

$$a_1 (bx)^{\sigma_1} + a_2 (bx)^{\sigma_2} + \cdots + a_r (bx)^{\sigma_r} = 0, \forall x \in K$$

ed esplicitando i prodotti

$$a_1 b^{\sigma_1} x^{\sigma_1} + a_2 b^{\sigma_2} x^{\sigma_2} + \cdots + a_r b^{\sigma_r} x^{\sigma_r} = 0,\ \forall x \in K \text{ formula 2}$$

Posso moltiplicare la formula 1 per b^{σ_1} , e ottengo:

$$a_1 b^{\sigma_1} x^{\sigma_1} + a_2 b^{\sigma_1} x^{\sigma_2} + \cdots + a_r b^{\sigma_1} x^{\sigma_r} = 0,\ \forall x \in K, \text{formula 3}$$

Se sottraggo la formula 3 alla formula 2 ottengo

$$a_2 (b^{\sigma_2} - b^{\sigma_1}) * x^{\sigma_2} + a_3 (b^{\sigma_3} - b^{\sigma_1}) x^{\sigma_3} + \cdots + a_r (b^{\sigma_r} - b^{\sigma_1}) x^{\sigma_r} = 0, \forall x \in K$$

e questa è una relazione di dipendenza lineare degli automorfismi di lunghezza minore del minimo, assurdo!

(notare che $b^{\sigma_2} - b^{\sigma_1} \neq 0$)

Osservazione 3.6

Sia $M \supseteq K$ un'estensione normale di grado finito, $G = \mathcal{G}(M/K) = \{g_1, \ldots, g_n\}$. Per $x \in M$, $t(x)$ è una combinazione lineare di $g_1, \ldots, g_n$, con tutti i coefficienti uguali a 1.

Siccome per il lemma $g_1, \ldots, g_n$ sono linearmente indipendenti, non si può avere $t(x) = 0,\ \forall x \in M$. Allora esiste $\alpha \in M$, tale che $t(\alpha) = c \neq 0$.

Dato $b \in K$, pongo $\beta := bc^{-1}\alpha$. Allora

$$t(\beta) = bc^{-1} t(\alpha) = b.$$

ovvero **la traccia è suriettiva**.

3 Elementi di traccia nulla

Proposizione 3.4

Sia $M \supseteq K$ un'estensione normale, con $\mathcal{G}(M/K)$ ciclico di ordine n , generato da un certo elemento g . Allora un elemento $\alpha \in M$ ha traccia 0 se e solo se $\alpha = \beta - \beta^g$ per un certo $\beta \in M$.

Dimostrazione

$1 \longrightarrow 2$: Siccome $\mathcal{G}(M/K)$ è ciclico si ha $\mathcal{G}(M/K) = \{1, g, g^2, \ldots, g^{n-1}\}$. Se $\alpha = \beta - \beta^g$,

$$\begin{aligned} t(\alpha) &= (\beta - \beta^g)^1 + (\beta - \beta^g)^g + \cdots + (\beta - \beta^g)^{g^{n-1}} \\ &= \beta - \beta^g + \beta^g - \beta^{g^2} + \cdots + \beta^{g^{n-1}} - \beta^{g^n} \end{aligned}$$

e siccome $g^n = 1$, $\beta^{g^n} = \beta$ quindi

$$= \beta - \beta^g + \beta^g - \beta^{g^2} + \cdots + \beta^{g^{n-1}} - \beta = 0.$$

$2 \longrightarrow 1$: sia $\alpha \in M$ un elemento di traccia 0. Siccome la traccia è suriettiva, esiste un elemento $c \in M$ di traccia 1. Definiamo i seguenti elementi:

$$\begin{aligned} \delta_0 &:= \alpha * c \\ \delta_1 &:= (\alpha + \alpha^g) * c^g \\ &\vdots \\ \delta_i &:= (\alpha + \alpha^g + \cdots + \alpha^{g^i}) * c^{g^i} \\ &\vdots \\ \delta_{n-2} &:= (\alpha + \alpha^g + \cdots + \alpha^{g^{n-2}}) * c^{g^{n-2}} \\ \delta_{n-1} &:= (\alpha + \alpha^g + \cdots + \alpha^{g^{n-1}}) * c^{g^{n-1}} = t(\alpha) * c^{g^{n-1}} = 0 \end{aligned}$$

Inoltre

$$\delta_i^g = (\alpha^g + \alpha^{g^2} + \cdots + \alpha^{g^{i+1}}) * c^{g^{i+1}} = \delta_{i+1} - \alpha c^{g^{i+1}}.$$

cioè

$$\delta_{i+1} - \delta_i^g = \alpha c^{g^{i+1}}, \text{ formula 1}$$

Pongo

$$\beta = \delta_0 + \delta_1 + \cdots + \delta_{n-2}$$

allora

$$\beta - \beta^g = \delta_0 + \delta_1 + \cdots + \delta_{n-2} - \delta_0^g - \delta_1^g - \cdots - \delta_{n-2}^g$$
$$= \delta_0 + (\delta_1 - \delta_0^g) + (\delta_2 - \delta_1^g) + \cdots + (\delta_{n-2} - \delta_{n-3}^g) - \delta_{n-2}^g$$

I termini tra parentesi sono della forma $\delta_{i+1} - \delta_i^g$ quindi posso usare la formula 1, e usando anche la definizione di δ_0 :

$$\beta - \beta^g = \alpha * c + \alpha * c^g + \alpha * c^{g^2} + \cdots + \alpha c^{g^{n-2}} - \delta_{n-2}^g$$

Si ricava anche

$$\delta_{n-2}^g = (\alpha^g + \alpha^{g^2} + \cdots + \alpha^{g^{n-1}}) * c^{g^{n-1}} = \delta_{n-1} - \alpha c^{g^{n-1}} = -\alpha c^{g^{n-1}}$$

perché $\delta_{n-1} = 0$. Quindi

$$\beta - \beta^g = \alpha c + \alpha c^g + \cdots + \alpha c^{g^{n-2}} + \alpha c^{g^{n-1}} = \alpha t(c) = \alpha$$

perché $t(c) = 1$ per la scelta di c . Allora per ogni elemento α di traccia nulla vale la relazione $\alpha = \beta - \beta^g$.

Proposizione 3.5 (applicazione)

Sia $M \supseteq K$ un'estensione normale di campi, con $\mathcal{G}(M/K)$ ciclico di ordine primo p , e sia p la caratteristica di K . Allora $M = K(\alpha)$ dove α è radice di un polinomio irriducibile della forma $x^p - x - a$, a coefficienti in $K[x]$.

Dimostrazione

Supponiamo che $\mathcal{G}(M/K)$ sia generato da un elemento g . Siccome $1 \in K$, $t(1) = p * 1 = 0$ in caratteristica p . Allora esiste $\beta \in M$ tale che $1 = \beta - \beta^g$, posto $\alpha = -\beta$, ottengo

$$1 = \alpha^g - \alpha$$

cioè $\alpha^g = \alpha + 1$, (uguaglianza 1).

Inoltre, usando l'uguaglianza 1,

$$(\alpha^p)^g = (\alpha^g)^p = (\alpha + 1)^p = \alpha^p + 1.$$

cioè $(\alpha^p)^g = \alpha^p + 1$ (uguaglianza 2).

Pongo $a = \alpha^p - \alpha$ **, e mostro che** $a \in K$. Poiché $M \supseteq K$ è normale e quindi $G' = K$, basta provare che $a^g = a$. Usando le uguaglianze 1 e 2,

$$a^g = (\alpha^p - \alpha)^g = (\alpha^p)^g - \alpha^g = \alpha^p + 1 - \alpha - 1 = \alpha^p - \alpha = a$$

allora $a \in K$.

Mostro ora che $M = K(\alpha)$: considero la catena di estensioni $M \supseteq K(\alpha) \supseteq K$, affermo che $K(\alpha) \neq K$ perché $\alpha \notin K$ (altrimenti, siccome g fissa K , si avrebbe $\alpha^g - \alpha = 0$, e questo non è vero perché per l'uguaglianza 1 $\alpha^g - \alpha = 1$).

Siccome $|M : K| = p$ primo, non ci sono campi intermedi propri tra K e M , quindi $M = K(\alpha)$.

Rimane da mostrare che $f(x) = x^p - x - a$ **è irriducibile**: questo è vero perché $f(x)$ è a coefficienti in K , è monico e ha grado p , allora sarà necessariamente il polinomio minimo di α su K e quindi è irriducibile.

4 Elementi di norma 1

Teorema 3.5 (Satz 90 di Hilbert)

Sia $M \supseteq K$ un'estensione normale, e $\mathcal{G}(M/K)$ ciclico, generato da un elemento g di ordine n . Un elemento $\alpha \in M$ ha norma 1 se e solo se $\alpha = \frac{\beta}{\beta^g}$, per un certo $\beta \neq 0 \in M$.

Dimostrazione

$1 \longrightarrow 2$: Come prima, $\mathcal{G}(M/K) = \{1, g, g^2, \ldots, g^{n-1}\}$. Se $\alpha = \frac{\beta}{\beta^g}$,

$$n(\alpha) = (\frac{\beta}{\beta^g})^1 * (\frac{\beta}{\beta^g})^g * \cdots * (\frac{\beta}{\beta^g})^{n-1}$$

$$= \frac{\beta}{\beta^g} * \frac{\beta^g}{\beta^{g^2}} * \cdots * \frac{\beta^{g^{n-1}}}{\beta^{g^n}} =$$

e siccome $\beta^{g^n} = \beta$:

$$= \frac{\beta}{\beta^g} * \frac{\beta^g}{\beta^{g^2}} * \cdots * \frac{\beta^{g^{n-1}}}{\beta} = 1.$$

$2 \longrightarrow 1$: viceversa, sia $\alpha \in M$ un elemento con norma 1. Allora per $c \in M$, definiamo

$$\delta_0 := \alpha c$$

$$\delta_1 := (\alpha * \alpha^g) * c^g$$

$$\delta_2 := (\alpha * \alpha^g * \alpha^{g^2}) * c^{g^2}$$

$$\ldots$$

$$\delta_i := (\alpha * \alpha^g * \cdots * \alpha^{g^i}) * c^{g^i}$$

$$\ldots$$

$$\delta_{n-1} := (\alpha * \alpha^g * \alpha^{g^2} * \cdots * \alpha^{g^{n-1}}) * c^{g^{n-1}} = n(\alpha) * c^{g^{n-1}} = c^{g^{n-1}}$$

Consideriamo la somma

$$\delta_0 + \delta_1 + \cdots + \delta_{n-1} = a_0 c + a_1 c^g + a_2 c^{g^2} + \cdots + a_{n-1} c^{g^{n-1}}$$

dove $a_i := \alpha * \alpha^g * \cdots * \alpha^{g^i}$, e $a_{n-1} = 1$.

Se fosse

$$\delta_0 + \delta_1 + \cdots + \delta_{n-1} = 0, \ \forall c \in M$$

cioè

$$a_0 c + a_1 c^g + a_2 c^{g^2} + \cdots + a_{n-1} c^{g^{n-1}} = 0, \ \forall c \in M$$

avrei una relazione di dipendenza lineare tra $1, g, g^2, \ldots, g^{n-1}$, ma questo non può avvenire perché $1, g, g^2, \ldots, g^{n-1}$ sono linearmente indipendenti essendo automorfismi (distinti) di un campo M . Allora esiste c per cui la somma non sia 0, chiamo β la somma in corrispondenza di tale c , e quindi $\beta \neq 0$.

Osservo che

$$\delta_i^g = \alpha^g * \alpha^{g^2} * \cdots * \alpha^{g^{i+1}} * c^{g^{i+1}} = \frac{\delta_{i+1}}{\alpha}$$

cioè $\alpha \delta_i^g = \delta_{i+1} \forall i = 1, \ldots, n-2$ (formula 1). Negli altri due casi:

$$i = 0, \longrightarrow \delta_0^g = \alpha^g c^g = \frac{\delta_1}{\alpha}$$

quindi la formula 1 vale anche per $i = 0$.

$$\begin{aligned} i = n-1 \longrightarrow \delta_{n-1}^g &= (\alpha * \alpha^g * \cdots * \alpha^{g^{n-1}} * c^{g^{n-1}})^g \\ &= (n(\alpha))^g * (c^{g^{n-1}})^g = 1 * c^{g^n} = c, \text{ formula 2} \end{aligned}$$

Calcoliamo β^g .

$$\beta^g = (\delta_0 + \delta_1 + \cdots + \delta_{n-1})^g = \delta_0^g + \delta_1^g + \cdots + \delta_{n-1}^g$$

e usando le formule 1 e 2:

$$= \delta_1/\alpha + \delta_2/\alpha + \cdots + \delta_{n-1}/\alpha + c = 1/\alpha * (\delta_1 + \delta_2 + \cdots + \delta_{n-1} + \alpha c)$$

ma $\alpha c = \delta_0$, quindi

$$\beta^g = \alpha * (\delta_1 + \delta_2 + \cdots + \delta_{n-1} + \delta_0) = \alpha\beta, \longrightarrow \alpha = \beta/\beta^g$$

cioè ogni elemento α di norma unitaria è tale che $\alpha = \frac{\beta}{\beta^g}$.

Proposizione 3.6

Sia $M \supseteq K$ un'estensione normale, con $\mathcal{G}(M/K)$ ciclico di ordine n , generato da un elemento g . Supponiamo che K contenga le radici n -esime dell'unità, cioè che $x^n - 1$ si spezzi su K in fattori lineari.

Supponiamo che la caratteristica di K non divida n . Allora $M = K(\alpha)$, dove α è radice di un polinomio irriducibile della forma $x^n - a$ a coefficienti in K .

Dimostrazione

Il polinomio $f(x) = x^n - 1$ ha n radici distinte, perché la sua derivata è nx^{n-1} e $M.C.D.(x^n - 1,\, nx^{n-1}) = 1$ per l'ipotesi sulla caratteristica di K .

Tutte le radici di $f(x)$ stanno in K , formano un sottogruppo ciclico Ω di $\mathcal{G}(M/K)$ in particolare $\Omega = \{1, \varepsilon, \varepsilon^2, \cdots, \varepsilon^{n-1}\}$.

Siccome $\varepsilon \in K$, segue subito che $n(\varepsilon) = \varepsilon^n = 1$. Allora per la Satz 90 di Hilbert, esiste $\beta \in M$ per cui $\varepsilon = \frac{\beta}{\beta^g}$. Se pongo $\alpha = 1/\beta$, si ha che $\varepsilon = \frac{\alpha^g}{\alpha}$, cioè $\alpha^g = \alpha\varepsilon$ (uguaglianza 1).

Voglio provare che $\alpha^n \in K$. Siccome l'estensione $M \supseteq K$ è normale, basta mostrare che $(\alpha^n)^g = \alpha^n$, applicando l'uguaglianza 1 si ha:

$$(\alpha^n)^g = (\alpha^g)^n = (\alpha\varepsilon)^n = \alpha^n\varepsilon^n = \alpha^n.$$

Allora $\alpha^n = a \in K$.

Considero $L := K(\alpha)$, che è campo di spezzamento su K del polinomio $x^n - \alpha^n = x^n - a \in K[x]$. Si verificano due casi:

CASO 1: $N = P$ PRIMO. Tra M e K non ci sono campi intermedi propri perché $|M : K| = p$. L è un campo intermedio diverso da K , perché $\alpha \notin K$ (infatti $\alpha \in K$ significherebbe $\varepsilon = \alpha^g/\alpha = 1$, e questo non avviene). Allora necessariamente $L = M$, α è radice del polinomio $x^p - \alpha^p$ a coefficienti in K e, siccome $|M : L| = p$, questo polinomio è il polinomio minimo di α su K e pertanto è necessariamente irriducibile.

CASO 2: N NON PRIMO. Considero $L = K(\alpha)$, L è campo di spezzamento su K del polinomio $x^n - \alpha^n = x^n - a \in K[x]$. Le radici di questo polinomio sono gli elementi dell'insieme

$$\{\alpha, \alpha\varepsilon, \alpha\varepsilon^2, \ldots, \alpha\varepsilon^{n-1}\}.$$

In particolare

$$\alpha^g = \alpha\varepsilon$$
$$\alpha^{g^2} = (\alpha\varepsilon)^g = \alpha^g\varepsilon^g = \alpha\varepsilon^2, \ldots\ldots$$
$$\alpha^{g^i} = \alpha\varepsilon^i, \ldots\ldots$$

Inoltre si ha che $L \supseteq K$ è normale, ovvero L è stabile sotto l'azione degli elementi di $\mathcal{G}(M/K)$. Allora, gli elementi di $\mathcal{G}(M/K)$ inducono per restrizione automorfismi di L su K , in particolare inducono n automorfismi distinti perché se $i \neq j$, $\alpha^{g^i} \neq \alpha^{g^j}$. Allora

$$|L : K| = o(\mathcal{G}(L/K) \geq n = |M : K| = o(\mathcal{G}(M/K)),$$

allora $L = M$ (infatti vale anche la disuguaglianza $o(\mathcal{G}(L/K)) \leq o(\mathcal{G}(M/K))$ perché $\mathcal{G}(L/K)$ è un sottogruppo di $\mathcal{G}(M/K)$).

Infine, come prima, si ha che il polinomio $x^n - \alpha^n$ è irriducibile essendo il polinomio minimo di α su K .

5 Teorema di risolubilità per radicali (seconda parte)

Teorema 3.6

Sia K un campo di caratteristica 0, sia $M \supseteq K$ un'estensione normale, con $\mathcal{G}(M/K)$ risolubile. Allora esiste un campo E tale che $E \supseteq M \supseteq K$, e tale che $E \supseteq K$ sia un'estensione radicale.

Dimostrazione

La dimostrazione è per induzione sul grado di M su K .

Chiamo $G = \mathcal{G}(M/K)$, per ipotesi G è risolubile e finito. Allora esiste H sottogruppo normale di G , con $|G : H| = p$ primo (dimostrazione $*$).

CASO 1: K CONTIENE LE RADICI P -ESIME DELL'UNITÀ. **Qui mostriamo in realtà che $M \supseteq K$ è radicale**. Pongo $L = H'$, allora L è un campo intermedio tra M e K , H è normale in G e quindi L è un'estensione normale di K . Inoltre $|L : K| = |K' : L'| = |G : H| = p$.

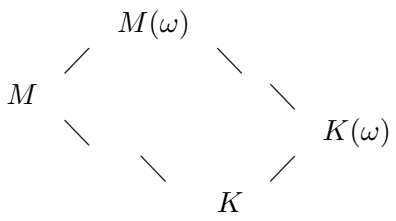
Siccome $o(\mathcal{G}(L/K)) = |L : K| = p$, $\mathcal{G}(L/K)$ è ciclico di ordine p e, poiche' K contiene le radici dell'unità per ipotesi, posso applicare il risultato precedente. Segue che $L = K(\alpha)$, dove α è radice di un polinomio irriducibile della forma $x^p - a$, $a \in K$. Allora $L \supseteq K$ è radicale perché $\alpha^p \in K$.

Siccome G è risolubile per ipotesi, H , che è un suo sottogruppo, è anch'esso risolubile. Inoltre poiché $|L : K| = p$, $|M : L| < |M : K|$. Allora, per induzione, $M \supseteq L$ è radicale, cioè $M = L(\beta_1, \ldots, \beta_s)$, con $\beta_i^{n_i} \in L(\beta_1, \ldots, \beta_{i-1})$. Inoltre $L = K(\alpha)$ e $L \supseteq K$ un'estensione radicale, segue che

$$M = L(\beta_1, \ldots, \beta_s) = K(\alpha)(\beta_1, \ldots, \beta_s) = K(\alpha, \beta_1, \ldots, \beta_s)$$

e $M \supseteq K$ è radicale.

CASO 2: K NON CONTIENE LE RADICI P -ESIME DELL'UNITÀ. Sia $\omega \in \bar{K}$ tale che $\omega^p = 1$. Considero il seguente diagramma:



Girando in senso antiorario ho la catena di estensioni $M(\omega) \supseteq M \supseteq K$, per ipotesi $M \supseteq K$ è normale, $M(\omega)$ è campo di spezzamento su M di $x^p - 1$, e K ha caratteristica 0, quindi anche $M(\omega) \supseteq M$ è normale. Inoltre posso sollevare gli automorfismi di M su K a automorfismi di $M(\omega)$ su K , allora, per una proposizione dimostrata precedentemente (Lezione del 14 aprile, proposizione 0.2.8), $M(\omega) \supseteq K$ è normale.

Inoltre, l'ipotesi $M \supseteq K$ normale implica che M è stabile sotto l'azione degli elementi di $\mathcal{G}(M(\omega)/K)$. In particolare, è possibile definire un omomorfismo di gruppi $\phi : \mathcal{G}(M(\omega)/K(\omega)) \to \mathcal{G}(M/K)$ tale che $g \mapsto g_{|_M}$, che è iniettivo: infatti, dati $g, h \in \mathcal{G}(M(\omega)/K(\omega))$, essi fissano ω , cioè $\omega^g = \omega = \omega^h$. Se imponiamo $\phi(g) = \phi(h)$ si ha che $g_{|_M} = h_{|_M}$, e quindi g, h sono uguali come automorfismi di $M(\omega)$ su $K(\omega)$. Segue che il gruppo di partenza, $\mathcal{G}(M(\omega)/K(\omega))$ è isomorfo a un sottogruppo di $\mathcal{G}(M/K)$, e siccome quest'ultimo è risolubile, anche $\mathcal{G}(M(\omega)/K(\omega))$ lo è. Possono quindi verificarsi due casi:

1. $\mathcal{G}(M(\omega)/K(\omega))$ è isomorfo a un sottogruppo proprio di $\mathcal{G}(M/K)$. Questo vuol dire che $M(\omega) \supseteq K(\omega)$ è un'estensione normale, perché $K(\omega)$ è un campo intermedio tra $M(\omega)$ e K (in generale, data la catena di estensioni $M \supseteq L \supseteq K$, se $M \supseteq K$ è normale segue che $M \supseteq L$ è normale).Si ha $o(\mathcal{G}(M(\omega)/K(\omega))) = |M(\omega) : K(\omega)| < |M : K|$, allora per induzione esiste E campo con $E \supseteq M(\omega) \supseteq K(\omega)$ tale che $E \supseteq K(\omega)$ è un'estensione radicale. Ma $K(\omega)$ è un'estensione radicale di K , allora per un ragionamento analogo al caso precedente $E \supseteq K$ è radicale, e $E \supseteq M \supseteq K$.

2. $\bar{G} := \mathcal{G}(M(\omega)/K(\omega)) \cong \mathcal{G}(M/K)$. Allora $\bar{G}$ è risolubile e contiene un sottogruppo S normale con $|\bar{G} : S| = p$ (questo perche' $\bar{G}$ e' isomorfo a G , quindi $\bar{G}$ contiene un sottogruppo isomorfo ad H). Ragionando come nel primo caso, pongo $L = S'$, allora, poiché S è normale in $\bar{G}$, L è un'estensione normale di $K(\omega)$, con $\mathcal{G}(L/K(\omega))$ ciclico di ordine p .Per il risultato precedente, siccome $K(\omega)$ contiene radici p -esime dell'unità per costruzione, segue che $L = K(\omega, \alpha)$, dove α è radice di un polinomio irriducibile della forma $x^p - a$ con $a \in K(\omega)$ .Poi, $o(\mathcal{G}(M(\omega)/L)) < o(\bar{G}) = o(G) = o(\mathcal{G}(M/K))$, e $\mathcal{G}(M(\omega)/L)$ è risolubile essendo un sottogruppo di $\bar{G}$, allora per induzione esiste E tale che $E \supseteq M(\omega) \supseteq L$ dove $E \supseteq L$ è radicale. Ma $L = K(\omega)(\alpha) = K(\omega, \alpha)$, e quindi L è un'estensione radicale di K . Quindi anche E è un'estensione radicale di K .

Nella dimostrazione abbiamo supposto che G , essendo un gruppo finito e risolubile, abbia un sottogruppo normale di indice p , per un certo primo p . Mostriamo questo fatto.

Dimostrazione (dimostrazione $\ast$)

Dato un gruppo risolubile finito G , il suo derivato primo G' è un sottogruppo proprio di G , e il quoziente G/G' è un gruppo abeliano (osservazione 1).

Inoltre, mostriamo che, **dato un gruppo qualsiasi G finito e $N \leq G$ normale a quoziente abeliano, se G/N non ha ordine primo, posso trovare un sottogruppo N' in G con $N < N'$ e N' normale in G , e G/N' abeliano** (osservazione 2).

Supponiamo che G/N non abbia ordine primo allora $o(G/N) = pn$ con p primo, e il quoziente contiene un sottogruppo di ordine p , i cui elementi sono laterali destri di $N : Ng_1, Ng_2, \ldots, Ng_p$ per certi $g_i \in G$.

Allora pongo $N' = \bigcup_{g_i \in G} Ng_i$ e osservo che

1. N' **è chiuso rispetto al prodotto**: siano $x = n_1 g_i$, $y = n_2 g_j$ elementi di N' , allora
$$xy = n_1 g_i n_2 g_j = n_1 * (g_i n_2) * g_j = n_1 n_3 g_i g_j$$
e poiché N è un gruppo, $n_1 n_3 = n_4 \in N$. Inoltre $\{Ng_1, Ng_2, \ldots, Ng_p\}$ e' un sottogruppo di G/N quindi $Ng_i \cdot Ng_j = Ng_k$ per un certo $k = 1, \ldots, p$ allora $g_i g_j = n_5 g_k$ e
$$xy = n_6 g_k \in Ng_k,\ k = 1, \ldots, p$$
e $Ng_k \subset N'$, quindi $xy \in N'$.

2. N' **è un sottogruppo di** G , infatti vale la chiusura rispetto al prodotto e poi N' contiene N e quindi è non vuoto.

3. N' **è normale**. Per le proprietà del derivato, siccome G/N è abeliano, $G' = [G, G] \subseteq N$ .Dato $g \in G$, $x = n_1 g_i \in N'$, mostro che $g^{-1}xg \in N'$. Osservo che
$$[g_i^{-1}, g^{-1}] = g_i g g_i^{-1} g^{-1} = n \in N$$
$$\longrightarrow\ g_i g = n g g_i$$
quindi
$$g^{-1}xg = g^{-1} n_1 g_i g = g^{-1} n_1 n g g_i$$
ma $n_1 n = \bar{n} \in N$, e siccome N è normale, $g^{-1}\bar{n}g = \hat{n} \in N$, e $g^{-1}xg = \hat{n}g_i \in N'$, allora N' è normale in G .

4. N' **contiene** N **propriamente**.

5. infine $G/(N')$ **è abeliano** per le proprietà del derivato, infatti $G' \subseteq N \subset N'$.

Torniamo a G risolubile finito. Per l'osservazione 1, G/G' è abeliano; se G/G' ha ordine un numero primo l'asserto è vero, cioè ho trovato un sottogruppo normale in G di indice p ; altrimenti, per l'osservazione 2, posso passare da G' a un sottogruppo N che lo contiene propriamente e che sia normale in G e sia a quoziente abeliano, e ripeto il procedimento su $G/N \ldots$.

Dal teorema precedente si evince:

Teorema 3.7

Sia K un campo di caratteristica 0, $f(x) \in K[x]$ un polinomio non costante, M campo di spezzamento per f su K . Allora l'equazione $f(x) = 0$ è risolubile per radicali se e solo se $\mathcal{G}(M/K)$ è risolubile.

6 Fonti per testo e immagini; autori; licenze

6.1 Testo

- **Corso:Algebra IV I1/Risoluzione di radicali/Inverso del teorema di risoluubilità per radicali** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Risoluzione_di_radicali/Inverso_del_teorema_di_risoluubilit%C3%A0_per_radicali?oldid=48459 *Contributori:* Toma.luca95, Irene, ScimmiaSpaziale e Mmontrasio

6.2 Immagini

6.3 Licenza dell'opera