AL210 - Appunti integrativi - 7

Prof. Stefania Gabelli - a.a. 2016-2017

Fattorizzazione in anelli di polinomi

Poiché l'anello dei polinomi $K[X]$ in una indeterminata X su un campo K è un dominio euclideo, esso è anche un dominio a fattorizzazione unica. Daremo ora una dimostrazione diretta di questa importante proprietà, che meglio illustra l'analogia di comportamento tra $K[X]$ e $\mathbb{Z}$.

Ricordiamo che, se K è un campo, gli elementi invertibili di $K[X]$ sono tutte e sole le costanti non nulle. Dunque un polinomio non costante $f(X) \in K[X]$ è irriducibile se e soltanto se gli unici suoi divisori sono le costanti non nulle ed i polinomi del tipo $cf(X)$, con $c \in K^*$. Inoltre, un polinomio irriducibile su K è un elemento primo di $K[X]$. Quindi, un polinomio di grado positivo $p(X)$ è un polinomio irriducibile se e soltanto se, quando $p(X)$ divide un prodotto in $K[X]$, esso divide almeno uno dei fattori.

Proposizione 1 *Sia K un campo. Un polinomio non nullo $f(X) \in K[X]$ è riducibile su K se e soltanto se $f(X)$ ha un divisore $g(X) \in K[X]$ tale che $1 \leq \deg g(X) < \deg f(X)$. In particolare, se $\deg f(X) = 1$, allora $f(X)$ è irriducibile.*

Dimostrazione: Per la formula del grado, se $g(X)$ divide $f(X)$, deve essere $\deg g(X) \leq \deg f(X)$. Basta allora osservare che i polinomi di grado zero sono tutte le costanti non nulle, cioè gli elementi invertibili di $K[X]$, e che due polinomi associati hanno lo stesso grado. □

Teorema 2 (Teorema di Fattorizzazione Unica) *Se K è un campo, ogni polinomio di grado positivo $f(X) \in K[X]$ ha una fattorizzazione del tipo*

$$f(X) = cp_1(X)p_2(X)\dots p_s(X),$$

dove $c \in K^*$ e $p_1(X), p_2(X), \dots, p_s(X) \in K[X]$ sono polinomi monici irriducibili. Inoltre la costante c ed i polinomi $p_1(X)$, $p_2(X), \dots,$ $p_s(X)$ sono univocamente determinati (a meno dell'ordine).

Dimostrazione: Per dimostrare l'esistenza di una fattorizzazione, si procede per induzione sul grado di $f(X)$. Se $\deg f(X) = 1$, allora $f(X) = c(X-\alpha)$ è irriducibile (Proposizione 1). Supponiamo dunque che $\deg f(X) \geq$

2 e che il teorema sia vero per tutti i polinomi di grado inferiore. Se $f(X)$ non è irriducibile, possiamo scrivere $f(X) = g(X)h(X)$, con $1 \leq \deg g(X), \deg h(X) < \deg f(X)$ (Proposizione 1). Per l'ipotesi induttiva, $g(X)$ e $h(X)$ si possono fattorizzare nel modo richiesto, quindi anche $f(X)$ si può fattorizzare.

Per l'unicità, supponiamo che $f(X)$ abbia due fattorizzazioni del tipo richiesto,

$$f(X) = ap_1(X)p_2(X)\dots p_s(X) = bq_1(X)q_2(X)\dots q_t(X).$$

Poiché i polinomi $p_i(X)$ e $q_j(X)$ sono monici, $a = b$ è il coefficiente direttore di $f(X)$. Inoltre, $p_i(X)$ è un elemento primo di $K[X]$ per ogni $i = 1, \dots, s$. Quindi ad esempio $p_1(X)$, dividendo $f(X)$, divide uno dei polinomi $q_j(X)$. A meno di riordinare i fattori, possiamo supporre che $p_1(X)$ divida $q_1(X)$. Allora, essendo $p_1(X)$ e $q_1(X)$ entrambi irriducibili e monici, deve essere $p_1(X) = q_1(X)$. Quindi $p_1(X)$ si può cancellare e

$$p_2(X)\dots p_s(X) = q_2(X)\dots q_t(X).$$

Così proseguendo, si ottiene che $s = t$ e $p_i(X) = q_i(X)$ per $i = 1, \dots, s$. □

La proprietà di fattorizzazione unica implica che il massimo comune divisore monico di due polinomi non costanti di $K[X]$ è il prodotto di tutti i polinomi monici irriducibili, non necessariamente distinti, che dividono entrambi i polinomi.

Polinomi su un dominio a fattorizzazione unica

Se A è un dominio con campo delle frazioni K, la differenza nel fattorizzare un polinomio $f(X) \in A[X]$ su A oppure su K consiste nel fatto che in $A[X]$ ci possono essere polinomi costanti irriducibili, contrariamente a quanto avviene in $K[X]$ dove tutte le costanti non nulle sono invertibili. Tuttavia, se A è un dominio a fattorizzazione unica, questa difficoltà può essere aggirata usando le proprietà del massimo comune divisore. Faremo infatti vedere che, se A è un dominio a fattorizzazione unica, un polinomio a coefficienti in A che si fattorizza su K può essere fattorizzato anche su A e illustreremo dei criteri di irriducibilità. I metodi usati saranno particolarmente utili per lo studio della fattorizzazione dei polinomi in più indeterminate a coefficienti interi o razionali.

Il lemma di Gauss

Il risultato principale di questo paragrafo mostra che, se A è un dominio a fattorizzazione unica, un anello di polinomi a coefficienti in A è ancora un dominio a fattorizzazione unica. Questo è un risultato molto importante ed

implica ad esempio che tutti gli anelli di polinomi a coefficienti interi oppure in un campo sono domini a fattorizzazione unica. Il metodo che useremo per dimostrarlo è dovuto a Gauss: in una indeterminata, esso consiste nel fattorizzare un polinomio a coefficienti in A sul campo delle frazioni K di A e da questa fattorizzazione ricavare poi una fattorizzazione in $A[X]$.

Ricordiamo che in un dominio a fattorizzazione unica il massimo comune divisore d di due elementi non nulli x, y è determinato a meno di elementi invertibili. Mantenendo al solito questa ambiguità di definizione, scriveremo $(x, y) = d$.

Se A è un dominio a fattorizzazione unica e $f(X) \in A[X]$, un qualsiasi massimo comune divisore dei coefficienti di $f(X)$ si chiama il *contenuto* di $f(X)$ e si denota con $\mathbf{c}(f)$. Se $\mathbf{c}(f) = 1$, si dice che $f(X)$ è un polinomio *primitivo*.

Se A è un dominio con campo delle frazioni K e $f(X) \in K[X]$ è un polinomio non nullo, riducendo i coefficienti di $f(X)$ a un denominatore comune d, si può sempre scrivere

$$f(X) = \frac{1}{d} f_1(X)\,; \quad \text{con } f_1(X) \in A[X].$$

Se poi A è un dominio a fattorizzazione unica, si ha anche

$$f(X) = \frac{\mathbf{c}(f_1)}{d} g(X)\,; \quad \text{con } g(X) \in A[X] \text{ un polinomio primitivo.}$$

Quindi, se A è un dominio a fattorizzazione unica, ogni polinomio di $K[X]$ è associato su K ad un polinomio primitivo di $A[X]$. Questa semplice osservazione fa intuire che i polinomi primitivi di $A[X]$ si comportano come i polinomi a coefficienti in K.

Il seguente lemma segue immediatamente dalle proprietà delle operazioni in $A[X]$ e dal Principio di Identità dei Polinomi.

Lemma 3 *Ogni omomorfismo di anelli commutativi unitari $\varphi : A \longrightarrow A'$ si può estendere ad un omorfismo $\varphi^* : A[X] \longrightarrow A'[X]$ ponendo*

$$\varphi^*(c_0 + c_1X + \cdots + c_nX^n) = \varphi(c_0) + \varphi(c_1)X + \cdots + \varphi(c_n)X^n.$$

Inoltre φ è iniettivo (suriettivo) se e soltanto se φ^* è iniettivo (suriettivo).

Se I è un ideale di A, di particolare interesse è l'omomorfismo suriettivo di anelli

$$\pi^* : A[X] \longrightarrow \frac{A}{I}[X]$$

che estende la proiezione canonica

$$\pi : A \longrightarrow \frac{A}{I}\,; \quad a \mapsto \overline{a} := a + I$$

ed è quindi definito da

$$c_0 + c_1X + \cdots + c_nX^n \mapsto \overline{f}(X) := \overline{c_0} + \overline{c_1}X + \cdots + \overline{c_n}X^n.$$

Se A è un dominio e p è un elemento primo di A, l'anello quoziente $A/\langle p\rangle$ è un dominio. In questo caso anche gli anelli di polinomi a coefficienti in $A/\langle p\rangle$ sono domini e l'omomorfismo

$$\pi^* : A[X] \longrightarrow \frac{A}{\langle p\rangle}[X]\,; \quad f(X) \mapsto \overline{f}(X)$$

si chiama la *riduzione modulo p*.

Proposizione 4 (Lemma di Gauss) *Sia A un dominio a fattorizzazione unica e sia $f(X) \in A[X]$ un polinomio non nullo. Se $f(X) = g(X)h(X)$, allora $\mathbf{c}(f)$ e $\mathbf{c}(g)\mathbf{c}(h)$ sono elementi associati di A. In particolare, il prodotto di due polinomi primitivi di $A[X]$ è un polinomio primitivo.*

Dimostrazione: Sia $p \in A$ un fattore irriducibile di $\mathbf{c}(f)$. Poiché p è un elemento primo di A, l'anello di polinomi $(A/\langle p\rangle)[X]$ è un dominio. Riducendo $f(X) = g(X)h(X)$ modulo p, si ottiene $\overline{0} = \overline{f}(X) = \overline{g}(X)\overline{h}(X)$. Quindi deve risultare $\overline{g}(X) = \overline{0}$ oppure $\overline{h}(X) = \overline{0}$. Questo significa che p divide tutti i coefficienti di $g(X)$, cioè $\mathbf{c}(g)$, oppure tutti i coefficienti di $h(X)$, cioè $\mathbf{c}(h)$. Viceversa, per come è definita la moltiplicazione tra polinomi, ogni elemento primo di A che divide $\mathbf{c}(g)$ oppure $\mathbf{c}(h)$ divide anche $\mathbf{c}(f)$. Quindi, per l'unicità della fattorizzazione in A, $\mathbf{c}(f)$ e $\mathbf{c}(g)\mathbf{c}(h)$ sono elementi associati. □

Corollario 5 *Sia A un dominio a fattorizzazione unica con campo delle frazioni K e sia $f(X) \in A[X]$ un polinomio di grado positivo. Se $f(X) = g(X)h(X)$, con $g(X)$, $h(X) \in K[X]$, allora esiste una costante non nulla $\lambda \in K$ tale che $\lambda g(X)$, $\lambda^{-1}h(X) \in A[X]$. In particolare, se $f(X)$ è riducibile su K, $f(X)$ è riducibile anche su A.*

Dimostrazione: Supponiamo che $f(X) = g(X)h(X)$, con $g(X)$, $h(X) \in K[X]$. Siano d_1 e d_2 denominatori comuni dei coefficienti di $g(X)$ e $h(X)$ rispettivamente. Moltiplicando per $d := d_1d_2$, otteniamo $df(X) = g_1(X)h_1(X)$, con $g_1(X)$, $h_1(X) \in A[X]$. Per il Lemma di Gauss, si ha $d\mathbf{c}(f) = \mathbf{c}(g_1)\mathbf{c}(h_1)$; quindi, per la proprietà di fattorizzazione unica in A, risulta $d = ab$ con a che divide $\mathbf{c}(g_1)$ e b che divide $\mathbf{c}(h_1)$. Ne segue che i polinomi $g_2(X) := a^{-1}g_1(X)$ e $h_2(X) := b^{-1}h_1(X)$ hanno coefficienti in A e $f(X) = g_2(X)h_2(X)$. Infine, $g(X)$ e $g_2(X)$ sono associati su K e, posto $g_2(X) := \lambda g(X)$, $\lambda \in K$, si ottiene $h_2 = \lambda^{-1}h(X)$.

Se poi $f(X)$ è riducibile su K, si ha $f(X) = g(X)h(X)$, con $g(X) \in K[X]$ di grado positivo strettamente minore di quello di $f(X)$. Allora $f(X) = \lambda g(X)\lambda^{-1}h(X)$ con $\lambda g(X), \lambda^{-1}h(X) \in A[X]$ e $0 < \deg g(X) = \deg \lambda g(X) < \deg f(X)$. Quindi $\lambda g(X)$ è un divisore proprio di $f(X)$ in $A[X]$ e $f(X)$ è riducibile anche su A. □

Corollario 6 *Sia A un dominio a fattorizzazione unica con campo delle frazioni K e sia $f(X) \in A[X]$ un polinomio di grado positivo. Allora $f(X)$ è irriducibile su A se e soltanto se $f(X)$ è primitivo e irriducibile su K.*

Dimostrazione: Se $f(X)$ è irriducibile in $A[X]$, i suoi unici divisori costanti sono gli elementi invertibili di A; quindi $f(X)$ è un polinomio primitivo. Inoltre $f(X)$ è irriducibile su K per il Corollario 5.

Viceversa, sia $f(X) \in A[X]$ primitivo e irriducibile su K. Allora $f(X)$ non ha in $K[X]$ divisori propri di grado positivo e quindi i suoi eventuali divisori propri in $A[X]$ sono tutti costanti. Ma, essendo $f(X)$ primitivo, i suoi divisori in A sono soltanto le costanti invertibili. Quindi $f(X)$ è irriducibile in $A[X]$. □

Corollario 7 *Sia A un dominio a fattorizzazione unica con campo delle frazioni K. I polinomi irriducibili di $A[X]$ sono:*

(a) *Gli elementi irriducibili di A;*

(b) *I polinomi primitivi di grado positivo di $A[X]$ che sono irriducibili in $K[X]$.*

Dimostrazione: Per la formula del grado, un polinomio di $A[X]$ costante e non nullo non può avere fattori di grado positivo. Quindi un polinomio costante $p \in A$ è irriducibile in $A[X]$ se e soltanto se è un elemento irriducibile di A.

Inoltre, per il Corollario 6, un polinomio di grado positivo di $A[X]$ è irriducibile su A se e soltanto se è primitivo e irriducibile in $K[X]$. □

Teorema 8 *Se A è un dominio a fattorizzazione unica anche $A[X]$ è un dominio a fattorizzazione unica. Precisamente, ogni polinomio non nullo e non invertibile $f(X) \in A[X]$ ha una fattorizzazione del tipo*

$$f(X) = p_1 p_2 \dots p_s q_1(X) q_2(X) \dots q_t(X),$$

dove, se $\mathbf{c}(f) \neq 1$, i p_i sono elementi irriducibili di A e, se $\deg f(X) \geq 1$, i $q_j(X)$ sono polinomi primitivi irriducibili di $A[X]$, univocamente determinati a meno dell'ordine e di elementi invertibili di A.

Dimostrazione: Possiamo scrivere $f(X) = \mathbf{c}(f) f_1(X)$, con $\mathbf{c}(f) \in A$ e $f_1(X) \in A[X]$ primitivo. Se $\mathbf{c}(f)$ non è invertibile, esso ha in A una fattorizzazione $\mathbf{c}(f) = p_1 p_2 \dots p_s$ in elementi irriducibili univocamente determinati, a meno dell'ordine e di elementi invertibili di A.

Inoltre, se $f_1(X)$ ha grado positivo e K è il campo delle frazioni di A, possiamo fattorizzare $f_1(X)$ in polinomi irriducibili su K, univocamente determinati a meno dell'ordine e di costanti non nulle di K (Teorema 2). Per il Corollario 5, moltiplicando ogni fattore per una opportuna costante,

otteniamo una fattorizzazione $f_1(X) = q_1(X)q_2(X)\dots q_t(X)$ in polinomi di $A[X]$, irriducibili su K e necessariamente primitivi per il Lemma di Gauss. Poiché i fattori p_i e $q_j(X)$ sono elementi irriducibili di $A[X]$ (Corollario 7), concludiamo che $A[X]$ è un dominio a fattorizzazione unica. □

Corollario 9 *Sia A un dominio e sia $\mathbf{X} := \{X_1, \dots, X_n\}$ un insieme di indeterminate indipendenti su A. Se A è un dominio a fattorizzazione unica, anche $A[\mathbf{X}]$ è un dominio a fattorizzazione unica. In particolare, $\mathbb{Z}[\mathbf{X}]$ è un dominio a fattorizzazione unica e, se K è un campo, $K[\mathbf{X}]$ è un dominio a fattorizzazione unica.*

Dimostrazione: Segue dal Teorema 8 per induzione sul numero delle indeterminate. Inoltre, poiché $\mathbb{Z}$ e $K[X]$ sono a fattorizzazione unica (Teorema 2), anche $\mathbb{Z}[\mathbf{X}]$ e $K[\mathbf{X}]$ lo sono. □

Esempio 10 (1) Se A è un dominio ma non è un campo, l'anello dei polinomi $A[X]$ non è mai ad ideali principali; ad esempio, l'anello dei polinomi $\mathbb{Z}[X]$ non è a ideali principali, anche se lo è $\mathbb{Z}$.

Infatti, se $a \in A$ è non nullo e non invertibile, l'ideale $\langle a, X\rangle = \{ac + Xf(X)\,; c \in A, f(X) \in A[X]\}$ non è principale. Per vedere questo, supponiamo che $\langle a, X\rangle = \langle g(X)\rangle$. Allora il polinomio $g(X)$, dividendo la costante a, deve essere un polinomio costante per la formula del grado. Inoltre, poiché $g(X)$ divide X e X è monico, deve essere $g(X) := u$ invertibile in A. Ma allora $\langle a, X\rangle = \langle u\rangle = A$, mentre $1 \notin \langle a, X\rangle$.

In modo simile si vede che, se K è un campo e $n \geq 2$, l'anello $K[X_1, \dots, X_n]$ non è a ideali principali. Ad esempio, poiché le indeterminate sono elementi irriducibili, l'ideale $\langle X_1, X_2\rangle$ non è principale.

(2) Il Lemma di Gauss (Proposizione 4) vale più generalmente per gli anelli di polinomi a coefficienti in un dominio con il massimo comune divisore. Da questo fatto segue che se A è un dominio con il massimo comune divisore, anche gli anelli di polinomi $A[X_1, \dots, X_n]$ in un numero finito di indeterminate indipendenti su A sono domini con il massimo comune divisore.

Criteri di irriducibilità

Abbiamo visto che, se A è un dominio a fattorizzazione unica con campo delle frazioni K e $f(X) \in K[X]$ è un polinomio di grado positivo, possiamo scrivere $f(X) = cf_1(X)$, con $c \in K^*$ e $f_1(X) \in A[X]$ primitivo. Poiché $f(X)$ è irriducibile su K se e soltanto se lo è $f_1(X)$, per stabilire se $f(X)$ è irriducibile su K, per il Lemma di Gauss, basta allora stabilire se $f_1(X)$ è irriducibile su A (Corollario 5). Nel seguito di questo paragrafo daremo alcuni criteri utili a questo scopo. Notiamo però che un polinomio può essere irriducibile anche senza soddisfare le ipotesi di alcun criterio di irriducibilità.

Teorema 11 (Criterio di Irriducibilità di F. G. Eisenstein, 1850) *Sia A un dominio a fattorizzazione unica con campo delle frazioni K e sia $f(X) := a_0 + a_1X + \cdots + a_nX^n \in A[X]$ un polinomio primitivo di grado $n \geq 1$. Se esiste un elemento primo $p \in A$ tale che:*

1. *p divide $a_0, \ldots, a_{n-1}$;*
2. *p non divide a_n;*
3. *p^2 non divide a_0;*

allora $f(X)$ è irriducibile su A e su K.

Dimostrazione: Sia $p \in A$ come nelle ipotesi e supponiamo che $f(X) = g(X)h(X)$ con $g(X) := b_0 + b_1X + \cdots + b_sX^s$ e $h(X) := c_0 + c_1X + \cdots + c_tX^t$ polinomi a coefficienti in A. Poiché $a_n = b_sc_t$ e p non divide a_n, allora p non divide né b_s né c_t. Inoltre, poiché $a_0 = b_0c_0$, p divide a_0 e p^2 non divide a_0, per la proprietà di fattorizzazione unica, p divide soltanto uno tra gli elementi b_0 e c_0. Supponiamo che p divida b_0 e non divida c_0. Sia s il più piccolo numero intero positivo tale che p non divida b_s, $1 \leq s \leq n$. Poiché $a_s = b_0c_s + b_1c_{s-1} + \cdots + b_sc_0$ e p divide $b_0, \ldots, b_{s-1}$ ma non divide né b_s né c_0, allora p non divide a_s. Dalle ipotesi, segue che $s = n$; ovvero $f(X)$ e $g(X)$ hanno lo stesso grado e $h(X) := c$ è una costante. Poiché abbiamo supposto che $f(X)$ sia primitivo, si ha che c è invertibile in A. Ne segue che $f(X)$ è irriducibile in $A[X]$ e quindi anche in $K[X]$ per il Corollario 6. □

Esempio 12 (1) Se A è un dominio a fattorizzazione unica con campo delle frazioni K e $q \in A$ è un elemento irriducibile, il polinomio $X^n + q$ è irriducibile su K per ogni $n \geq 1$. Ad esempio, il polinomio $X^n \pm p \in \mathbb{Z}[X]$ è irriducibile su $\mathbb{Q}$ per ogni numero primo p.

(2) Se F è un campo, il polinomio $X^n \pm Y \in F[X, Y] = (F[Y])[X]$ è irriducibile su $F(Y)$, e quindi anche su F. Infatti $F[Y]$ è un dominio a fattorizzazione unica e l'indeterminata Y è un elemento irriducibile di $F[Y]$.

(3) Per fornire un'applicazione del suo criterio, Eisenstein ha dimostrato nel seguente modo l'irriducibilità su $\mathbb{Q}$ del p-simo polinomio ciclotomico

$$\Phi_p(X) := \frac{X^p - 1}{X - 1} = X^p + X^{p-1} + \cdots + X + 1,$$

con $p \geq 2$ primo.

Con il cambio di variabile $X = T + 1$, si ottiene il polinomio

$$\begin{aligned}\widetilde{\Phi_p}(T) &:= \frac{(T+1)^p - 1}{(T+1) - 1} = \frac{(T+1)^p - 1}{T} \\ &= T^{p-1} + \binom{p}{1}T^{p-2} + \cdots + \binom{p}{p-2}T + \binom{p}{p-1}.\end{aligned}$$

Poiché p divide tutti i coefficienti binomiali $\binom{p}{k} := \frac{p!}{k!(p-k)!}$, per $k = 1, \ldots, p-1$, ma p^2 non divide il termine noto $\binom{p}{p-1} = p$, il polinomio $\widetilde{\Phi_p}(T)$ è irriducibile e quindi anche $\Phi_p(X)$ è irriducibile.

(4) Con il cambio di variabile $X = 1/T$ otteniamo la seguente *versione reciproca* del Criterio di Irriducibilità di Eisenstein:

Sia A un dominio a fattorizzazione unica con campo delle frazioni K e sia $f(X) := a_0 + a_1X + \cdots + a_nX^n \in A[X]$ un polinomio primitivo non costante. Se esiste un elemento primo $p \in A$ tale che:

1. p divide $a_1, \ldots, a_n$;
2. p non divide a_0;
3. p^2 non divide a_n;

allora $f(X)$ è irriducibile su A e su K.

Nel prossimo criterio di irriducibilità si usa la riduzione modulo un elemento primo p, ovvero l'omomorfismo

$$\pi^* : A[X] \longrightarrow \frac{A}{\langle p \rangle}[X]\,; \quad f(X) \mapsto \overline{f}(X)$$

che estende la proiezione canonica $\pi : A \longrightarrow A/\langle p \rangle$. Diremo che un polinomio $f(X) \in A[X]$ è *irriducibile modulo* p se $\overline{f}(X)$ è irriducibile su $A/\langle p \rangle$.

Teorema 13 (Criterio di Irriducibilità modulo p) *Sia A un dominio a fattorizzazione unica e sia $f(X) := a_0 + a_1X + \cdots + a_nX^n \in A[X]$ un polinomio primitivo di grado $n \geq 1$. Se esiste un elemento primo $p \in A$ tale che:*

1. *p non divide a_n;*
2. *$f(X)$ è irriducibile modulo p;*

allora $f(X)$ è irriducibile su A e su K.

Dimostrazione: Poiché $f(X)$ è primitivo, se $f(X)$ è riducibile su A, esistono $g(X) = b_sX^s + \cdots + b_0$, $h(X) = c_tX^t + \cdots + c_0 \in A[X]$ di grado positivo s e t tali che $f(X) = g(X)h(X)$. Poiché p non divide $a_n = b_sc_t$, allora p non divide né b_s né c_t. Riducendo modulo p, otteniamo $\overline{f}(X) = \overline{g}(X)\overline{h}(X)$, con $\deg g(X) = \deg \overline{g}(X) = s \geq 1$ e $\deg h(X) = \deg \overline{h}(X) = t \geq 1$. Quindi $\overline{f}(X)$ è riducibile modulo p. Infine, se $f(X)$ è irriducibile in $A[X]$, lo è anche in $K[X]$ per il Corollario 6. □

Il Criterio di Irriducibilità modulo p è particolarmente utile quando $A = \mathbb{Z}$. In questo caso infatti $\mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$ è un un campo finito con p elementi.

Esempio 14 **(1)** Riducendo modulo 3 il polinomio

$$f(X) := 5X^3 - 562X + 1400 \in \mathbb{Z}[X]$$

si ottiene il polinomio

$$\overline{f}(X) = 2X^3 + X + 2 \in \mathbb{F}_3[X].$$

Poiché $\overline{f}(0) = \overline{f}(1) = \overline{f}(2) = 2$, allora $\overline{f}(X)$ non ha radici in $\mathbb{F}_3$. Ne segue che $\overline{f}(X)$, essendo di terzo grado, è irriducibile su $\mathbb{F}_3$ e quindi $f(X)$ è irriducibile su $\mathbb{Q}$.

(2) Il polinomio

$$f(X) := X^5 - 5X^4 - 6X - 1 \in \mathbb{Z}[X]$$

è riducibile modulo 2. Infatti su $\mathbb{F}_2$ risulta

$$\overline{f}(X) = X^5 + X^4 + 1 = (X^2 + X + 1)(X^3 + X + 1).$$

Però $f(X)$ è irriducibile su $\mathbb{Q}$, ad esempio perché lo è modulo 3. Per vedere questo, osserviamo che i soli polinomi di secondo grado irriducibili su $\mathbb{F}_3$ sono

$$X^2 + 1\,; \quad X^2 + X + 1\,; \quad X^2 + 2X + 2;$$

ma nessuno di questi polinomi divide $\overline{f}(X)$.