<u>Lezione 15</u>

Prerequisiti: Lezioni 3, 12, 13, 14.

Estensioni radicali. Risolubilità per radicali.

Sia F un campo, e sia K una chiusura algebrica di F. Supporremo che la caratteristica di F sia 0.

Definizione 15.1 Siano $a_1,\dots,a_r \in K$, e, per ogni $i = 1,\dots,r$ sia $\sqrt[n_i]{a_i} \in K$ una radice n_i-esima di a_i. Allora $F(\sqrt[n_1]{a_1},\dots,\sqrt[n_r]{a_r})$ si dice un'*estensione radicale* di F se, per ogni $i = 1,\dots,r$, $a_i \in F(\sqrt[n_1]{a_1},\dots,\sqrt[n_{i-1}]{a_{i-1}})$. Si dice un'*estensione n-radicale* se $n_1 = \dots = n_r = n$.

Osservazione 15.2 Se $n = \mathrm{mcm}(n_1,\dots,n_r)$, allora $F(\sqrt[n_1]{a_1},\dots,\sqrt[n_r]{a_r})$ è un'estensione *n-radicale* di F.

Esempio 15.3

a) $\mathbf{Q}(\sqrt[4]{2})$ è una 4-estensione di $\mathbf{Q}$, ma è anche una 2-estensione di $\mathbf{Q}$, in quanto

$$\mathbf{Q}(\sqrt[4]{2}) = \mathbf{Q}(\sqrt{2},\sqrt{\sqrt{2}}).$$

b) Se $a \in F$, ed $\alpha_1,\dots,\alpha_r$ sono radici n-esime di a in K, allora $F(\alpha_1,\dots,\alpha_r)$ è un'estensione n-radicale di F.

Osservazione 15.4

a) La nozione di estensione n-radicale si può pensare come il risultato di una costruzione ricorsiva, basata su ampliamenti successivi: ad ogni passo, si aggiunge una radice n-esima di un elemento del campo ottenuto al passo precedente. Da questa interpretazione risulta chiaro che vale una proprietà di transitività: se L è un'estensione radicale di F, ogni estensione radicale di L è un'estensione radicale di F.

b) Supponiamo che F contenga tutte le radici n-esime dell'unità. Sia $\alpha \in K$ una radice n-esima di un elemento $a \in F$ non nullo. Allora $F(\alpha)$ è un campo di spezzamento su F di $f(x) = x^n - a$, e, pertanto, è un'estensione normale di F. In particolare, poiché, in caratteristica 0, le radici di $x^n - 1$ sono a due a due distinte, F contiene una radice primitiva n-esima dell'unità e $F(\alpha)$ è una sua estensione galoisiana. Questa affermazione sarà generalizzata nella Proposizione 15.5.

c) Adattando l'argomentazione sviluppata nella dimostrazione della Proposizione 13.13, si può provare che il gruppo di Galois di un'estensione n-radicale di un campo contenente una radice primitiva n-esima dell'unità è sempre abeliano. In realtà vale un risultato più forte:

****Proposizione 15.5** Supponiamo che F contenga una radice primitiva n-esima dell'unità. Sia L un'estensione finita di F. Allora esistono elementi $a_1,\dots,a_r \in F$ tali che $L = F(\sqrt[n]{a_1},\dots,\sqrt[n]{a_r})$ se e solo se $G(L,F)$ è un gruppo abeliano e i periodi dei suoi elementi sono divisori di n. Inoltre, in tal caso, L è un'estensione galoisiana di F.

<u>Dimostrazione</u>: [Mo], Theorem 11.4.

Definizione 15.6 Un polinomio non costante $f(x) \in F[x]$ si dice *risolubile per radicali* se esiste un'estensione radicale L di F tale che $f(x)$ si spezza su L nel prodotto di fattori lineari (ossia: se esiste un'estensione radicale di F contenente un campo di spezzamento di $f(x)$ su F).

Esempio 15.7 Sia $f(x) \in F[x]$. Alla luce di quanto stabilito nella Lezione 14, possiamo concludere che $f(x)$ è risolubile per radicali nei seguenti casi.

a) Se $f(x)$ è un polinomio quadratico: infatti, detto Δ il suo discriminante, un suo campo di spezzamento è $F(\sqrt{\Delta})$, che è un'estensione 2-radicale di F.
b) Se $f(x)$ è un polinomio cubico: infatti, con le notazioni della Lezione 14, un suo campo di spezzamento su F è contenuto in $F\left(\sqrt{\frac{-\Delta}{3}}, \omega, \sqrt[3]{-\frac{q}{2}+\frac{1}{6}\sqrt{\frac{-\Delta}{3}}}, \sqrt[3]{-\frac{q}{2}-\frac{1}{6}\sqrt{\frac{-\Delta}{3}}}\right)$.
c) Se $f(x)$ è un polinomio quartico: infatti, un suo campo di spezzamento su F si ottiene ampliando un campo di spezzamento del risolvente (che è un polinomio cubico) con le radici quadrate dei discriminanti dei polinomi quadratici risultanti dal procedimento risolutivo. Per transitività (vedi Osservazione 15.4), si ottiene così un'estensione radicale di F.
d) Se $f(x) = x^n - a$: infatti, un suo campo di spezzamento si ottiene ampliando F con le radici n-esime di a in K (vedi Esempio 15.3 b)).

La risolubilità per radicali del polinomio $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ di grado n=2, 3, 4 non dipende dal campo dei coefficienti F. In particolare, essa vale quando il campo dei coefficienti è il campo delle funzioni razionali $F(a_1,..,a_n)$ nelle indeterminate $a_1,..,a_n$, cioè, quando $f(x)$ è il polinomio generale di grado n. Ciò discende da un importante risultato generale, valido per i campi di caratteristica 0. Per dimostrarlo, utilizzeremo il seguente lemma, di cui omettiamo la dimostrazione. Esso ricorda, nella forma, il Secondo Teorema di Isomorfismo per i gruppi (Teorema 2.4).

Nota preliminare Dati due campi intermedi L e M tra F e K, con LM denoteremo il sottocampo di K generato da L e M.

****Lemma 15.8** Siano L ed M sottocampi di K tali che L sia un'estensione galoisiana di F e M sia un'estensione di F. Allora LM è un'estensione galoisiana di M e $G(LM, M) \cong G(L, L \cap M)$. Inoltre $[LM : M] = [L : L \cap M]$.

Dimostrazione: [Mo], Theorem 5.5.

Teorema 15.9 Sia F un campo di caratteristica 0. Il polinomio non costante $f(x) \in F[x]$ è risolubile per radicali se e solo se il suo gruppo di Galois su F è risolubile.

Dimostrazione: Sia L un campo di spezzamento di $f(x)$ su F contenuto in K. Allora, in virtù dell'Osservazione 11.10, L è un'estensione galoisiana di F. Supponiamo dapprima che il gruppo di Galois $G = G(L, F)$ di $f(x)$ su F sia risolubile. Esiste allora, in virtù della Proposizione 3.8, una catena di sottogruppi normali

$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_n = \{\mathrm{id}\}$$

tale che, per ogni $i=0,\dots,n-1$, il gruppo quoziente H_i / H_{i+1} è abeliano. Sia, per ogni $i=0,\dots,n$, K_i il campo fisso di H_i. Allora $F=K_0$, $L=K_{H_n}=K_n$ e, per ogni $i=0,\dots,n-1$, in virtù dell'Osservazione 12.1 c) si ha che $F\subset K_i\subset K_{i+1}\subset L$. Dall'Osservazione 11.2 segue allora che L è un'estensione galoisiana di K_i, quindi possiamo applicare il Teorema Fondamentale della Teoria di Galois a questa estensione. Sappiamo che, per il Teorema 12.2, essendo

$$G(L,K_i)=G(L,K_{H_i})=H_i \triangleright H_{i+1}=G(L,K_{H_{i+1}})=G(L,K_{i+1}),$$

K_{i+1} è un'estensione normale (galoisiana) di K_i. Pertanto possiamo applicare al campo intermedio K_{i+1} tra K_i e L il Teorema 12.5 b), e dedurre che

$$G(K_{i+1},K_i)\cong G(L,K_i) / G(L,K_{i+1}) = H_i / H_{i+1}.$$

Segue che $G(K_{i+1},K_i)$ è abeliano finito. Sia d il minimo comune multiplo dei periodi degli elementi di $G(K_{i+1},K_i)$, sia ω una radice primitiva d-esima dell'unità in K (esistente perché la caratteristica di F, e quindi di K, è 0); per ogni $i=0,\dots,n$ poniamo $L_i=K_i(\omega)$. Si hanno allora le estensioni successive

$$F\subset L_0\subset\cdots\subset L_n,$$

ove $L_0=F(\omega)$ e $L\subset L_n=L(\omega)$. Si noti che $L_{i+1}=L_iK_{i+1}$, per ogni $i=0,\dots,n-1$. Poiché K_{i+1} è un'estensione galoisiana di K_i, per il Lemma 15.8 L_{i+1} è un'estensione galoisiana di L_i, e $G(L_{i+1},L_i)$ è isomorfo a $G(K_{i+1},K_{i+1}\cap L_i)$, che, essendo $K_i\subset K_{i+1}\cap L_i$, per l'Osservazione 12.1 c), è un sottogruppo di $G(K_{i+1},K_i)$, e quindi è abeliano. Sia e il minimo comune multiplo dei periodi degli elementi di $G(L_{i+1},L_i)$. Allora e divide d. Per la Proposizione 15.5, segue allora che L_{i+1} è una estensione d-radicale di L_i. Quindi, per transitività, L_n è un'estensione d-radicale di L_0, che è un'estensione radicale di F. Segue che L_n è un'estensione radicale di F contenente L, e quindi $f(x)$ è risolubile per radicali.

Supponiamo ora che $f(x)$ sia risolubile per radicali. Allora esiste una estensione n-radicale $L=F(\alpha_1,\dots,\alpha_r)$ di F (contenuta in K) contenente un campo di spezzamento di $f(x)$ su F (supponiamo, per ogni $i>1$, che $F(\alpha_1,\dots,\alpha_i)$ sia un'estensione n-radicale di $F(\alpha_1,\dots,\alpha_{i-1})$). In virtù di [Mo], Lemma 16.6, possiamo supporre che L sia un'estensione normale di F. Sia $\omega\in K$ una radice primitiva n-esima dell'unità. Allora $L(\omega)$ è un'estensione galoisiana di F.

Poniamo quindi $L_0=F$, $L_1=F(\omega)$, e, per ogni $i=2,\dots,r+1$, $L_i=F(\omega,\alpha_1,\dots,\alpha_{i-1})$. Allora $L_{r+1}=L(\omega)$, e si hanno le estensioni successive

$$F=L_0\subset L_1\subset\cdots\subset L_{r+1}=L(\omega),$$

dove, per ogni $i=1,\dots,r-1$, $L_{i+1}=L_i(\alpha_i)$, e quindi, per l'Osservazione 15.4 b), le estensioni sono tutte normali, e dunque galoisiane.

In base al Teorema Fondamentale della Teoria di Galois (Teorema 12.2), applicato all'estensione galoisiana $L(\omega)$ di F, se ne deriva la catena di sottogruppi normali

$$G(L(\omega),F) \triangleright G(L(\omega),L_1) \triangleright \cdots \triangleright G(L(\omega),L(\omega)) = \{\mathrm{id}\}.$$

In virtù del Teorema 12.5 b), per ogni $i = 0,\dots,r-1$, $G(L(\omega),L_i) \big/ G(L(\omega),L_{i+1}) \cong G(L_{i+1},L_i)$, che è abeliano in base alla Proposizione 13.11 ed alla Proposizione 13.13. Ciò basta per concludere che $G(L(\omega),F)$ è risolubile. Sia M un campo di spezzamento di $f(x)$ su F contenuto in L. Allora M è un'estensione normale di F contenuta in $L(\omega)$. Dal Teorema 12.5 b) segue che $G(M,F)$ è isomorfo ad un quoziente di $G(L(\omega),F)$. Ma ogni gruppo quoziente di un gruppo risolubile è risolubile in virtù della Proposizione 3.9. La tesi segue. □

Dal Teorema 15.9, dal Teorema 13.16 e dal Teorema di Galois-Jordan (Teorema 3.14) segue subito:

Corollario 15.10 (*Teorema di Abel-Ruffini*) In caratteristica zero, il polinomio generale di grado $n \geq 5$ non è risolubile per radicali.

Osservazione 15.11 Il fatto che il polinomio generale di grado $n \geq 5$ non è risolubile significa che non esiste una formula risolutiva generale per le equazioni di grado n in cui compaiano solo le quattro operazioni e l'estrazione di radice. Ciò non impedisce che una formula siffatta esista per certe particolari equazioni di grado n, come, ad esempio, le equazioni binomie.