Lezione 13

Prerequisiti: Lezioni 1, 11 e 12.

Campi algebricamente chiusi.
Teorema Fondamentale dell'Algebra.
Polinomi a coefficienti reali.

Proposizione 13.1 Sia K un campo. Sono equivalenti le seguenti condizioni.

(i) Ogni polinomio non costante di $K[X]$ ha una radice in K.

(ii) Ogni polinomio non costante di $K[X]$ avente grado n ha in K esattamente n radici (contate con le rispettive molteplicità).

(iii) Ogni polinomio non costante di $K[X]$ si decompone in $K[X]$ nel prodotto di fattori lineari.

Dimostrazione: (i) $\Rightarrow$ (ii) Supponiamo che valga (i). Sia $f(X) \in K[X]$ non costante, avente grado n. Proviamo, per induzione su n, che $f(X)$ ha in K esattamente n radici (contate con le rispettive molteplicità). Per $n = 1$ la tesi è vera: in tal caso, infatti, $f(X) = aX + b$, per opportuni $a, b \in K, a \neq 0$, e $\alpha = -a^{-1}b$ è la sua unica radice in K. Sia ora $n > 1$ e supponiamo la tesi vera per tutti i polinomi di $K[X]$ aventi grado $n-1$. Per ipotesi $f(X)$ ha una radice $\alpha \in K$. Per il Teorema di Ruffini (Teorema 12.5) esiste allora $g(X) \in K[X]$ tale che $f(X) = (X - \alpha)g(X)$. Per la formula del grado per il prodotto di polinomi (Proposizione 10.2 (b)), segue che $g(X)$ ha grado $n-1$. In particolare, non è un polinomio costante. Per l'ipotesi induttiva, $g(X)$ ha dunque esattamente $n-1$ radici contate con le rispettive molteplicità. Se a queste si aggiunge la radice α, si ottengono tutte le radici di $f(X)$, che sono dunque esattamente n.

(ii) $\Rightarrow$ (iii) Supponiamo ora che valga (ii). Sia $f(X) \in K[X]$ non costante, avente grado n. Per ipotesi, le sue radici sono elementi $\alpha_1, ..., \alpha_t \in K$, a due a due distinti, tali che, dette $r_1, ..., r_t$ le loro rispettive molteplicità, si abbia $\sum_{i=1}^{t} r_i = n$. In virtù della Proposizione 12.14, si ha allora

$$f(X) = (X - \alpha_1)^{r_1} \cdots (X - \alpha_t)^{r_t} \, q(X) \qquad (1)$$

per qualche $q(X) \in K[X]$. Per la formula del grado segue che $\deg(q) = n - \sum_{i=1}^{t} r_i = 0$, ossia $q(X) = q \in K^*$. Quindi dalla (1) ricaviamo la seguente fattorizzazione di $f(X)$ nel prodotto di fattori lineari:

$$f(X) = (qX - q\alpha_1)(X - \alpha_1)^{r_1 - 1} \cdots (X - \alpha_t)^{r_t}.$$

(iii) $\Rightarrow$ (i) Questa implicazione segue dal primo corollario al Teorema di Ruffini (Corollario 12.7). □

Definizione 13.2 Un campo K verificante le condizioni equivalenti della Proposizione 13.1 si dice *algebricamente chiuso.*

Proposizione 13.3 Ogni campo algebricamente chiuso è infinito.

Dimostrazione: Sia K un campo finito, siano $\alpha_1,\ldots,\alpha_n$ i suoi elementi (a due a due distinti). Sia

$$f(X)=1+\prod_{i=1}^{n}(X-\alpha_i).$$

Allora $\deg(f)=n$ e, per ogni $i=1,\ldots,n$, $f(\alpha_i)=1\neq 0$. Quindi $f(X)$, che non è costante, è privo di radici in K. Ciò prova che K non è algebricamente chiuso. □

Esempio 13.4 La Proposizione 13.3 non si inverte: esistono, infatti, campi infiniti che non sono algericamente chiusi. Il campo $\mathbb{R}$ non è algebricamente chiuso: infatti il polinomio $f(X)=X^2+1\in\mathbb{R}[X]$, che non è costante, non ha radici in $\mathbb{R}$. Quindi la (i) e la (ii) risultano violate per $K=\mathbb{R}$. Inoltre, in base al secondo corollario al Teorema di Ruffini (Corollario 12.9), $f(X)$ è irriducibile in $\mathbb{R}[X]$, e quindi anche la (iii) risulta violata. Tutto quanto precede resta vero se a $\mathbb{R}$ si sostituisce $\mathbb{Q}$. Quindi nemmeno $\mathbb{Q}$ è algebricamente chiuso.

Il prossimo enunciato, di cui omettiamo la dimostrazione, fu provato per la prima volta da Carl Friedrich Gauss nella sua tesi di dottorato (1799). Altre due sue dimostrazioni seguirono nel 1816.

Teorema 13.5 *(Teorema Fondamentale dell'Algebra)* Il campo $\mathbb{C}$ è algebricamente chiuso.

Corollario 13.6 Un polinomio di $\mathbb{C}[X]$ è irriducibile se e solo se è di grado uno.

Dimostrazione: Sia $f(X)\in\mathbb{C}[X]$. Se $\deg(f)=1$, allora $f(X)$ è irriducibile in base al Corollario 11.13. Viceversa, sia $f(X)$ irriducibile. Siccome per il campo $\mathbb{C}$, in base al Teorema Fondamentale dell'Algebra, vale la condizione (iii) della Proposizione 13.1, il polinomio $f(X)$, d'altra parte, si decompone in $\mathbb{C}[X]$ nel prodotto di $\deg(f)$ fattori lineari. Quindi deve essere $\deg(f)=1$. □

Dal Teorema 13.5 vogliamo trarre conseguenze sulla fattorizzazione dei polinomi a coefficienti reali. Proviamo prima un risultato preliminare.

Lemma 13.7 Sia $f(X)\in\mathbb{R}[X]$, e sia $\alpha\in\mathbb{C}$. Allora, se α è radice di $f(X)$, lo è anche il suo complesso coniugato $\overline{\alpha}$.

Dimostrazione: Sia $f(X)=\sum_{i=0}^{n}a_iX^i$, ove $a_i\in\mathbb{R}$ per ogni $i=0,\ldots,n$. Se α è radice di $f(X)$, si ha

$$0=f(\alpha)=\sum_{i=0}^{n}a_i\alpha^i=\overline{\sum_{i=0}^{n}a_i\alpha^i}=\sum_{i=0}^{n}\overline{a}_i\overline{\alpha}^i=\sum_{i=0}^{n}a_i\overline{\alpha}^i=f(\overline{\alpha}),$$

ove la terza uguaglianza è dovuta al fatto che zero, in quanto numero reale, coincide col proprio complesso coniugato (v. Proposizione 1.9 b)), la quarta al fatto che la formazione del complesso coniugato commuta con la somma ed il prodotto, e in particolare con l'elevamento a potenza (v. Proposizione 1.9 f), g)), la quinta al fatto che i coefficienti di $f(X)$ sono reali. □

Osservazione 13.8 Il Lemma 13.7 generalizza il risultato, stabilito nell'Esercizio 1.7, in base al quale un polinomio di grado due privo di radici reali ha per radici due numeri complessi che sono uno il coniugato dell'altro.

Proposizione 13.9 Un polinomio di $\mathbb{R}[X]$ è irriducibile se e solo se è di grado uno oppure è di grado due e privo di radici reali.

Dimostrazione: Sia $f(X) \in \mathbb{R}[X]$. Se $\deg(f) = 1$, allora $f(X)$ è irriducibile in base al Corollario 11.13. Se $\deg(f) = 2$ e $f(X)$ non ha radici reali, allora $f(X)$ è irriducibile in base al secondo corollario al Teorema di Ruffini. Viceversa, supponiamo che $f(X)$ sia irriducibile. Allora $f(X)$, per definizione, è non costante. Inoltre $f(X) \in \mathbb{C}[X]$. Per il Teorema Fondamentale dell'Algebra segue che $f(X)$ ha una radice $\alpha \in \mathbb{C}$. Se $\alpha \in \mathbb{R}$, allora, per il primo corollario al Teorema di Ruffini, $f(X)$ ha in $\mathbb{R}[X]$ un fattore irriducibile di grado uno e quindi, essendo irriducibile, coincide, a meno di un fattore costante non nullo, con questo fattore irriducibile. In tal caso $f(X)$ ha grado uno. Supponiamo allora che $\alpha \notin \mathbb{R}$. Allora, in base alla Proposizione 1.9 b), $\alpha \neq \bar{\alpha}$, e, in base al Lemma 13.7, anche $\bar{\alpha}$ è radice di $f(X)$. Dalla Proposizione 12.14 segue allora che $f(X)$ è divisibile per il polinomio

$$g(X) = (X - \alpha)(X - \bar{\alpha}) = X^2 - (\alpha + \bar{\alpha})X + \alpha\bar{\alpha} = X^2 - 2\,\mathrm{Re}(\alpha)X + |\alpha|^2.$$

La terza uguaglianza è dovuta alla Proposizione 1.9 (d) e (h). Ora, $g(X) \in \mathbb{R}[X]$, $\deg(g) = 2$ e $g(X)$ è privo di radici in $\mathbb{R}$ (le sue uniche radici sono α e $\bar{\alpha}$, entrambe non reali). In base al secondo corollario al Teorema di Ruffini, segue che $g(X)$ è irriducibile in $\mathbb{R}[X]$, quindi $f(X)$, essendo esso stesso irriducibile, coincide con $g(X)$ a meno di un fattore costante non nullo. Quindi, in questo caso, $f(X)$ ha grado due ed è privo di radici reali. □

Dalla Proposizione 13.9 e dal Teorema di fattorizzazione unica (Teorema 11.15) segue immediatamente il seguente:

Corollario 13.10 Ogni polinomio di $\mathbb{R}[X]$ non costante si decompone nel prodotto di polinomi di $\mathbb{R}[X]$ aventi grado al più due.

Corollario 13.11 Ogni polinomio di $\mathbb{R}[X]$ di grado dispari ha una radice reale.

Dimostrazione: Sia $f(X) \in \mathbb{R}[X]$ di grado dispari. Allora $f(X)$ non è costante, e quindi, in base, al Corollario 13.10, si decompone nel prodotto di fattori di grado al più due. Tra questi v'è almeno un fattore di grado uno (altrimenti, in base alla formula del grado per il prodotto, il grado di $f(X)$ sarebbe pari). In base al primo corollario al Teorema di Ruffini segue allora che $f(X)$ ha una radice in $\mathbb{R}$. □