[Criterio di irriducibilità Eisenstein]
Dato A UFD e $f(x) \in A[x]$ primitivo, con $f(x) = \sum_{i=0}^{n} a_i x^i$, e $p \in A$ un primo tale che:

1. $p \nmid a_n$.
2. $p \mid a_i$, $\forall i \in \{0, \ldots, n-1\}$.
3. $p^2 \nmid a_0$.

Allora $f(x)$ è irriducibile in $A[x]$ (quindi in $K[x]$, con K campo dei quozienti di A).

La dimostrazione è simile a quella già trattata in Aritmetica, con la differenza che in questo caso utilizziamo un UFD generico al posto di Z.
Posso supporre $\deg f(x) = n \geq 2$: infatti un polinomio primitivo di primo grado ($\deg f(x) = 1$) è sempre irriducibile su $K[x]$ (e quindi su $A[x]$), perché, per questioni di grado, si può fattorizzare solo come un altro polinomio di primo grado per una costante non nulla (altrimenti anche $f(x)$ sarebbe nullo) ed, essendo K un campo, ogni costante non nulla è invertibile; mentre se $f(x)$ fosse una costante ($\deg f(x) = 0$) allora non sarebbero soddisfatte le ipotesi, perché si avrebbe $p \nmid a_n$ e $p \mid a_0$ ma $a_n = a_0 = f(x)$, assurdo.
Supponiamo per assurdo che $f(x)$ sia riducibile in $A[x]$, allora:

$$f(x) = g(x)h(x)$$

con $\deg g(x) = m \geq 1$, $\deg h(x) = n - m \geq 1$ e supponiamo (WLOG) che $m \geq n - m$. [1] Possiamo applicare la proiezione al quoziente modulo (p), e per le ipotesi si ha:

$$\pi_{(p)}(f(x)) = \overline{f(x)} = \overline{a_n} x^n \neq \overline{0}$$

e inoltre:

$$\pi_{(p)}(f(x)) = \pi_{(p)}(g(x))\pi_{(p)}(h(x))$$

con:

$$\pi_{(p)}(g(x)) = \overline{b_m} x^m + \ldots + \overline{b_0} \qquad \text{e} \qquad \pi_{(p)}(h(x)) = \overline{c_{n-m}} x^{n-m} + \ldots + \overline{c_0}$$

[1] Posso supporre questi gradi ≥ 1 perché se, per assurdo, $f(x)$ si potesse spezzare solo come prodotto di un polinomio dello stesso grado per una costante non nulla, allora questa costante divide $f(x)$, in particolare divide tutti i suoi coefficienti, dunque divide il loro M.C.D, cioè $c(f(x))$, che è uguale a 1, perché f è primitivo; ma questo può accadere soltanto se la costante è invertibile, quindi $f(x)$ era irriducibile.

Per concludere basta mostrare che $\overline{b_0} = \overline{c_0} = 0$, infatti da questo segue che $b_0 \equiv c_0 \equiv 0 \pmod{p} \implies a_0 = b_0c_0 \equiv 0 \pmod{p^2} \implies p^2 \mid a_0$ che è assurdo. Intanto osserviamo che tutti i coefficienti stanno in $\dfrac{A}{(p)}$ che è un dominio, perché p primo (proposizione 2.56). [2] Dato che $\overline{b_0}\overline{c_0} = \overline{a_0} = 0$, abbiamo che o $\overline{b_0} = 0$ o $\overline{c_0} = 0$. Sia (WLOG) $\overline{b_0} = 0$ e supponiamo, per assurdo, che $\overline{c_0} \neq 0$. Allora si dimostra per induzione (forte) che tutti i coefficienti di $\overline{g(x)}$ sono nulli. Infatti si può scrivere:

$$\overline{f(x)} = \overline{g(x)h(x)} = \sum_{k=0}^{n} \Big(\sum_{\substack{0 \leq i \leq m \\ 0 \leq j \leq n-m \\ i+j=k}} \overline{b_i}\overline{c_j} \Big) x^k$$

Abbiamo già visto che il caso base $\overline{b_0} = 0$ vale. Sia $k \leq m$ e supponiamo che $\overline{b_h} = 0 \quad \forall\ 0 \leq h \leq k-1$, allora

$$\sum_{\substack{0 \leq i \leq m \\ 0 \leq j \leq n-m \\ i+j=k}} \overline{b_i}\overline{c_j} = b_k c_0 = 0 \implies b_k = 0$$

che mostra in particolare $\overline{b_m} = 0$, che è assurdo perché $\overline{b_m}\overline{c_{n-m}} = \overline{a_n} \neq 0$. Perciò anche $\overline{c_0} = 0$ e si potrebbe già concludere per quanto detto sopra. In realtà continuando per induzione con questo procedimento si può mostrare che tutti i coefficienti di $\overline{g(x)}$ e $\overline{h(x)}$ tranne quelli direttori sono nulli cioè:

$$\pi_{(p)}(g(x)) = \overline{g(x)} = \overline{b_m}x^m \qquad \text{e} \qquad \pi_{(p)}(h(x)) = \overline{h(x)} = \overline{c_{n-m}}x^{n-m}$$

[Da riguardare perché mi sembra di non star usando l'ipotesi A UFD. D'altro canto A UFD $\implies$ p irriducibile non dimostra che $\dfrac{A}{(p)}$ è un campo, perché (p) è massimale solo tra gli ideali principali (se A fosse anche PID andrebbe bene).]

[2] Notare come nella dimostrazione per $A = \mathbb{Z}$ si usa il fatto che $\dfrac{\mathbb{Z}}{(p)}$ sia un campo, che per un anello generico non vale (per esempio $\dfrac{\mathbb{Z}}{(x^2+5)} \cong \mathbb{Z}[\sqrt{-5}]$)