Lezione 14

Prerequisiti: Numeri primi. Lezioni 10-13.

Polinomi a coefficienti interi

In questa lezione studiamo le fattorizzazioni di polinomi a coefficienti razionali. Ciascuno di questi può essere trasformato in un polinomio a coefficienti interi tramite la moltiplicazione per un numero intero non nullo. Quindi ogni polinomio di $\mathbb{Q}[X]$ è associato ad un polinomio di $\mathbb{Z}[X]$, con il quale ha in comune le radici e tutti i fattori irriducibili. Nel nostro studio possiamo quindi limitarci a considerare i polinomi a coefficienti interi, tanto più che, come conseguenza del prossimo enunciato, (di cui omettiamo la dimostrazione) ogni polinomio non costante di $\mathbb{Z}[X]$ possiede una fattorizzazione in cui tutti i fattori appartengono a $\mathbb{Z}[X]$.

Teorema 14.1 *(Lemma di Gauss)* Sia $f(X) \in \mathbb{Z}[X]$, e siano $g(X), h(X) \in \mathbb{Q}[X]$ tali che $f(X) = g(X)h(X)$. Allora esiste $c \in \mathbb{Q}^*$ tale che, posto $g^*(X) = cg(X)$ e $h^*(X) = c^{-1}h(X)$, si abbia che $g^*(X), h^*(X) \in \mathbb{Z}[X]$ (oltre, naturalmente, a $f(X) = g^*(X)h^*(X)$).

Esempio 14.2 Sia $f(X) = X^4 + 10X^2 + 24 \in \mathbb{Z}[X]$. Allora $f(X) = g(X)h(X)$, ove $g(X) = \left(\frac{2}{3}X^2 + \frac{8}{3}\right), h(X) = \left(\frac{3}{2}X^2 + 9\right)$. Si prenda $c = \frac{3}{2}, c^{-1} = \frac{2}{3}$. Allora

$$g^*(X) = \frac{3}{2}\left(\frac{2}{3}X^2 + \frac{8}{3}\right) = X^2 + 4 \in \mathbb{Z}[X],$$

$$h^*(X) = \frac{2}{3}\left(\frac{3}{2}X^2 + 9\right) = X^2 + 6 \in \mathbb{Z}[X],$$

e $f(X) = g(X)h(X) = \frac{3}{2}g(X)\frac{2}{3}h(X) = g^*(X)h^*(X)$.

Dal Teorema 14.1, con un facile ragionamento induttivo, si deduce il seguente

Corollario 14.3 Sia $f(X) \in \mathbb{Z}[X]$ non costante. Sia

$$f(X) = p_1(X) \cdots p_s(X)$$

una sua fattorizzazione in $\mathbb{Q}[X]$. Allora esistono $c_1, \dots, c_s \in \mathbb{Q}^*$ tali che, per ogni $i = 1, \dots, s$, $p_i^*(X) = c_i p_i(X) \in \mathbb{Z}[X]$ e

$$f(X) = p_1^*(X) \cdots p_s^*(X).$$

Pertanto, il problema della fattorizzazione di un polinomio in $\mathbb{Q}[X]$ si riconduce al problema di determinare, per un polinomio di $\mathbb{Z}[X]$, una fattorizzazione in polinomi appartenenti a $\mathbb{Z}[X]$. I passaggi sono i seguenti:

1.) Dato $f(X) \in \mathbb{Q}[X]$, si determina $m \in \mathbb{Z}^*$ tale che $\tilde{f}(X) = mf(X) \in \mathbb{Z}[X]$.
2.) Si trova una fattorizzazione di $\tilde{f}(X)$ in $\mathbb{Q}[X]$ i cui fattori appartengano tutti a $\mathbb{Z}[X]$.
3.) Si trasforma tale fattorizzazione in una fattorizzazione di $f(X)$ moltiplicando uno dei fattori per m^{-1}.

Per il passaggio fondamentale 2.) esistono validi metodi, applicabili con buona generalità.

In base al primo corollario al Teorema di Ruffini (Corollario 12.7), determinare i fattori irriducibili di grado uno di un polinomio di $\mathbb{Z}[X]$ equivale a determinarne le radici in $\mathbb{Q}$.

Proposizione 14.4 *(Esistenza di radici razionali)* Sia $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$, non costante e sia $\alpha = \frac{r}{s}$ $(r, s \in \mathbb{Z}, s \neq 0, \mathrm{MCD}(r,s) = 1)$ una sua radice. Allora *s* divide a_n ed *r* divide a_0.

Dimostrazione: Per ipotesi si ha $0 = f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i = \sum_{i=0}^{n} a_i \frac{r^i}{s^i}$. Quindi

$$0 = s^n \sum_{i=0}^{n} a_i \frac{r^i}{s^i} = \sum_{i=0}^{n} a_i r^i s^{n-i} = a_0 s^n + \sum_{i=1}^{n-1} a_i r^i s^{n-i} + a_n r^n.$$

Il numero intero *s* divide tutta la somma, ed anche ciascuno dei termini di indici $i = 0, ..., n-1$. Segue che *s* divide anche l'addendo $a_n r^n$. Essendo r^n ed *s* coprimi, in virtù della Proposizione 6.24, segue che *s* divide a_n. Inoltre, anche *r* divide tutta la somma, ed anche ciascuno dei termini di indici $i = 1, ..., n$. Segue che *r* divide anche l'addendo $a_0 s^n$. Da ciò si deduce come sopra che *r* divide a_0. □

Esempio 14.5 Sia $f(X) = 2X^3 + X - 1 \in \mathbb{Z}[X]$. Se $\alpha = \frac{r}{s}$ $(r, s \in \mathbb{Z}, s \neq 0, \mathrm{MCD}(r,s) = 1)$ è una radice di $f(X)$, allora *s* divide $a_3 = 2$ ed *r* divide $a_0 = 1$. Dunque $s \in \{1, -1, 2, -2\}$, $r \in \{1, -1\}$. Segue che $\alpha \in \left\{1, -1, \frac{1}{2}, -\frac{1}{2}\right\}$. Ora

$$\begin{aligned}
f(1) &= \quad 2 + 1 - 1 = \quad 2 \\
f(-1) &= \quad -2 - 1 - 1 = \quad -4 \\
f\left(\frac{1}{2}\right) &= \quad \frac{1}{4} + \frac{1}{2} - 1 = \quad -\frac{1}{4} \\
f\left(-\frac{1}{2}\right) &= \quad -\frac{1}{4} - \frac{1}{2} - 1 = \quad -\frac{7}{4}
\end{aligned}$$

Quindi $f(X)$ non ha radici razionali. Per il secondo corollario al Teorema di Ruffini (Corollario 12.9), essendo $\deg(f) = 3$, segue che $f(X)$ è irriducibile in $\mathbb{Q}[X]$. □

Teorema 14.6 *(Criterio di irriducibilità di Eisenstein)* Sia $f(X)=\sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ non costante. Sia p un numero primo tale che

a) p non divide a_n;
b) p divide a_i per ogni $i=0,\ldots,n-1$;
c) p^2 non divide a_0.

Allora $f(X)$ è irriducibile in $\mathbb{Q}[X]$.

Dimostrazione: In base alla a), $a_n \neq 0$, quindi $\deg(f)=n.$ Supponiamo per assurdo che, nelle ipotesi assegnate, $f(X)$ sia riducibile in $\mathbb{Q}[X].$ Allora $f(X)$ è prodotto di due polinomi non costanti di $\mathbb{Q}[X].$ In base al Teorema 14.1 esistono quindi $g(X), h(X) \in \mathbb{Z}[X]$ non costanti tali che $f(X)=g(X)h(X).$ Siano $g(X)=\sum_{i=0}^{r} b_i X^i$, $h(X)=\sum_{i=0}^{s} c_i X^i$, ove $b_i \in \mathbb{Z}$ per ogni $i=0,\ldots,r$ e $c_i \in \mathbb{Z}$ per ogni $i=0,\ldots,s.$ Supponiamo inoltre che $\deg(g)=r$, $\deg(h)=s$, così che $b_r \neq 0$, $c_s \neq 0.$ Allora, in base alla formula del grado per il prodotto di polinomi, $n=r+s$, ove $1\leq r\leq n-1$, $1\leq s\leq n-1.$ Inoltre $a_0=b_0c_0.$ Dalla condizione b) e dalla definizione di numero primo (Definizione 7.1) segue che p divide b_0 oppure p divide c_0; d'altra parte, in virtù di c), non può dividerli entrambi. Possiamo supporre, senza ledere la generalità, che p divida b_0 e non divida c_0. Ora, si ha $a_n=b_rc_s$, e quindi, in base ad a), p non divide $b_r.$ Allora l'insieme $\{i \mid p \nmid b_i\} \subset \mathbb{N}$ è non vuoto, e dunque ammette un minimo k. Si noti che $1\leq k\leq r\leq n-1.$ Si ha

$$a_k=\sum_{i+j=k} b_i c_j=\sum_{i=0}^{k} b_i c_{k-i}=\sum_{i=0}^{k-1} b_i c_{k-i}+b_k c_0.$$

Ora, per la condizione b), p divide la somma a_k e, per definizione di k, p divide b_i per ogni $i=0,\ldots,k-1$, e quindi divide i primi k addendi della somma. Segue che p divide anche l'addendo $b_kc_0.$ Ciò, però, è impossibile, dato che p è primo e p non divide nessuno dei due fattori b_k e c_0. Abbiamo così trovato la contraddizione cercata, e provato che $f(X)$ è irriducibile in $\mathbb{Q}[X]$. □

Esempio 14.7 Per ogni numero primo p ed ogni intero positivo n, il polinomio $f(X)=X^n+p \in \mathbb{Z}[X]$ soddisfa le condizioni a), b), c) del Teorema 14.6, ed è quindi irriducibile in $\mathbb{Q}[X].$ Ciò mostra che, contrariamente a quanto avviene in $\mathbb{C}[X]$ (dove, in base al Corollario 13.6, i polinomi irriducibili hanno tutti grado uno) o in $\mathbb{R}[X]$ (dove, in base alla Proposizione 13.9, i polinomi irriducibili hanno grado al più due), in $\mathbb{Q}[X]$ esistono polinomi irriducibili di qualunque grado positivo.

Esempio 14.8 Il polinomio $f(X)=5X^4+2X^3-4X+6 \in \mathbb{Z}[X]$ è irriducibile in $\mathbb{Q}[X]$. Infatti esso verifica le ipotesi del Criterio di Eisenstein con $p=2$.

Osservazione 14.9 Il criterio di Eisenstein è un criterio solo *sufficiente*, e non necessario, di irriducibilità in $\mathbb{Q}[X]$. In altri termini, un polinomio $f(X) \in \mathbb{Z}[X]$ può essere irriducibile in $\mathbb{Q}[X]$ pur non verificando le condizioni a), b) e c) per alcun primo p. Come abbiamo visto nell'Esempio

14.5, il polinomio $f(X) = 2X^3 + X - 1 \in \mathbb{Z}[X]$ è irriducibile in $\mathbb{Q}[X]$, però non verifica la condizione b) per alcun primo *p*, poiché nessun primo *p* divide il termine noto –1.

Introduciamo ora il metodo della *riduzione modulo p.*

Definizione 14.10 Sia $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$. Sia *p* un numero primo. Allora il polinomio

$$\overline{f}(X) = \sum_{i=0}^{n} [a_i]_p X^i \in \mathbb{Z}_p[X]$$

si dice la *riduzione modulo p* di $f(X)$.

Per semplicità, nel seguito indicheremo le classi di resto con un soprassegno.

Esempio 14.11 Sia $f(X) = 3X^3 + 2X^2 - 5X + 4 \in \mathbb{Z}[X]$. Allora la sua riduzione modulo 2 è

$$\overline{f}(X) = X^3 + X \in \mathbb{Z}_2[X],$$

la sua riduzione modulo 3 è

$$\overline{f}(X) = \overline{2}X^2 + X + \overline{1} \in \mathbb{Z}_3[X],$$

la sua riduzione modulo 5 è

$$\overline{f}(X) = \overline{3}X^3 + \overline{2}X^2 + \overline{4} \in \mathbb{Z}_5[X].$$

Proposizione 14.12 *(Irriducibilità e riduzione modulo p)* Sia $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ non costante e sia *p* un primo tale che *p* non divide a_n. Sia $\overline{f}(X) = \sum_{i=0}^{n} \overline{a}_i X^i \in \mathbb{Z}_p[X]$ la riduzione di $f(X)$ modulo *p*. Allora, se $\overline{f}(X)$ è irriducibile in $\mathbb{Z}_p[X]$, $f(X)$ è irriducibile in $\mathbb{Q}[X]$.

<u>Dimostrazione</u>: Supponiamo che $f(X)$ sia riducibile in $\mathbb{Q}[X]$. Allora, in virtù del Teorema 14.1, esistono $g(X), h(X) \in \mathbb{Z}[X]$, di gradi $r, s \geq 1$ rispettivamente, tali che $f(X) = g(X)h(X)$. Siano *b* e *c* i coefficienti direttori di $g(X)$ ed $h(X)$ rispettivamente. Allora $a_n = bc$, quindi *p* non divide né *b* né *c*. Pertanto $\overline{b} \neq \overline{0}, \overline{c} \neq \overline{0}$ in $\mathbb{Z}_p$, e quindi $\deg(\overline{g}) = r, \deg(\overline{h}) = s$. Inoltre si ha

$$\overline{f}(X) = \overline{g}(X)\overline{h}(X).$$

Quindi $\overline{f}(X)$ è riducibile in $\mathbb{Z}_p[X]$. □

Esercizio 14.13* Provare che il polinomio $f(X) = X^4 + 2X^2 + 2 \in \mathbb{Z}[X]$ è irriducibile in $\mathbb{Q}[X]$.

(Suggerimento per lo svolgimento. Provare che la sua riduzione $\overline{f}(X)$ modulo 3 è irriducibile in $\mathbb{Z}_3[X]$, verificando, con opportuni calcoli, che essa non si decompone né nel prodotto di un fattore lineare ed un fattore di grado 3, né nel prodotto di due fattori di grado due.)

Osservazione 14.14 Il criterio di Eisenstein ed il metodo di riduzione modulo *p* hanno, in generale, campi di applicabilità diversi. Ad esempio, se $f(X)=X^3+6X+2$, il criterio di Eisenstein, applicato per $p=2$, ci consente di concludere che $f(X)$ è irriducibile in $\mathbb{Q}[X]$. Per contro, non è utile effettuare la riduzione modulo 2 ($\overline{f}(X)=X^3\in\mathbb{Z}_2[X]$ è riducibile) o la riduzione modulo 3 ($\overline{f}(X)=X^3+\overline{2}\in\mathbb{Z}_3[X]$ è riducibile, in quanto possiede la radice $\overline{1}\in\mathbb{Z}_3$.)