Lezione 12

Prerequisiti: Lezione 11.

Funzioni polinomiali.
Radici di un polinomio.
Teorema di Ruffini.

Sia K un campo e sia L un campo di cui K è sottocampo (in tal caso si dice anche che L è un'*estensione di K)*.

Sia $f(X) \in K[X]$ e sia $\alpha \in L$. Allora, se $f(X) = \sum_{i=0}^{n} a_i X^i$, si pone $f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i \in L$. Questo elemento è detto *valutazione di* $f(X)$ in α.

Definizione 12.1 Sia $f(X) \in K[X]$. Si dice *funzione polinomiale (da L a L) associata a* $f(X)$ l'applicazione $F : L \to L$ definita ponendo, per ogni $\alpha \in L$, $F(\alpha) = f(\alpha)$.

Osservazione 12.2 Funzioni polinomiali associate a polinomi distinti non sono necessariamente distinte. Sia, ad esempio, $K = L = \mathbb{Z}_2$ e siano $f_1(X) = X^2 + X, f_2(X) = 0$. Allora le funzioni polinomiali F_1, F_2 da $\mathbb{Z}_2$ a $\mathbb{Z}_2$ associate, rispettivamente, a $f_1(X)$ e $f_2(X)$ sono entrambe costanti di costante valore $[0]_2$. Infatti $F_1([0]_2) = [0]_2, F_1([1]_2) = [1]_2{}^2 + [1]_2 = [0]_2$. Dunque $F_1 = F_2$, pur essendo $f_1(X) \neq f_2(X)$.

Definizione 12.3 Sia $f(X) \in K[X]$ e sia $\alpha \in L$. Allora α si dice una *radice* di $f(X)$ se $f(\alpha) = 0$.

Esempio 12.4 Sia $f(X) = X^2 - 2 \in \mathbb{Q}[X]$. Allora $\alpha = \sqrt{2} \in \mathbb{R}$ è una radice di $f(X)$. Anche $-\alpha = -\sqrt{2} \in \mathbb{R}$ è una sua radice. Invece 7 non è radice di $f(X)$, poiché $f(7) = 47 \neq 0$.

Nota Le radici di $f(X) \in K[X]$ in L sono le soluzioni in L dell'equazione (algebrica) $f(x) = 0$, ove x, che sostituisce l'indeterminata X, è l'incognita.
Si osservi che $f(X) \in L[X]$, e quindi l'equazione è a coefficienti in L.

La nozione di radice è strettamente legata a quella di divisibilità, a cui è stata dedicata la Lezione 11. Lo mostra il seguente risultato, la cui dimostrazione utilizza il Teorema di divisione euclidea (Teorema 11.1).

Teorema 12.5 *(Teorema di Ruffini)* Sia $f(X) \in K[X]$ e sia $\alpha \in L$. Allora α è una radice di $f(X)$ se e solo se il polinomio $X - \alpha$ divide $f(X)$ in $L[X]$.

Dimostrazione: Supponiamo dapprima che $X - \alpha$ divida $f(X)$ in $L[X]$. Allora esiste $q(X) \in L[X]$ tale che $f(X) = (X - \alpha)q(X)$. Pertanto

$$f(\alpha)=(\alpha-\alpha)q(\alpha)=0q(\alpha)=0.$$

Ciò prova che α è una radice di $f(X)$. Viceversa, supponiamo che α sia una radice di $f(X)$. Siano $q(X)$ ed $r(X)$, rispettivamente, il quoziente ed il resto della divisione euclidea di $f(X)$ per $X-\alpha$ in $L[X]$. Allora

$$f(X)=(X-\alpha)q(X)+r(X), \tag{1}$$

ove $r(X)=0$, oppure $r(X)\neq 0$ e $\deg(r)<\deg(X-\alpha)=1$; la seconda condizione equivale a $\deg(r)=0$, quindi, in ogni caso, $r(X)$ è un polinomio costante, ossia $r(X)=a_0\in L$. Dalla (1) ricaviamo dunque, considerando la valutazione in α:

$$f(\alpha)=(\alpha-\alpha)q(\alpha)+a_0. \tag{2}$$

Ma, per ipotesi $f(\alpha)=0$, mentre il secondo membro della (2) è uguale ad a_0. Segue che $a_0=0$, cioè $r(X)=0$. Ciò, alla luce della (1), prova che $X-\alpha$ divide $f(X)$ in $L[X]$. □

Esempio 12.6 Sia $f(X)=X^3-3X^2+X+1\in\mathbb{Q}[X]$. Allora $f(1)=1-3+1+1=0$. Quindi il polinomio $X-1$ divide $f(X)$ in $\mathbb{Q}[X]$. In effetti,

$$X^3-3X^2+X+1=(X-1)(X^2-2X-1).$$

Corollario 12.7 *(Primo corollario al Teorema di Ruffini)*. Sia $f(X)\in K[X]$. Allora $f(X)$ ha una radice in K se e solo se è divisibile in $K[X]$ per un polinomio avente grado 1.

Dimostrazione: Se $f(X)$ ha una radice $\alpha\in K$, allora, in base al Teorema di Ruffini, è divisibile in $K[X]$ per il polinomio $X-\alpha$, che ha grado 1. Viceversa, sia $g(X)=aX+b$, $(a,b\in K, a\neq 0)$ un polinomio di grado 1 per il quale $f(X)$ è divisibile. Allora esiste $q(X)\in K[X]$ tale che $f(X)=g(X)q(X)$. Inoltre posto $\alpha=-ba^{-1}\in K$, si ha $g(\alpha)=0$. Segue che $f(\alpha)=g(\alpha)q(\alpha)=0$, e quindi α è una radice di $f(X)$. □

Osservazione 12.8 Poiché, come stabilito dal Corollario 11.13, ogni polinomio di grado 1 è irriducibile, l'enunciato del Corollario 12.7 si può riformulare nel modo seguente: *un polinomio di* $K[X]$ *ha una radice in K se e solo se ha in* $K[X]$ *un fattore irriducibile di grado* 1.

Corollario 12.9 *(Secondo corollario al Teorema di Ruffini)*. Sia $f(X)\in K[X]$ e sia $\deg(f)\in\{2,3\}$. Allora $f(X)$ è irriducibile in $K[X]$ se e solo se non ha radici in K.

Dimostrazione: Supponiamo che $f(X)$ sia irriducibile in $K[X]$. Allora, per l'unicità della fattorizzazione, $f(X)$ non ha in $K[X]$ fattori irriducibili di grado 1. Pertanto, per il Corollario 12.7, non ha radici in K. Viceversa, supponiamo che $f(X)$ sia riducibile in $K[X]$. Allora esistono $a(X),b(X)\in K[X]$ non invertibili (ossia aventi grado maggiore o uguale a 1) tali che $f(X)=a(X)b(X)$. In virtù della formula del grado per il prodotto (Proposizione 10.2 (b)), si ha $\deg(f)=\deg(a)+\deg(b)$. Se $\deg(f)=2$, ciò implica che $\deg(a)=\deg(b)=1$. Se $\deg(f)=3$, ciò implica che $\{\deg(a),\deg(b)\}=\{1,2\}$. Quindi, in entrambi i casi, uno tra $a(X)$ e $b(X)$ ha grado 1.

Dal Corollario 12.7 segue allora che uno tra $a(X)$ e $b(X)$ ha una radice in *K*. Poiché entrambi dividono $f(X)$, segue che anche $f(X)$ ha una radice in *K*. □

Osservazione 12.10 Il Corollario 12.9 non si estende ai polinomi di grado superiore a 3. Lo mostra il seguente esempio. Sia $f(X) = X^4 - 4 \in \mathbb{Q}[X]$. Questo è un polinomio di grado 4, privo di radici in $\mathbb{Q}$ (4 non ha radici quarte in $\mathbb{Q}$). Tuttavia è riducibile in $\mathbb{Q}[X]$, in quanto $f(X) = (X^2 - 2)(X^2 + 2)$.

Il Teorema di Ruffini ed i suoi corollari possono risultare utili al fine di determinare una fattorizzazione di un polinomio a coefficienti in un campo.

Esercizio 12.11 Sia $f(X) = X^3 - 3X^2 + X + 1 \in \mathbb{Q}[X]$. Determinare una fattorizzazione di $f(X)$ in $\mathbb{Q}[X]$ e in $\mathbb{R}[X]$.

Svolgimento: Nell'Esempio 12.6 abbiamo visto che $f(X) = (X-1)(X^2 - 2X - 1)$. Poniamo $q(X) = X^2 - 2X - 1$. Essendo $\deg(q) = 2$, a $q(X)$ si applica (sia in $\mathbb{Q}[X]$ sia in $\mathbb{R}[X]$) il Corollario 12.9. Notiamo che il discriminante di $q(X)$ è $\Delta = 4 + 4 = 8 > 0$, quindi $q(X)$ ha due radici reali distinte, e, precisamente, $\alpha_1 = 1 + \frac{1}{2}\sqrt{8} = 1 + \sqrt{2}$, $\alpha_2 = 1 - \sqrt{2}$. Poiché queste non sono razionali, $q(X)$ non ammette radici in $\mathbb{Q}$, e quindi $q(X)$ è irriducibile in $\mathbb{Q}[X]$. Dunque la fattorizzazione di $f(X)$ in $\mathbb{Q}[X]$ è

$$f(X) = (X-1)(X^2 - 2X - 1).$$

Invece, in base al Teorema di Ruffini, in $\mathbb{R}[X]$ $q(X)$ ammette i fattori irriducibili (non associati) $X - \alpha_1, X - \alpha_2$, quindi il prodotto $(X - \alpha_1)(X - \alpha_2)$ è parte della fattorizzazione di $q(X)$ in $\mathbb{R}[X]$. Dunque $q(X) = h(X)(X - \alpha_1)(X - \alpha_2)$ per qualche $h(X) \in \mathbb{R}[X]$. Ma dalla formula del grado per il prodotto segue che $\deg(h) = 0$. Quindi $h \in \mathbb{R}^*$. D'altra parte h è il coefficiente direttore del polinomio $h(X - \alpha_1)(X - \alpha_2)$, quindi è il coefficiente direttore di $q(X)$. Ma allora $h = 1$. Dunque $q(X) = (X - \alpha_1)(X - \alpha_2)$ è una fattorizzazione di $q(X)$ in $\mathbb{R}[X]$. Otteniamo, così, la seguente fattorizzazione di $f(X)$ in $\mathbb{R}[X]$:

$$f(X) = (X-1)(X-1-\sqrt{2})(X-1+\sqrt{2}).$$

Osservazione 12.12 Sia $f(X) \in K[X]$ non nullo, sia $\alpha \in K$ una radice di $f(X)$. Allora, in base al Teorema di Ruffini, $X - \alpha$ divide $f(X)$ in $K[X]$. Quindi $(X - \alpha)^s$ divide $f(X)$ in $K[X]$ per $s = 1$. D'altra parte, se $(X - \alpha)^s$ divide $f(X)$ in $K[X]$ per qualche intero $s \geq 1$, allora, in base alla formula del grado per il prodotto, $s = \deg((X - \alpha)^s) \leq \deg(f)$. Riassumendo, l'insieme

$$\left\{ s \in \mathbb{N}^* \,\middle|\, (X - \alpha)^s \text{ divide } f(X) \right\}$$

è un sottoinsieme non vuoto e superiormente limitato di $\mathbb{N}$. Quindi è finito, e pertanto ammette un massimo.

Definizione 12.13 Sia $f(X) \in K[X]$ non nullo, sia $\alpha \in K$ una radice di $f(X)$. Allora il numero

$$\max\left\{ s \in \mathbb{N}^* \,\middle|\, (X-\alpha)^s \text{ divide } f(X) \right\}$$

si dice *molteplicità* della radice α di $f(X)$.

Nota In altri termini, il numero intero positivo *r* è la molteplicità della radice α di $f(X)$ se e solo se $(X-\alpha)^r$ divide $f(X)$, mentre $(X-\alpha)^{r+1}$ non divide $f(X)$.

Nota Una radice di molteplicità 1 (2, 3) si dice *semplice* (*doppia, tripla*).

La nozione di molteplicità di una radice ci consente di perfezionare la relazione che abbiamo già individuato tra le radici di un polinomio e la sua fattorizzazione.

Proposizione 12.14 *(Radici e fattorizzazioni di polinomi)* Sia $f(X) \in K[X]$ non nullo e siano $\alpha_1, \alpha_2, ..., \alpha_t \in K$ sue radici a due a due distinte, ove, per ogni $i = 1,..,t,$ la molteplicità di α_i è r_i. Allora $(X-\alpha_1)^{r_1}(X-\alpha_2)^{r_2}\cdots(X-\alpha_t)^{r_t}$ divide $f(X)$ in $K[X]$.

Dimostrazione: Procediamo per induzione su $t \geq 1$. Per $t = 1$ la tesi segue banalmente dalla Definizione 12.13. Sia ora $t \geq 2$ e supponiamo la tesi vera per $t-1$. Poiché α_t è una radice di $f(X)$ di molteplicità r_t, si ha che

$$f(X) = (X-\alpha_t)^{r_t} q(X) \tag{3}$$

per qualche $q(X) \in K[X]$. Sia ora $i \in \{1,...,t-1\}$. Allora $X-\alpha_i$ ed $X-\alpha_t$ sono fattori irriducibili non associati di $f(X)$ in $K[X]$, quindi sono coprimi, e lo stesso vale dunque per $(X-\alpha_i)^{r_i}$ e $(X-\alpha_t)^{r_t}$. Poiché $(X-\alpha_i)^{r_i}$ divide $(X-\alpha_t)^{r_t} q(X)$, come nella Proposizione 6.24 segue dunque che $(X-\alpha_i)^{r_i}$ divide $q(X)$. Dunque per ogni $i = 1,...,t-1,$ α_i è una radice di $q(X)$ avente molteplicità r_i. Al polinomio $q(X)$ si applica quindi l'ipotesi induttiva. Segue che $(X-\alpha_1)^{r_1}(X-\alpha_2)^{r_2}\cdots(X-\alpha_{t-1})^{r_{t-1}}$ divide $q(X)$ in $K[X]$. Alla luce della (3), ciò implica la tesi. □

Nelle ipotesi della Proposizione 12.14 si ha una decomposizione

$$f(X) = (X-\alpha_1)^{r_1}(X-\alpha_2)^{r_2}\cdots(X-\alpha_t)^{r_t} g(X) \tag{4}$$

per qualche $g(X) \in K[X]$. Tenendo conto della formula del grado per il prodotto di polinomi, si deduce subito il seguente risultato.

Corollario 12.15 *(Radici e grado di un polinomio)* Sia $f(X) \in K[X]$ non nullo e siano $\alpha_1, \alpha_2, ..., \alpha_t \in K$ sue radici a due a due distinte, ove, per ogni $i = 1,..,t,$ la molteplicità di α_i è r_i. Allora $\sum_{i=1}^{t} r_i \leq \deg(f)$.

Nota L'enunciato del Corollario 12.15 si può riformulare come segue: *un polinomio di grado n ha al più n radici (contate con le rispettive molteplicità).*

Osservazione 12.16 Nell'enunciato del Corollario 12.15 vale l'uguaglianza se e solo se nella (4) $g(X)$ è costante. In tal caso la (4) è una fattorizzazione di $f(X)$, in cui tutti i fattori irriducibili sono lineari. Ciò non avviene sempre: nell'Esercizio 12.11 abbiamo visto, ad esempio, che la fattorizzazione del polinomio $f(X) = X^3 - 3X^2 + X + 1$ in $\mathbb{Q}[X]$ contiene un fattore di grado 2.

Esercizio 12.17* Dire se i seguenti polinomi sono irriducibili in $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$:

(a) $X^2 - 1$;

(b) $X^2 + 1$;

(c) $X^2 - 2$.