Campi e polinomi irriducibili

$\mathbb{K}[x]/(f(x))$ è campo se e solo se $f(x)$ è irriducibile.

Se $f(x) = g(x)\,h(x)$ con $MCD(g(x), h(x)) = 1$, allora, per il Teorema cinese del resto, si ha che:

$$\mathbb{K}[x]/(f(x)) \cong \mathbb{K}[x]/(g(x)) \times \mathbb{K}[x]/(h(x))$$

Questo non è mai un campo, perché ammette divisori di zero (e.g. $(1,0)\cdot(0,1) = (0,0)$).

Criteri di riducibilità

es. Sia $f: A_1 \to A_2$ un omomorfismo, allora

$\varphi : A_1[x] \to A_2[x]$, $a_1 + a_2 x + \cdots \mapsto f(a_1) + f(a_2)x + \cdots$

è un omomorfismo.

es. $x^3 + 5x + 1$ in $\mathbb{Z}[x]$ $\quad \varphi : \mathbb{Z}[x] \to \mathbb{Z}_2[x]$

$\varphi(x^3 + 5x + 1) = \underbrace{x^3 + x + 1}_{\text{irriducibile}} \implies x^3 + 5x + 1$ è irriducibile

In generale dati $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$, $p \nmid a_n$

e $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, $\varphi(f(x))$ irriducibile $\Rightarrow$

$\Rightarrow f(x)$ irriducibile.

Criterio di Eisenstein Sia $f(x) \in \mathbb{Z}[x]$ e p primo t.c.

(i) $p \nmid a_n$

(ii) $p \mid a_i$, $i = 0 \to n-1$

(iii) $p^2 \nmid a_0$

Allora $f(x)$ è IRRIDUCIBILE.

Supponiamo che $f(x) = h(x)\, g(x)$ con $\deg h(x), \deg g(x) \geq 1$.

Si applichi φ:

$$\begin{cases} \varphi(f(x)) = [a_n]_p x^n \\ \varphi(f(x)) = \varphi(h(x))\, \varphi(g(x)) \end{cases} \Rightarrow \begin{cases} \varphi(h(x)) = [h_a]\, x^a \\ \varphi(g(x)) = [g_b]\, x^b \end{cases} \Rightarrow$$

$$\Rightarrow p \mid h_0 \wedge p \mid g_0 \xRightarrow{\text{moltiplicati tra loro}} p^2 \mid a_0 \text{, } \lightning \Rightarrow f(x) \text{ irriducibile}$$

Teorema delle radici razionali Sia $f(x) \in \mathbb{Q}[x]$, allora ogni sua radice razionale $\frac{p}{q}$ (con $(p,q) = 1$), se esiste, è t.c.

(i) $p \mid a_0$

(ii) $q \mid a_n$

Def. $f(x) \in \mathbb{Z}[x]$ si dice **PRIMITIVO** se $(a_n, a_{n-1}, \dots, a_0) = 1$.

Lemma di Gauss Il prodotto di due polinomi primitivi è ancora primitivo

Siano $f(x) = \sum_{i=0}^{n} a_i x^i$ e $g(x) = \sum_{i=0}^{m} b_i x^i$ primitivi. Se $f(x)g(x)$ non è primitivo allora $\exists p$ t.c. $p \mid c_i \ \forall i$, dove i c_i sono i coefficienti di $f(x)g(x)$.

Si consideri la coppia dei coefficienti a_s, b_r t.c. siano i massimi coefficienti dei rispettivi polinomi non divisibili per p. Si consideri il coefficiente c_{s+r}:

$$c_{s+r} = \sum_{\substack{i+j=s+r \\ i \leq n \\ j \leq m}} a_i b_j = a_s b_r + \sum_{\substack{i+j=s+r \\ i \leq n \wedge i \neq r \\ j \leq m}} a_i b_j$$

Nel caso $i \neq r$, almeno uno dei due coefficienti supera in indice il rispettivo coefficiente massimo stabilito. Quindi $p \mid \sum_{\substack{i+j=s+r \\ i \leq n \wedge i \neq r \\ j \leq m}} a_i b_j$. Allora, poiché $p \mid c_{s+r}$, $p \mid a_s b_r \Rightarrow$

$\Rightarrow p \mid a_s \vee p \mid b_r$, assurdo $\lightning$. $\boxtimes$

Corollario $\deg f(x) > 0$. $f(x) \in \mathbb{Z}[x]$ irriducibile in $\mathbb{Z}[x]$ $\Longleftrightarrow$ $f(x)$ è primitivo e irriducibile in $\mathbb{Q}[x]$

(i) $\Rightarrow$ (ii): Assumiamo $f(x)$ primitivo, altrimenti $\exists p \in \mathbb{Z} \mid p \mid f(x)$, e quindi $f(x)$ non sarebbe irriducibile in $\mathbb{Z}[x]$. Infatti verrebbe $f(x) = p\, g(x)$ con $\deg g(x) > 0$, e quindi, poiché $p \notin \mathbb{Z}[x]^* \wedge g(x) \notin \mathbb{Z}[x]^*$, $f(x)$ non sarebbe irriducibile.

Sia allora $f(x)$ primitivo in $\mathbb{Z}[x]$. Assumiamo $f(x) = a(x)\, b(x)$, $a(x), b(x) \in \mathbb{Q}[x]$ di grado positivo (ossia che $f(x)$ è riducibile in $\mathbb{Q}[x]$) $\exists\, \alpha, \beta \in \mathbb{Q} \mid a'(x) = \alpha\, a(x)$, $b'(x) = \beta\, b(x)$ t.c. $a'(x), b'(x) \in \mathbb{Z}[x]$ e primitivi. Infatti:

$$\underbrace{\frac{\left(\frac{p_0}{q_0}\frac{m}{d}, \dots, \frac{p_n}{q_n}\frac{m}{d}\right)}{\overbrace{[q_0, \dots, q_n]}^{m}\ \underbrace{(p_0, \dots, p_n)}_{d}}}_{\alpha} \underbrace{\left(\frac{p_0}{q_0} + \frac{p_1}{q_1}x + \dots + \frac{p_n}{q_n}x^n\right)}_{a(x)} \quad \text{con}$$

$(p_0, q_0) = \dots = (p_n, q_n) = 1$ è primitivo e appartenente a $\mathbb{Z}[x]$. Per il lemma di Gauss $a'(x)\, b'(x) = \alpha\beta\, f(x)$ è primitivo.

Innanzitutto $\alpha\beta \in \mathbb{Z}$, altrimenti $\alpha\beta\, f(x) \notin \mathbb{Z}[x]$, $\lightning$.

Inoltre $\alpha\beta = \pm 1$, altrimenti $\alpha\beta f(x)$ non sarebbe primitivo. Allora $f(x) = \pm\, a'(x)\, b'(x)$, ossia è prodotto di non invertibili, quindi riducibile.

Quindi $f(x)$ non primitivo o riducibile in $\mathbb{Q}[x] \Rightarrow$

$\rightarrow f(x)$ riducibile in $\mathbb{Z}[x]$, dunque

$f(x)$ irriducibile in $\mathbb{Z}[x] \Rightarrow f(x)$ primitivo e irriducibile in $\mathbb{Q}[x]$.

(ii) $\Rightarrow$ (i): Se $f(x)$ fosse riducibile in $\mathbb{Z}[x]$, lo sarebbe anche in $\mathbb{Q}[x]$, $\lightning$.

$\boxtimes$